

# **Ascend NavisAccess User Guide**

*Ascend Communications*

---

NavisAccess<sup>TM</sup> is a trademark of Ascend Communications, Inc. Other trademarks and trade names mentioned in this publication belong to their respective owners.

Copyright © 1997, Ascend Communications, Inc. All Rights Reserved.

This document contains information that is the property of Ascend Communications, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Ascend Communications, Inc.

Part Number 7820-0511-001 July 31, 1997

---

## Ascend Customer Service

When you contact Ascend Customer Service, make sure you have this information:

- The product name and model
- The software version
- The operating system and version
- The type of installation (server, workstation, standalone)
- A description of the problem

## How to contact Ascend Customer Service

Ways to contact Ascend Customer Service	Telephone number or address
Telephone in the United States	800-ASCEND-4    800-272-3634
Telephone outside the United States	510-769-8027
E-mail	support@ascend.com
Facsimile (FAX)	510-814-2300

You can also contact the Ascend main office by dialing 510-769-6001, or you can write to Ascend at the following address:

Ascend Communications, Inc.  
1701 Harbor Parkway  
Alameda, CA 94502

## Need information on new features and products?

We are committed to constantly improving our products. You can find out about new features and product improvement as follows:

- For the latest information on the Ascend product line, visit our site on the World Wide Web: <http://www.ascend.com/>
- For software upgrades, release notes, and addenda to this manual, visit our FTP site: <ftp.ascend.com>



---

## CONTENTS

Ascend Customer Service .....	iii
How to contact Ascend Customer Service .....	iii
Need information on new features and products? .....	iii

### CHAPTER 1 : Getting Started with NavisAccess

Before you run NavisAccess for the first time .....	1
Starting NavisAccess.....	1
Security information .....	2
Viewing current software information .....	2
Preparing Devices for use with NavisAccess.....	3
Special considerations for Ascend devices.....	3
MAX and Pipeline families.....	3
Configuring SNMP Trap destinations for the MAX and Pipeline.....	3
Setting SNMP community strings for the MAX and Pipeline.....	5
Enabling Call Logging on the MAX and Pipeline .....	6
Restricting SNMP manager access for the MAX.....	8
MAX TNT.....	9
SNMP management support on the MAX TNT.....	9
Configuring SNMP Trap destinations for the MAX TNT.....	10
Enabling SNMP, community strings on the MAX TNT.....	11
Enabling Call Logging on the MAX TNT .....	14
Special considerations for 3Com routers .....	17
Configuring SNMP Community Names .....	17
Configuring SNMP managers for SNMP Traps .....	19
Configuring line bandwidth.....	19
Configuring MIB variables .....	20
Special considerations for Bay/Wellfleet routers.....	21
Configuring SNMP and Trap Sessions.....	21
Configuring line bandwidth.....	26
Configuring MIB variables .....	29
Configuring Management Priority to high .....	30

---

Special considerations for Cisco routers.....	32
Configuring SNMP Community Names .....	32
Configuring SNMP Trap destinations .....	33
Configuring line bandwidth.....	34
Configuring SNMP packet size.....	35
Configuring MIB variables .....	35
Special considerations for Novell MPR.....	36
Configuring SNMP Community Names .....	36
Configuring SNMP managers for SNMP Traps .....	37
Configuring MIB variables .....	38
Special considerations for Digital Equipment devices .....	39
Configuring SNMP Community Names and traps .....	41
Configuring SNMP system MIB variables .....	44
Configuring interface bandwidth .....	46
Configuring SNMP packet size (DECbrouter 90).....	47

## **CHAPTER 2 : Device Discovery**

Introduction to device discovery .....	48
Visual indicators for discovery.....	49
Automatic discovery - the Explorer.....	49
Introduction to the Explorer .....	49
To run the Explorer .....	50
Manual discovery.....	52
Introduction to manually adding new devices.....	52
To Manually add a new device.....	52
Troubleshooting / restarting discovery .....	54
Why did discovery fail?.....	54
Identifying an unknown device.....	54
To restart discovery of a device .....	54
To restart discovery of multiple devices .....	55

## **CHAPTER 3 : User Management - Security**

Security: Overview.....	57
Logging in.....	59
Changing passwords.....	60
Adding and deleting users, assigning rights .....	60
Logging out.....	63

---

## **CHAPTER 4 : The Group Wizard**

The Group Wizard: Overview .....	65
The Group Wizard window .....	65
Other buttons .....	68
Filtering and finding devices in Group Wizard .....	68
Device grouping: overview .....	70
Ideas for creating groups .....	70
Creating device groups .....	71
Linking, copying, moving, editing and deleting groups.....	75

## **CHAPTER 5 : Access Watch - Remote Access at a Glance**

Access Watch: Overview.....	79
Starting and using Access Watch .....	80
Reading the Access Watch window: top level .....	81
More about Dropped Calls .....	84
Configuring Access Watch .....	91
Calculating the moving average .....	93
Access Watch drill-down levels .....	94
The Active Sessions window.....	94
The Call Monitor window.....	95
The Modem Pools window.....	97
The Modem Pool window .....	99
The Slot Modem Table window .....	100
The Wan Line Table window.....	104
The WAN Line Channel Table window.....	108

## **CHAPTER 6 : The Boxmap**

The Boxmap .....	113
Physical view .....	113
Application view .....	116

## **CHAPTER 7 : The Internet Map**

The Internet Map: Overview.....	117
Reading the Internet Map .....	118
Map navigation and manipulation.....	123
The Internet Map Navigator .....	124

---

Search Node function .....	125
Moving and Scaling Map Icons .....	126
Cutting, pasting and copying in the Internet Map .....	128
The Network Filter .....	129
Saving an Internet Map .....	130
Launching applications from the Map .....	131
Grouping map items into logical entities .....	132
Rollup Functionality .....	133
Adding a link to the Map .....	137
Cutting nodes from the Map .....	139
Internet Map drill down levels .....	141
Subnet Maps .....	141
Segment Map .....	143
Circuit Map .....	144
The Consolidate Map option .....	145
Zooming in with submaps .....	148
Alarm functions from the Map .....	149
Virtual Elements .....	150
Configuring Virtual Elements .....	150
Using Virtual Elements .....	151
Table of device icons .....	151
Table of Digital Equipment device icons .....	152
Segment icons - Internet Map .....	155
Circuit icons - Internet Map .....	155

## **CHAPTER 8 : Device Management - Configuration Tools**

Device Configuration: overview .....	156
The Configuration applet .....	157
The Configure Router applet .....	159
Starting the Configure Router applet .....	160
Downloading a configuration file from a device .....	161
Select Download Mode options window .....	164
Saving a configuration file .....	166
Deleting a configuration file from the database .....	168
Retrieving a configuration file from the database .....	169
How to edit a configuration file .....	169
Exporting a configuration file .....	172

---

Importing a configuration file .....	173
Comparing files: performing a differences operation.....	173
Uploading a configuration file.....	176
Cisco specific tools.....	177
Write Memory: Cisco specific .....	177
Erase Memory: Cisco specific.....	177
Device software tools .....	179
Binary Image applet: Ascend specific.....	179
Using the Binary Image applet.....	179
The File Manager applet: 3Com specific.....	181
Using the File Manager applet .....	181
The Flash Manager applet: Cisco specific.....	185
Using the Flash Manager applet: Cisco specific.....	186
The File Manager applet: Bay/Wellfleet specific .....	190
Using the File Manager applet: Bay/Wellfleet specific.....	191
System reset - Ascend devices.....	196
Radius Server applet - Ascend devices .....	196
The TFTP Server .....	198
TFTP Server Session tabs .....	198
TFTP Server Statistics tab .....	200
TFTP Server Setup tab.....	201
The Telnet applet .....	203
Starting the Telnet applet.....	203
Configuring the Telnet applet.....	203
The Show Commands applet: Cisco specific .....	204
The Chassis Report applet: Overview .....	206
Using the Chassis Report.....	206
The Chassis Report for Ascend devices.....	207
The Chassis Report for Digital devices .....	208
The Chassis Report for Cisco devices and the Digital Gigaswitch.....	210

## **CHAPTER 9 : Automating Data Collection: The Schedule Wizard**

The Schedule Wizard: Overview.....	216
Data collection and reporting: How it works.....	216
Schedule Wizard applications.....	218
AutoScan .....	218
Background Alarm Monitor .....	218

---

Background AppleTalk Performance .....	218
Background CIR Trending.....	219
Background CPU Utilization .....	219
Background Image Uploader.....	219
Background Interface Utilization .....	220
Background IP Performance .....	220
Background IPX/SPX Performance .....	221
Configuration Uploader .....	221
Device Change Control.....	222
Database Groomer .....	222
Explorer.....	223
Interface Status Monitor .....	223
Using the Schedule Wizard.....	224
Creating schedules .....	225
Creating a utilization schedule: protocols, CPU.....	225
Creating a Frame Relay schedule: CIR trending .....	230
Creating an Image Uploader schedule .....	235
Creating a Configuration Uploader schedule .....	238
Creating a Device Change Control schedule .....	242
Creating an Explorer schedule .....	246

## **CHAPTER 10 : Reporting and Database Management**

Device Database: Overview.....	251
Starting The Device Database program.....	252
Database Maintenance: DeviceDB.....	253
Database Maintenance: overview .....	253
Deleting devices, interfaces and protocols .....	255
Chassis information: viewing and deleting.....	256
Configuration File Database: viewing and deleting .....	258
Database Tools: overview .....	261
Database backup and restore .....	262
Generating a fresh database .....	263
Repairing a database .....	264
Reporting.....	265
Reporting: overview .....	265
Creating a Performance Report.....	269
Running, editing and deleting performance reports .....	275

---

Creating Configuration and Query Reports .....	277
Creating an Address Summary report .....	277
Creating a Chassis Report .....	280
Creating a Device Configuration report.....	282
Creating a Device Summary report .....	284
Creating a Device Version report .....	285
Creating an Account Disconnect report.....	286
Exporting graph data.....	287
Publishing Web reports .....	288
Report details and samples .....	292
Remote Access Reports .....	292
Hourly/Daily Network Channel Availability/Utilization.....	292
Hourly/Daily Average Network Connect Time .....	294
Hourly/Daily Modem Availability/Utilization.....	295
Hourly/Daily Number of Logins .....	295
Hourly/Daily Active Sessions .....	297
Network Performance Reports .....	298
Daily Network Capacity .....	298
Network Capacity Leaders .....	298
Hourly Network Capacity.....	300
Interface Utilization With Protocols .....	301
Interface Utilization Versus Time .....	301
Interface Utilization As A Percentage Of Time.....	302
CPU Utilization.....	304
AppleTalk Protocol Performance .....	305
IP Protocol Performance.....	306
IPX Protocol Performance .....	308
Frame Relay VC Utilization .....	308
Frame Relay Network Capacity Leaders .....	310
Frame Relay Hourly Network Capacity .....	312
Frame Relay Daily Network Capacity.....	313
Configuration and Query Reports .....	319
Device Summary Report.....	314
Address Summary Report.....	315
Device Configuration Report .....	316
Chassis Report.....	317
Device Version Report.....	317

---

---

Account Disconnect Report .....	318
Graph functionality .....	319

## CHAPTER 11 : Network Awareness - Fault Detection

Fault detection .....	322
ACE - Event Correlation .....	324
Setting error thresholds .....	326
The Threshold Manager.....	326
Setting the Threshold Level .....	327
Creating a Threshold Manager schedule.....	331
Threshold Manager error types .....	333
AppleTalk errors .....	333
IP errors.....	334
IPX errors .....	334
System/Interface errors.....	335
TokenRing errors .....	335
Ethernet Errors.....	337
FDDI errors .....	338
Source Route Bridging errors .....	338
Spanning Tree Protocol errors .....	338
CISCO specific errors .....	339
Frame Relay errors.....	339
Setting interface utilization levels .....	340
The Interface Utilization Thresholds applet .....	340
Setting Interface Utilization Thresholds.....	340
Creating an Interface Utilization Thresholds schedule.....	342
Setting interface up/down status levels.....	346
The Interface Status Thresholds applet .....	346
Setting the Interface Status Thresholds .....	347
Creating an Interface Status Thresholds schedule .....	348
Monitoring for device errors .....	350
Alarm Monitor: Overview.....	350
Starting the Alarm Monitor.....	353
Monitoring interface up/down status.....	356
Alert overview.....	356
Using the Alert applet.....	357
Comprehensive system events.....	358

---

The Event Viewer: Overview .....	358
Using the Event Viewer applet .....	363
Historical event data.....	364
Event Report: Overview .....	364
Using the Event Report.....	366
Miscellaneous fault tools .....	368
Incident Monitor.....	368
System Log Monitor.....	369
Using the System Log Monitor .....	370
Trap Handler.....	371
Ascend Correlation Engine: Overview.....	373
ACE - New Interface Detection .....	374
ACE - Interface Status Monitor .....	378
ACE - Chronic Unstable Interface .....	381
ACE - Chronic Link Overload .....	384
ACE - Device Specific Configuration .....	387
ACE - Multiple Device Configuration.....	388

## **CHAPTER 12 : The PathFinder Tool**

PathFinder: Overview .....	395
Starting PathFinder from the main window .....	389
Starting PathFinder from the Internet Map window .....	390
Understanding the PathFinder results .....	391
Configuring PathFinder .....	395
Creating a PathFinder Virtual Element.....	398

## **CHAPTER 13 : Network Performance - Monitoring Tools**

Performance Distribution .....	401
The Performance Distribution applet: Overview .....	401
Top 10 Utilization .....	404
The Top-10 Utilization applet: Overview .....	404
IP Tools.....	407
IP Tools: Overview .....	407
The IP Performance applet .....	408
The IP Route Table applet.....	411
The IP Address Table applet.....	415
The IP Translation Table applet.....	416

---

The ICMP Statistics applet.....	418
The SNMP Statistics applet.....	421
The Clear ARP Applet: Cisco specific .....	424
IPX tools .....	425
IPX/SPX Tools: Overview.....	425
The IPX/SPX Performance applet .....	426
The IPX/SPX Route Table applet.....	428
The IPX/SPX SAP Table applet.....	431
The IPX/SPX Overview applet.....	435
NLSP Applets.....	442
NLSP Tools: Overview .....	442
The NLSP Overview Applet .....	443
The NLSP Area Addresses Applet.....	446
The NLSP Neighbors Table Applet .....	448
The NLSP Learned Routers Applet.....	449
The NLSP Learned Networks Table Applet .....	451
AppleTalk tools .....	453
AppleTalk Tools: Overview.....	460
The AppleTalk Performance applet.....	454
The AppleTalk Route Table applet .....	456
The AppleTalk Translation Table applet.....	458
Interface Table applet.....	460
Using the Interface Table applet .....	463
Individual interface tools .....	464
Individual Interface tools: Overview.....	470
The Description applet .....	466
The Utilization applet .....	467
The Virtual Circuit Utilization applet.....	469
The Output Queue Length applet.....	472
The X.25 Circuits applet .....	474
The X.25 Statistics applet.....	477
Tools for Cisco devices .....	480
Cisco Specific Interface tools: Overview .....	480
The Utilization Applet- Cisco Specific.....	480
The Utilization Distribution Applet - Cisco Specific.....	483
The Clear Interface Applet - Cisco Specific .....	485
The Mean Packet Size Applet - Cisco Specific.....	486

---

---

The Mean Packet Size Distribution applet - Cisco Specific.....	489
Tools for 3Com devices.....	493
3Com Specific Interface Tools: Overview .....	493
The Ethernet Statistics Applet:3Com Specific .....	494
The TokenRing Statistics applet - 3Com Specific.....	496
CPU Utilization tools .....	499
The CPU Utilization applet - Cisco specific .....	499
The CPU Utilization applet - 3Com specific.....	502
ISDN tools.....	504
The ISDN Neighbor Table applet - Cisco specific.....	504
Using the ISDN Neighbor Table applet.....	505
Frame Relay tools .....	506
The Frame Relay Interface Configuration applet .....	507
The Frame Relay Virtual Circuit Utilization applet .....	510
The Frame Relay Virtual Circuit Statistics applet .....	512
The Frame Relay Virtual Circuit Link Utilization applet .....	515
The Frame Relay Virtual Circuit Link Statistics applet .....	517
The DLCI Configuration applet.....	521
Configuring Virtual Circuit Links.....	523
X.25 Tools.....	527
X.25 Administrative Table applet .....	529
X.25 Administrative Table Overview applet.....	532
X.25 Administrative Table Timer Variables applet.....	536
X.25 Administrative Table Counter Variables applet.....	538
X.25 Call Parameters Table applet .....	539
X.25 Operational Table applet.....	540
X.25 Operational Table Overview applet .....	543
X.25 Operational Table Timer Variables applet .....	546
X.25 Operational Table Counter Variables applet .....	548
Bridging tools .....	550
The Learned Bridging applet.....	551
The Static Bridging Table.....	555
The Spanning Tree Port Table .....	558
The Base Port Table.....	560
The Source Route Bridging applet .....	561
The Static Bridging Table, source route .....	564
The Bridge Telnet Show Commands applet: Cisco specific.....	566

---

---

Port applet: for DEC Gigaswitch .....	567
Port applets: overview .....	567
The Group Port Info applet.....	567
The Port Utilization applet.....	569

## **CHAPTER 14 : Accounting Applets - Bytes and packets**

Accounting applets.....	571
The IP Accounting applet .....	571
The IPX Accounting applet .....	573

## **CHAPTER 15 : Memory and Resource applets**

The Small through Huge Buffer Information applets .....	575
The Memory Protocol Resource applet for Digital.....	579
The Buffer Protocol Resource applet for Digital.....	581

## **CHAPTER 16: MIB Tools**

The MIB Compiler .....	583
Using the MIB Compiler .....	583
The MIB Browser: overview.....	585
Using the MIB Browser .....	586
Running a MIB Profile .....	591
MIB profile example 1: Table display .....	592
MIB profile example 2: Column display.....	595
MIB profile example 3: Graph display .....	598
MIB Compiler Errors .....	600

## **CHAPTER 17 : The BOOTP Server**

BOOTP Server Options tab.....	606
BOOTP Server Clients tab .....	607
BOOTP Server Files tab.....	609

## **CHAPTER 18 : Generic functions**

What are "Applets"?.....	611
Protocol and performance applets .....	611
Applet parameters .....	611
Mountain style (filled in line with peaks):.....	613
Line style .....	614

---

Toolbars .....	615
Line graphs .....	616
Pie charts .....	617
Gauges.....	618
Tables .....	620
Exporting data.....	621
The About applet.....	622

## **CHAPTER 19 : Configuring System Options**

Introduction to configuring system options.....	624
The Community String tab .....	626
The SNMP tab.....	627
The Alarm Monitor tab.....	628
The Color tab.....	629
The Boxmap tab.....	630
The Applet tab .....	631
The AutoStart tab.....	632
The Internet tab.....	633
The WebReport tab.....	634

<b>GLOSSARY.....</b>	<b>636</b>
----------------------	------------

<b>INDEX .....</b>	<b>646</b>
--------------------	------------



## **Before you run NavisAccess for the first time**

Please note the following items that must be in place before using NavisAccess:

- Ascend Pipeline, MAX and MAX TNT devices must be running appropriate device software. Consult the NavisAccess *Getting Started Guide* and the README file for the latest information.
- Ascend Pipeline, MAX and MAX TNT devices must have SNMP enabled. See “Special Considerations for Ascend Devices” on page 3 for details.
- To use the Access Watch application, Ascend Pipeline, MAX and MAX TNT devices must have Call Logging enabled (see page 6).
- Device read and read/write community strings must be properly configured. See the following, as applicable:
  - Special Considerations for Ascend devices (page 3).
  - Special Considerations for 3Com Routers (page 17).
  - Special Considerations for Bay/Wellfleet Routers (page ).
  - Special Considerations for the Cisco Router (page 32).
  - Special Considerations for Digital Equipment devices (page 39).
  - Special Considerations for Novell MPR (page 36).
- Any required MIBs should be compiled. See “The MIB Compiler” on page 583 for details.

## **Starting NavisAccess**

1. To start NavisAccess, choose one of the following:

### **Windows NT 3.51 Users:**

From the NavisAccess program group, double-click on the NavisAccess icon.

### **Windows NT 4.0 Users:**

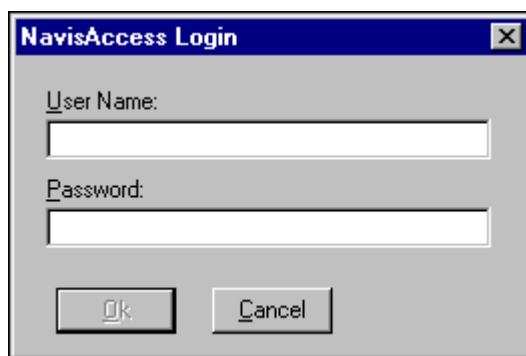
Select NavisAccess from the Start menu on the Taskbar.

## Getting Started

---

(You can also create a shortcut to NavisAccess by right-clicking on the desktop and selecting **New > Shortcut**, then using the browser to locate SRM.EXE in the NavisAccess folder.)

The NavisAccess Login screen appears:



2. Enter your User Name and Password to log in to NavisAccess.

The first time you launch the software, you must use the default User Name of **Admin** and default Password of **Admin**. For more information on security, please see "Security Information" below.

3. Click [OK]. The SNMP and TFTP servers begin automatically.

## Security information

The default login User Name of **Admin** and the default Password of **Admin** must both be changed by an Administrator in order to secure the workstation. In addition, since this initial security login is set at an Administrator Level, only an Administrator can add and modify users and passwords to tailor security requirements for individual networks.

**NOTE:** All security words are CASE sensitive.

For complete security information, please see "Security: Overview" on page 57.

## Viewing current software information

**Menu Bar:** Help > About

To be certain that the license(s) have been added correctly to the software, view the current license information.

The Installed Products window shows which components have been licensed.

## **Preparing Devices for use with NavisAccess**

### **Special considerations for Ascend devices**

Please review the following items before using NavisAccess:

- Ascend Pipeline, MAX and MAX TNT devices must be running appropriate device software. Consult the NavisAccess *Getting Started Guide* and the README file for the latest information.
- To use the Access Watch application, the Call Logging parameters must be set on MAX, Pipeline and MAX TNT devices.
- SNMP Traps must be configured for sending to the IP address of the NavisAccess workstation(s).
- SNMP community strings must be configured.
- You must compile the necessary Ascend MIBs into a format that NavisAccess can use. See "The MIB Compiler" (page 583) for details. Ascend MIBs are installed with NavisAccess. Updates are accessible via FTP on Ascend's FTP server.
- The Ascend device must be able to communicate via TCP/IP with NavisAccess. Make sure that the device can locate that host, either by enabling RIP on the Ethernet interface or by configuring a static route.

Details on the above are found in the sections that follow.

### **MAX and Pipeline families**

#### **Configuring SNMP Trap destinations for the MAX and Pipeline**

The Ascend MAX and Pipeline products send alarm messages in the form of SNMP Traps. These Traps are sent to a management station (such as NavisAccess) for logging and interpretation. If there is an existing management station in your network, the devices may be set up to pass all Traps to it. Contact the network administrator for this information.

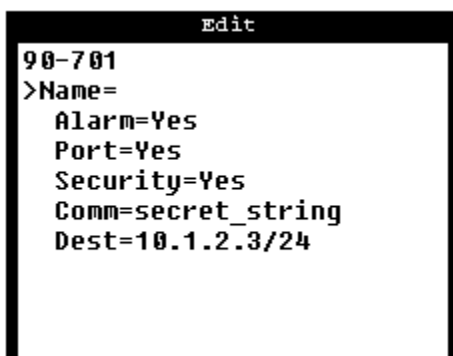
##### **To configure the MAX/Pipeline Trap destination:**

1. Attach to the MAX/Pipeline via Telnet or through the console port.
2. Log in with write access.

## Getting Started

---

3. Open the Ethernet menu.
4. Open the SNMP Traps menu.
5. Press [Enter] to open a profile.



6. Assign a name to the profile. For example:

**Name=Navis\_Machine**

The name can be up to 31 characters. It is typically set to the destination of the trap PDUs (for example, the hostname of the NavisAccess machine).

7. Turn on traps for alarm events, port state changes and security events.

**Alarm=Yes**  
**Port=Yes**  
**Security=Yes**

8. Enter the SNMP community string for the MAX. For example:

**Comm=secret\_string**

The entered string must match the SNMP R/W or read “community name,” which becomes a password sent to the SNMP management station when an SNMP trap event occurs. It authenticates the sender who is identified by the source IP address. See “Setting SNMP community strings for the MAX and Pipeline”.

**NOTE:** To turn off SNMP traps, delete the value for the Comm parameter and set the next parameter (Dest) to 0.0.0.0.

9. Specify the IP address of a NavisAccess machine. If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine. Information will be shared across all NavisAccess stations via the NavisAccess common event system. For example:

**Dest=10.1.2.3/24**

Dest establishes the destination address of the trap-status report. Use IP dotted decimal format. Its default value is 0.0.0.0.

**NOTE:** To turn off SNMP traps, set Dest=0.0.0.0 and delete the value for Comm.

10. Save and close the SNMP Traps Profile.

### Setting SNMP community strings for the MAX and Pipeline

SNMP validates each message with a password-like mechanism called a Community Name. There are two communities defined on the MAX and Pipeline families:

- **Read Comm**  
Enables an SNMP manager to perform read commands (GET and GET NEXT) to request specific information. The default Read Comm string is **public**.
- **R/W Comm**  
Enables an SNMP manager to perform both read and write commands (GET, GET NEXT, and SET), which means the application can access management information, set alarm thresholds, and change some settings on the devices. The default R/W Comm string is **write**.

If there is an existing management station on your network, the community names may have been changed from the default values. Contact the network administrator for this information.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

**SECURITY NOTE:** There is no way to turn off SNMP write, so you must change the default read-write string to secure the unit against unauthorized SNMP access.

### To configure the MAX and Pipeline community names:

1. Attach to the MAX/Pipeline via Telnet or through the console port.
2. Log in with write access.
3. Open the Ethernet menu.
4. Open the Mod Config submenu.
5. Open the SNMP Options submenu.
6. Enter up to 16 characters for the Read Comm parameter. For example:  
**Read Comm=*secret\_string***
7. Enter up to 16 characters for the R/W Comm parameter. For example:  
**R/W Comm=*unique\_string***
8. Save and close the Ethernet profile.

## Enabling Call Logging on the MAX and Pipeline

In order for the Access Watch application to receive data from the MAX and/or Pipeline devices, the Call Logging feature must be enabled and set to send data to the NavisAccess workstation(s). Up to three IP addresses can be configured.

**NOTE:** If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine(s). Information will be shared across all NavisAccess stations via the NavisAccess common event system. This means that data can be propagated over more than the number of IP addresses enabled on the device.

### To configure Call Logging for use with Access Watch:

1. Attach to the MAX/Pipeline via Telnet or through the console port.
2. Log in with write access.
3. Open the Ethernet menu.
4. Open the Mod Config menu.
5. Open the Call Logging menu. (You may need to scroll down the menu list to see this entry.)

```
      Edit
90-900 Mod Config
Call Logging...
>Call Log=Yes
  Host #1=0.0.0.0
  Host #2=0.0.0.0
  Host #3=0.0.0.0
  Dst Port=1646
  Call Log Timeout=1 A
  Key=
  Acct-ID Base=10
  Reset Timeout=0
```

6. Set the Call Log field to Yes. To do so, move the cursor to the field and press [Enter].
7. Enter up to three Host IP addresses. These are NavisAccess machines to which Call Logging will send information. For example:

```
Host #1 = 10.1.2.3
Host #2 = 10.1.2.4
Host #3 = 10.1.30.10
```

8. If necessary, change the Dst Port value. This is the destination port through which the device will send information.
9. Set the Call Log Timeout period from 1 to 60 seconds.

The device sends a request to the first host on the list of hosts specified (see step 7) and waits for a response from the server for the number of seconds specified in the Call Log Timeout parameter. If the device does not receive a response within that time, it sends a second request for authentication to the same server and waits for the same amount of time. If the device does not receive a response within the specified timeout, it sends a request to the next host on the list and repeats the process.

10. Enter a Call Logging Key. (up to 20 characters). The Key is used to provide NavisAccess with access to the device. The same Key entered on the device must also be entered in NavisAccess. This is similar in function to the community string, but not the same.

A default Call Logging Key can be entered in NavisAccess using the Default Secret field on the Access Watch Configuration tab found under **Config > System Options**.

11. The Acct-ID Base parameter determines if data is sent in Base 10 (decimal) or Base 16 (hexadecimal) format. *This value must be set to 10 for Call Logging to work properly.*
12. Set a Reset Timeout period, from 0 to 86400 seconds. (86400 seconds = 1 day.)
13. Save and close the Call Logging profile.

## Restricting SNMP manager access for the MAX

If NavisAccess has the Ascend default read-write community string (“write”), it can control operations such as dialing and hanging up, and monitor the unit’s operational status. To control this level of access to the MAX, we recommend that you specify which IP hosts can access the unit via SNMP manager application, and that you assign a community string other than the defaults that are set when the unit is shipped from the factory.

You can list up to five IP hosts that can access the MIB read-write access, and up to five hosts that can read traps and other information. Following are details about specifying which hosts can access the MIB.

**NOTE:** If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine(s). Information will be shared across all NavisAccess stations via the NavisAccess common event system. This means that data can be propagated over more than the five IP addresses enabled on the MAX.

### To restrict SNMP manager access on the MAX:

1. Attach to the MAX via Telnet or through the console port.
2. Log in with write access.
3. Open the Ethernet menu.
4. Open the Mod Config submenu.
5. Open the SNMP Options submenu.
6. Set the Security parameter to Yes.

#### **Security=Yes**

This parameter specifies that the MAX must compare the source IP address of packets containing SNMP commands against a list of qualified

IP addresses. The unit checks the version and community strings before making source IP address comparisons. (The Security parameter does not affect those checks.)

7. Specify the IP addresses of hosts that will have SNMP read permission. For example:

```
RD Mgr1=10.1.2.3
RD Mgr2=10.1.2.4
RD Mgr3=10.1.2.5
RD Mgr4=10.1.2.6
RD Mgr5=10.1.2.7
```

If the Security parameter is set to Yes, only SNMP managers at those IP addresses will be allowed to execute the SNMP GET and GET-NEXT commands.

8. Specify the IP addresses of hosts that will have SNMP write permission. For example:

```
WR Mgr1=10.1.2.3
WR Mgr2=10.1.2.4
WR Mgr3=10.1.2.5
WR Mgr4=10.1.2.6
WR Mgr5=10.1.2.7
```

If the Security parameter is set to Yes, only SNMP managers at those IP addresses will be allowed to execute the SNMP SET command.

9. Save and close the Ethernet profile.

## MAX TNT

### SNMP management support on the MAX TNT

The MAX TNT supports SNMP on a TCP/IP network. NavisAccess must be running on a host on the local IP network, and the MAX TNT must be able to find that host, either via static route or RIP. In addition to these restrictions, the MAX TNT has its own SNMP password security (community strings) which you should set up to protect the MAX TNT from unauthorized access.

### Configuring SNMP Trap destinations for the MAX TNT

The Ascend MAX TNT sends messages in the form of SNMP Traps. These Traps are sent to a management station (such as NavisAccess) for logging and interpretation. If there is an existing management station in your network, the devices may be set up to pass all Traps to it. Contact the network administrator for this information.

#### To configure the MAX TNT Trap destination:

1. Attach to the MAX TNT via Telnet or through the console port.
2. Log in with write access.
3. At the command prompt, enter:

```
new trap
```

This will return a **TRAP/** “ **read** message and a new command prompt.

4. At the command prompt, enter:

```
list
```

This will return the following parameter list:

```
host-name* = " "  
community-name = " "  
host-address = 0.0.0.0  
alarm-enabled = yes  
security-enabled = no  
port-enabled = no
```

5. Enter a host-name (up to 16 characters), as follows:

```
set host-name = my_host_name
```

The host-name specifies the hostname of the NavisAccess station. This is the host to which the MAX TNT will send SNMP traps. If the host-address field contains an IP address, the specified name is not used to actually locate the host.

6. Enter a community-name (up to 31 characters), as follows:

```
set community-name = my_community_name
```

This specifies the SNMP community name associated with the SNMP PDU (Protocol Data Units). The string you specify becomes a password

that the MAX TNT sends to NavisAccess when an SNMP trap event occurs. The password authenticates the sender identified by the host address.

7. Enter an IP address for the host-address. For example:

```
set host-address = 10.2.3.4
```

The host-address is the same address as that of the NavisAccess station.

**NOTE:** If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine(s). Information will be shared across all NavisAccess stations via the NavisAccess common event system. This means that data can be propagated over more than the number of IP addresses enabled on the MAX.

8. Enable all three classes of Traps.

```
set alarm-enabled = yes  
set security-enabled = yes  
set port-enabled = yes
```

9. Finish the configuration by writing the new parameters to the device, as follows:

```
write
```

This will be followed by a “TRAP/*host-name* written” message.

## Enabling SNMP, community strings on the MAX TNT

The SNMP profile contains SNMP-readable information related to the MAX TNT and its SNMP security. There are two levels of security: community strings, which must be known by NavisAccess to access the box, and address security, which excludes SNMP access unless it is initiated from a specified IP address.

### To enable SNMP and set security on the MAX TNT:

1. Attach to the MAX TNT via Telnet or through the console port.
2. Log in with write access.
3. At the command prompt, enter:

```
read snmp
```

This will return a “SNMP read” message, and a new command prompt.

4. At the command prompt, enter:

```
list
```

This will return the following parameter list:

```
enabled = no
read-community = public
read-write-community = write
enforce-address-security = no
read-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 ]
write-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 ]
contact = " "
location = " "
```

5. Set the enabled parameter to yes as follows.

```
set enabled = yes
```

If the enabled parameter in the SNMP profile is set to No (the default), the MAX TNT cannot be accessed by NavisAccess.

6. If necessary, set new read-community and read-write-community strings (up to 32 characters) as follows:

```
set read-community = secret_string
set read-write-community = unique_string
```

The read-community string permits read access to the MAX TNT and the read-write string permits read/write access.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified on the MAX TNT. Otherwise, communication cannot be established with the device.

7. Set the enforce-address-security parameter to yes, as follows:

```
set enforce-address-security = yes
```

If the enforce-address-security parameter is set to No (its default value), any SNMP manager that presents the right community name will be allowed access. If it is set to Yes, the MAX TNT checks the source IP

address of the SNMP manager and allows access only to those IP addresses listed in the read-access-host and write-access-host arrays. Each array can include up to five host addresses.

8. Set IP addresses for up to five read-access-hosts. For example:

```
set read-access-hosts 1 = 10.2.3.4
set read-access-hosts 2 = 10.2.3.5
set read-access-hosts 3 = 10.2.3.6
set read-access-hosts 4 = 10.2.50.123
set read-access-hosts 5 = 10.2.50.124
```

When this parameter is set, only NavisAccess stations logging in from the set IP addresses will be granted read-access to the MAX TNT.

**NOTE:** If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine(s). Information will be shared across all NavisAccess stations via the NavisAccess common event system. This means that data can be propagated over more than the five IP addresses enabled on the MAX.

9. Set IP addresses for up to five write-access hosts. For example:

```
set write-access-hosts 1 = 10.2.3.4
set write-access-hosts 2 = 10.2.3.5
set write-access-hosts 3 = 10.2.3.6
set write-access-hosts 4 = 10.2.50.123
set write-access-hosts 5 = 10.2.50.124
```

When this parameter is set, only NavisAccess stations logging in from the set IP addresses will be granted write-access to the MAX TNT.

10. It is recommended that you set the contact and location parameters with the name and location of the person to contact if there is a problem with the unit (up to 84 characters). For example:

```
set contact = Mary Smith
set location = Green Bay office, 555-1212
```

11. Finish the configuration by writing the new parameters to the device, as follows:

```
write
```

This will be followed by an “SNMP written” message.

### Enabling Call Logging on the MAX TNT

In order for the Access Watch application to receive data from the MAX TNT, the Call Logging feature must be enabled and set to send data to the NavisAccess workstation(s). Up to three IP addresses can be configured.

**NOTE:** If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine(s). Information will be shared across all NavisAccess stations via the NavisAccess common event system. This means that data can be propagated over more than the three IP addresses enabled on the device.

#### To configure Call Logging for use with Access Watch:

1. Attach to the MAX TNT via Telnet or through the console port.
2. Log in with write access
3. At the command prompt, enter:

**read external-auth**

This will return an "SNMP read" message, and a new command prompt.

4. At the command prompt, enter:

**list**

This will return a parameter list similar to the following. {...} signifies parameter values that will vary based on the device.

**auth-type = None**

**acct-type = None**

**rad-serve-enable = no**

**rad-auth-client = {...}**

**rad-acct-client = {...}**

**rad-auth-server = {...}**

**tac-auth-client = {...}**

**tacplus-auth-client = {...}**

**tacplus-acct-client = {...}**

**local-profiles-first = yes**

5. Set the acct-type parameter to radius as follows:

**set acct-type = radius**

6. Set the rad-serv-enable parameter to yes as follows:

**set rad-serve-enable = yes**

7. Open the rad-acct-client profile as follows:

**list rad-acct-client**

This will return a parameter list similar to the following:

**acct-server-1 = 0.0.0.0**

**acct-server-2 = 0.0.0.0**

**acct-server-3 = 0.0.0.0**

**acct-port = 0**

**acct-key =**

**acct-timeout = 1**

**acct-sess-interval = 0**

**acct-id-base = acct-base-10**

**acct-reset-time = 0**

**acct-checkpoint = 0**

**acct-stop-only = yes**

**acct-limit-retry = 0**

The following parameters must be set for use with NavisAccess:

**acct-server-1 = 0.0.0.0**

This points call logging information to the NavisAccess console. Set this parameter to the IP address of a NavisAccess console.

**NOTE:** If you are using multiple NavisAccess consoles logging in to a common server, you can specify any NavisAccess machine(s).

Information will be shared across all NavisAccess stations via the NavisAccess common event system. This means that data can be propagated over more than the three IP addresses enabled on the MAX.

**acct-server-2 =**

**acct-server-3 =**

These are alternates to the acct-server-1 setting. If the MAX TNT does not receive a response from the NavisAccess console set in acct-server-1, it will try to connect to acct-server-2. Failing that, it will try acct-server-3. These settings are optional.

### **acct-port =**

Set this to match the port setting for the RADIUS daemon's accounting port. This is configured in the daemon's /etc/services file, for example:

**radacct 1646/udp #radius-accounting**

If you used 1646 in the /etc/services file, you must enter 1646 for the acct-port parameter. Values other than 1646 can be used, but both settings must match.

### **acct-key =**

Enter a Call Logging key. The key is used to provide NavisAccess with access to the device. *The same key entered on the device must also be entered in NavisAccess.* This is similar in function to the community string, but not the same.

A default Call Logging key can be entered in NavisAccess using the Default Secret field on the Access Watch Configuration tab found under **Config > System Options**.

To enter a key different from the default, open the device Boxmap, right-click on the Configuration icon and choose **Configuration**. Enter the new key in the Call Logging Secret field.

### **acct-timeout =**

The number of seconds the MAX TNT will wait for a response. This value can be set from 1 to 10. 1 is the default.

### **acct-id-base =**

Specifies if data is sent in Base 10 (decimal) or Base-16 (hexadecimal) format. Parameter settings are Acct-Base-10 and Acct-Base-16, respectively. *This value must be set to Acct-Base-10 for NavisAccess to function properly.*

8. Make the necessary setting changes to the parameters discussed in Step 7. Following is a sample setting of these parameters. Comments are shown in brackets [ ].

<b>set acct-server-1 = 150.10.10.10</b>	[NavisAccess console]
<b>set acct-server-2 = 150.10.10.12</b>	[Alternate NavisAccess console]
<b>set acct-port = 1646</b>	
<b>set acct-key = mysecretstring</b>	[Must match string entered via NavisAccess.]

**set acct-timeout = 2**

**set acct-id-base = Acct-Base-10** [This parameter must be set as shown.]

9. Finish the configuration by writing the new parameters to the device, as follows:

**write**

This will be followed by and "EXTERNAL-AUTH written" message.

### Special considerations for 3Com routers

NavisAccess requires 3Com Software Version 6.2 or higher for the application to operate correctly with a 3Com router. In addition, certain router functions must be configured for the application to operate. The router can be configured by logging into it via a Telnet session or by connecting to the router's console port.

There are four router configuration parameters that must be addressed:

- Configuring SNMP Community Names
- Configuring SNMP Managers for SNMP Traps
- Configuring line bandwidth
- Configuring MIB variables

### Configuring SNMP Community Names

SNMP validates each message with a password-like mechanism called a Community Name. There are two communities defined: read-only and read/write. Each has a unique password. The default values are public and private, respectively. If there is an existing management station on your network, the community names may have been changed from the default values. Contact the network administrator for this information.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

**To configure the router's Community Names:**

1. Connect to the router via Telnet, or through the console port.
2. Log in to the router

### Read-only string

3. To add a read-only Community String type:

```
add -snmp community "com.name" tr no ro
```

The syntax options are:

**com.name**

The read-only community name. It can be up to 16 characters long. Only alphanumeric characters are allowed, and the string must be enclosed within a pair of quotation marks (" ").

**tr**

Enables trivial authentication

**no**

Disables all traps for this community string

**ro**

Makes this community name have read-only access

### Read/write string

4. To add a read/write Community String type:

```
add -snmp community "com.name" tr no rw
```

The syntax options for **tr** and **no** are the same as in Step 3.

**com.name**

The read/write community name. It can be up to 16 characters long. Only alphanumeric characters are allowed, and the string must be enclosed within a pair of quotation marks (" "). This may be the same as or different than the read-only community name.

**rw**

Makes this community name have read-write access

### Trap-community string

5. To add a Trap Community String type:

```
add -snmp community "com.name" tr all ro
```

The syntax options for **tr** and **ro** are the same as in Step 3.

**com.name**

The Trap community name. It can be up to 16 characters long. Only alphanumeric characters are allowed, and the string must be enclosed within a pair of quotation marks (" ").

### **all**

Sends all traps for this community string

This adds a new community which will be configured to send traps to this workstation. See the section "Configuring SNMP Managers for SNMP Traps" below.

## Configuring SNMP managers for SNMP Traps

The 3Com router sends alarm messages in the form of SNMP Traps. These Traps are sent to the management station (such as NavisAccess) for logging and interpretation. If there is an existing management station in your network, the router may be set up to pass all Traps to it. Contact the network administrator for this information.

### **To configure the router's Trap destination:**

1. Attach to the router via Telnet, or through the console port.
2. Log into the router.
3. To add the network management station as a trap destination, type:

```
add -snmp manager "com.name" <ip address>
```

The syntax options are:

#### **com.name**

The Trap community string name. It can be up to 16 characters long. Only alphanumeric characters are allowed, and the string must be enclosed within a pair of quotation marks (" "). This name must match the community name entered in Step 5 of the section "Configuring SNMP Community Names" above.

#### **<ip address>**

The IP Address of the management station, for example, the IP address of the machine running NavisAccess.

## Configuring line bandwidth

The interface utilization of your line can be calculated. To accomplish this, the

interface's available bandwidth must be retrievable. This variable can be configured on the 3Com router. It is only necessary to set the bandwidth on serial media, as all other media default this parameter correctly.

### To configure an interface's bandwidth:

1. Attach to the router via Telnet, or through the console port.
2. Log into the router.
3. At the command line type:

```
setd !<path> -path baud = <bandwidth>
```

The syntax options are:

**<path>**

The interface to configure.

**<bandwidth>**

Can be any one of the following values: 1.2, 2.4, 4.8, 9.6, 9.2, 38.4, 56, 64, 128, 256, 448, 1536, 2048, 3072, 4000, 4608, 6114, 7680, 9216, or 16000.

## Configuring MIB variables

The 3Com router software allows editing of the MIB II variables **sysContact** and **sysLocation**. These variables are displayed in the top pane of the Boxmap. The sysContact variable should contain the name of the person to call if there is a problem on the router. The sysLocation variable should contain the location of the router.

### To configure the router's contact and location:

1. Attach to the router via Telnet, or through the console port.
2. Log into the router
3. To set the sysContact variable, at the command line type:

```
setd -sys syscontact = "contact"
```

**contact**

The name of the person to contact if there is a problem.

4. To set the sysLocation variable, at the command line type:

```
setd -sys syslocation = "location"
```

### **location**

The physical location of the router.

## **Special considerations for Bay/Wellfleet routers**

NavisAccess requires Bay/Wellfleet software Version 5.7 or higher to operate correctly with a Bay/Wellfleet router. In addition, certain router functions must be configured for the application to operate. A Version 5.xx router can be configured by logging into it via a Telnet session, or by connecting to the router's console port. For Version 7.xx routers and above, Bay/Wellfleet Site Manager must be used to configure the router.

There are four Router Configuration Parameters that must be addressed:

- Configuring SNMP and Trap Sessions
- Configuring line bandwidth
- Configuring MIB variables
- Configuring Management Priority to High (only necessary for Version 5.xx routers)

## **Configuring SNMP and Trap Sessions**

SNMP validates each message with a password-like mechanism called a Community Name. There are two communities defined: read-only and read/write. Each has a unique password.

The Bay/Wellfleet router allows for the addition of **SNMP Sessions**. These define the SNMP Community names allowable to manage your router. If there is an existing management station on your network, the SNMP Sessions may have already been added. If so, contact the network administrator for this information.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

The Bay/Wellfleet router sends alarm messages in the form of SNMP Traps. These Traps are sent to the management station (such as NavisAccess) for logging and interpretation. The Bay/Wellfleet router requires that an SNMP Session be added to configure SNMP Trap destinations. If there is an existing management station in your network, the router may already be configured to

pass all Traps to it. Contact the network administrator for this information.

### To Configure SNMP and Trap Sessions for Version 5.xx routers

1. Connect to the router via Telnet or through the console port on the back of the router.
2. Press the Left Arrow [←] key to re-display the Main Menu.
3. Use the arrow keys to move the ---> to the configuration selection.
4. Press [Enter] and the router prompts for the name of the config file. Type **config** [Enter] (if this is the name of your configuration file).
5. The Configuration Editor screen is displayed.
6. To configure SNMP Sessions, type **9** (SNMP Sessions) from the Configuration Editor main menu.
7. The router displays the following information, if no sessions are defined:

```
No SNMP Sessions record(s) found
Do you wish to add SNMP Sessions record(s)?
```

Otherwise, it will display the SNMP Sessions screen. This lists Sessions which have been defined. If a Read Session has been defined, add the IP address of the management station to the list of valid IP addresses. See step 12-17 for the procedure to add additional IP addresses.

8. If no SNMP Sessions have been defined, press [Enter] to display the SNMP Parameters screen:

```
===== SESSION 4 - MGR MODE =====
Configuration Editor 1.19
Current File : CONFIG
Community Name : _____
Session Mode : Read
Session type : Regular
```

9. At the Community Name field, enter the password for the read-only session of the router.
10. At the Session Mode field select **Read**.
11. At the Session Type field select **Regular**. This specifies the query/response model of SNMP.

12. Now the IP address allowed to use this password must be configured. Type **1** in the Enter Selection prompt at the bottom of the screen.

**Enter Selection (0 for Previous Menu) : \_\_\_\_\_**

13. The router displays the following:

```
No Node Addresses record(s) found
Do you wish to add Node Addresses record(s)?  Yes
```

only if no IP Address exists for the current SNMP Session. Otherwise, the Community Members Summary screen is displayed. This screen lists the valid IP address for the current SNMP Session. If this is the case proceed to step 18.

14. Press [Enter] to display the SNMP Community Member Address screen..

```
I 07/14/93 09:22:05 tftp: 'transfer CONFIG
complete'
=====SESSION 4 - MGR MODE =====
Configuration Editor 1.19
Current File : CONFIG
Node Address : _____
```

15. At the Node Address field, enter the IP address of the community member granted access to the local MIB.
16. After the screen prompts, **Hit Return to Continue**, do so to revert to the SNMP Community Member Access Screen.
17. To grant access to another IP address, type **1** [Enter] at the prompt of the Community Members Summary screen. This lists the IP address of all community members granted MIB access.

**NOTE:** IP address 0.0.0.0 is a special case that is valid only for communities with a Session Type of Regular. IP address 0.0.0.0 permits all IP addresses to use the community name.

18. Now an SNMP TRAP Session must be added. This is done in the same way a Regular session was added, follow steps 7-17. However, in step 11 instead of specifying **Regular** for the Session type field, specify **Trap**.
19. Two additional fields will be displayed after [Enter] is pressed from the **Session Mode** field.

```
Send Event Messages As Traps : No
Event Filter Level : Show All Events
```

## Getting Started

---

See the Bay/Wellfleet Configuration Guide for a description of these two fields.

20. Add the IP address of the management station as one of the TRAP destinations.
21. Press [Enter] until the main menu is displayed.
22. Save the configuration file and reboot the router for the changes to take effect.

### To Configure SNMP and TRAP Sessions for Version 7.xx and above routers

This section details how to configure the SNMP software to operate with the application.

1. To edit the SNMP global parameters, from the Bay/Wellfleet Configuration Manager menu, select **Protocols > IP > SNMP > Global** to display the global parameters screen:

**NOTE:** Your Configuration Information Screens may vary depending on the software installed.

Edit SNMP Global Parameters

Configuration Mode: dynamic  
SNMP Agent: 150.50.10.2

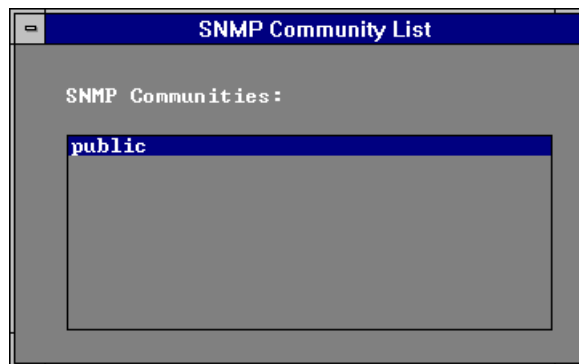
Save Values... Help... Cancel

SNMP Global Parameters

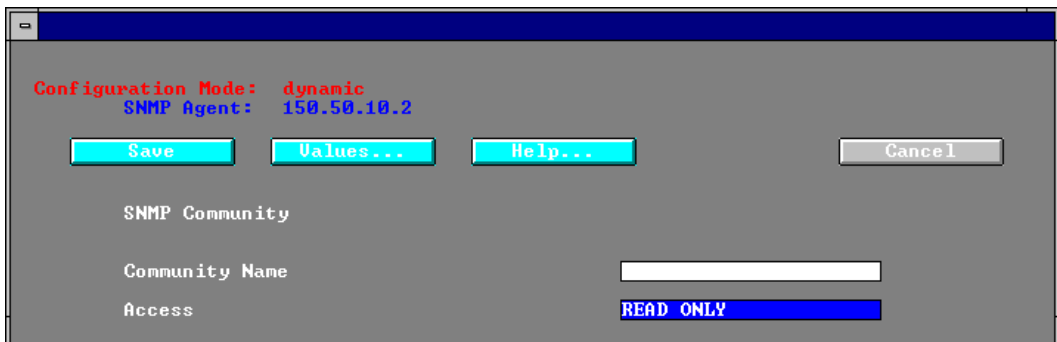
Enable	ENABLE
Use Lock	ENABLE
Lock TimeOut	2
Authentication Failure Traps	ENABLE
Trap Debug Events	ON
Trap Trace Events	ON
Trap Info Events	ON
Trap Warning Events	ON
Trap Fault Events	ON

Your router should be configured to send Trap messages for Warning Events and Fault Events. All other Traps should be disabled.

2. Once the global configuration has been established, SNMP Communities must be added for the management stations. To add an SNMP community, from the Bay/Wellfleet Configuration Manager menu select **Protocols > IP > SNMP > Communities** menu option to display the SNMP Community List:



3. To add a community, select **Community > Add Community** to display the SNMP Community Window.



4. Type in the Community Name and change the Access to Read-Write. Click on the [Save] button to complete the operation, or on the [Cancel] button to abort the operation.

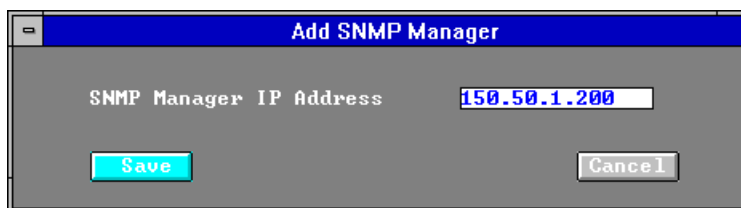
**NOTE:** A read write password is only necessary for the File Management applet.

5. Once the new SNMP Community has been added, SNMP Managers must

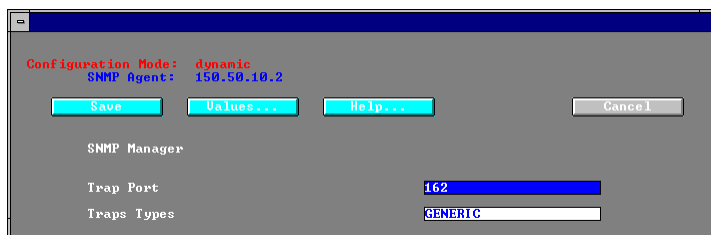
## Getting Started

---

be added to this community. To begin, select the new community from the SNMP Community List window displayed above. Then select **Community > Add Manager** menu option, to display the Add SNMP Manager window.



6. Enter the IP Address of the management station and click on the [Save] button, or on the [Cancel] button to abort.
7. The management station's IP Address should be configured to receive TRAP messages from the router. To accomplish this, from the Bay/Wellfleet Configuration Manager menu, select the **Manager > Edit Manager** menu option, to display the Edit Manager window.



8. Select Specific for the Traps Types field to enable all Bay/Wellfleet specific Traps to be generated to the management station.

## Configuring line bandwidth

The Interface Utilization of your Line can be calculated. In order to accomplish this task, each interface's available bandwidth must be able to be retrieved. This variable can be configured on the Bay/Wellfleet router.

### To Configure Line Bandwidth for Version 5.xx routers

1. Connect to the router via Telnet, or through the console port on the back of the router.
2. Hit the Left Arrow [←] key to re-display the Main Menu.

3. Use the arrow keys to move the ---> to the configuration selection.
4. Press [Enter] and the router prompts for the name of the config file. Type **config** [Enter] (if this is the name of the configuration file).
5. The Configuration Editor screen is displayed.
6. To configure an interface's bandwidth, type **5** (Circuit Groups) from the Configuration Editor main menu.
7. The router displays the available circuit groups:

```

=====--  SESSION 4 - MGR MODE=====
Configuration Editor 1.19
Current File : CONFIG
Circuit Groups
Circuit Group Name  -----
  1. G_E21
  2. G_S21
  3. G_S22

```

**Action (-> for selections) : Previous Display**

8. Press the Right Arrow [→] key to choose the “Modify” action and press [Enter].

**Action (-> for selections) : Modify**

9. The router prompts for the desired selection.

**Enter Selection (0 for Previous Menu) : \_\_\_\_**

10. Enter the number of the circuit group to modify and press [Enter]. The router displays the group configuration screen:

```

=====--  SESSION 4 - MGR MODE  -----
Configuration Editor 1.19
Current File : CONFIG
Circuit Group Name : G_E21_____
Circuit Group Speed : 10000000

```

11. Press [Enter] until the “Circuit Group Speed” field is selected and enter the correct line speed (e.g. 10,000,000 for an Ethernet interface, 16,000,000 for Token Ring, etc.).
12. Press [Enter] until the Configuration Editor main menu is displayed.

## Getting Started

---

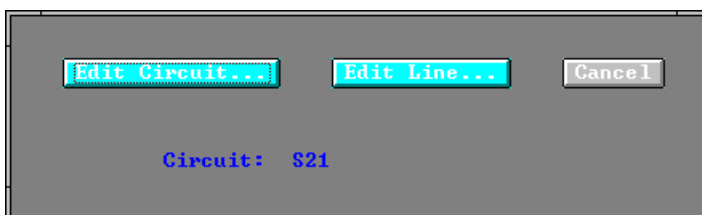
13. Save the configuration file. Reboot the router for the changes to take effect.

### To Configure Line Bandwidth for Version 7.xx and above Routers

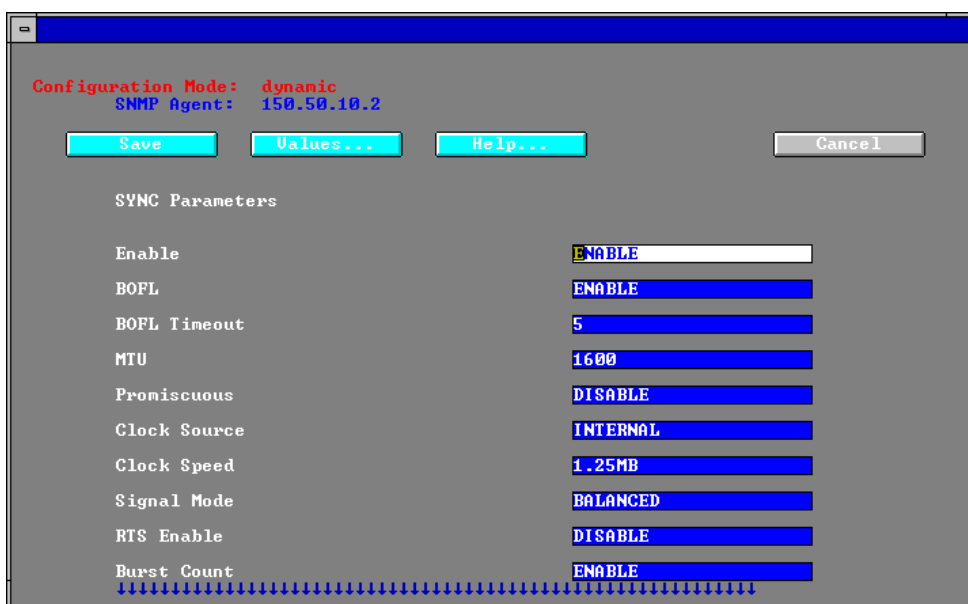
This section describes how to configure the Line Bandwidth reported by a Bay/Wellfleet router.

1. To edit this parameter, click the left mouse button over the desired circuit to edit. This displays the Circuit screen:

**NOTE:** Your screens may vary depending on the software installed.



2. Click on the Edit Line button to display the Edit Line Parameters window.



3. Edit the Clock Speed field of this screen to match the Clock Speed of the Line.

## Configuring MIB variables

The Bay/Wellfleet router software allows editing of the MIB II variables **sysContact** and **sysLocation**. These variables are displayed in the top pane of the Boxmap. The sysContact variable should contain the name of the person to call if there is a problem on the router. The sysLocation variable should contain the location of the router.

### To Configure MIB Variables for Version 5.xx Routers

1. Connect to the router via Telnet, or through the console port on the back of the router.
2. Hit the Left Arrow [←] key to re-display the Main Menu.
3. Use the arrow keys to move the ---> to the configuration selection.
4. Press [Enter] and the router prompts for the name of the config file. Type **config** [Enter] (if this is the name of the configuration file).
5. The Configuration Editor screen is displayed.
6. To change the contact and Location variables of the router, type **1** (System) from the Configuration Editor main menu.
7. The router prompts for an action to perform at the bottom of the display.  
**Action (-> for selections) : Browse**
8. Press the Right Arrow [→] key to choose the “Modify” action and press [Enter]  
**Action (-> for selections) : Modify**
9. The System Configuration screen is displayed. Press [Enter] until either the System Contact, or System Location field is highlighted.

```
=====-- SESSION 4 - MGR MODE -=====
Configuration Editor 1.19
Current File : CONFIG

System Name : WFL_EAST_____
Auto Enable : Yes
```

## Getting Started

---

```
Automatic Reboot : No
Enable Logging : Yes

System Contact : Jack Dempsey 516 555-6060

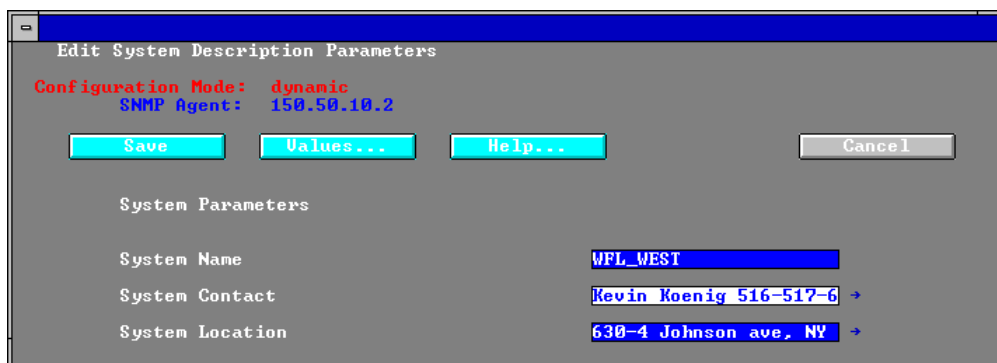
System Location : 630 Johnson Ave Bohem ny 11716
office 32
```

10. Enter text into each field. This information will be displayed in the Boxmap.
11. Press [Enter] until the Configuration Editor main menu is re-displayed.
12. Save the configuration file. Reboot the router for the changes to take effect.

### To Configure MIB Variables for Version 7.xx and above Routers

1. To configure the MIB variables select **System Record** from the Bay/Wellfleet Configuration menu to display the Edit System Record window.

**NOTE:** Your screens may vary depending on the software installed.



2. Change the System Contact, System Name, and System Location. Click on the [Save] button to save the data, or on the [Cancel] button to abort.

## Configuring Management Priority to high

The Bay/Wellfleet router software allows for the priority SNMP messages to be configured. The default setting causes many SNMP messages to be discarded by the router. This will cause significant problems for NavisAccess.

The routers management priority **MUST** be configured to **HIGH** for the application to operate correctly.

**NOTE:** This is only necessary for Bay/Wellfleet routers with Version 5.xx software.

### To Configure Management Priority for Version 5.xx Routers

1. Connect to the router via Telnet, or through the console port on the back of the router.
2. Hit the Left Arrow [←] key to re-display the Main Menu.
3. Use the arrow keys to move the ---> to the configuration selection.
4. Press [Enter] and the router prompts for the name of the config file. Type **config** [Enter] (if this is the name of the configuration file).
5. The Configuration Editor screen is displayed.
6. To change the management priority to **HIGH**, type **7** (DoD Internet Router) from the Configuration Editor main menu.
7. The router prompts for an action to perform at the bottom of the display:  
**Action (-> for selections) : Browse**
8. Press the *Right Arrow* key to choose the “Modify” action and press [Enter].  
**Action (-> for selections) : Modify**
9. The IP Router Configuration screen is displayed. Press [Enter] until the cursor is on the “Management Priority” field.

```
=====--  SESSION 4 - MGR MODE  =====
Configuration Editor 1.19
Current File : CONFIG

Auto Enabled           : Yes
Global Broadcast       : Yes

RIP Network Diameter  : 15
Mode : Router/Host
Management Priority    : High
Non Local ARP Source   : Drop and Log
Bootp Gateway Support  : No
```

**Bootp Gateway Auto Enable : Yes**

**Bootp Gateway Max Hops : 3**

**Suppress Authentication Traps : Yes**

10. Press the Right Arrow [→] key until “High” is displayed in this field
11. Press [Enter] until the Configuration Editor main menu is displayed.
12. Save the configuration file. Reboot the router for the changes to take effect.

## Special considerations for Cisco routers

NavisAccess requires Cisco Software Version 8.26 or higher for the application to operate correctly with a Cisco router. In addition, certain router functions must be configured for the application to operate. The router can be configured by logging into it via a Telnet session or by connecting to the router’s console port.

There are five router configuration parameters that must be addressed:

- Configuring SNMP Community Names
- Configuring SNMP Trap destinations
- Configuring line bandwidth
- Configuring SNMP packet size
- Configuring MIB variables

## Configuring SNMP Community Names

SNMP validates each message with a password-like mechanism called a Community Name. There are two communities defined: Read-Only and Read-Write. Each has a unique password. The default values are public and private, respectively. If there is an existing management station on your network, the community names may have been changed from the default values. Contact the network administrator for this information.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

**To configure the router’s Community Names:**

1. Attach to the router via Telnet or through the console port.
2. Log in and enter Enable mode.
3. At the Enable prompt (Hostname#) type **config** and select “terminal”.

### Read-only string

4. Type

```
SNMP-server community <read-only commun name> ro
```

The syntax options are:

**read-only commun name**

The read-only community name.

**ro**

Makes this community name have read-only access

### Read/write string

5. Type

```
SNMP-server community <read-write commun name> rw
```

The syntax options are:

**read-write commun name**

The read/write community name.

**rw**

Makes this community name have read/write access

6. Press [CTRL-Z] to exit configuration mode
7. Make note of the Community Names entered in steps 4 and 5 since they will be required for NavisAccess management tasks.

## Configuring SNMP Trap destinations

The Cisco router sends alarm messages in the form of SNMP Traps. These Traps are sent to a management station (such as NavisAccess) for logging and interpretation. If there is an existing management station in your network, the router may be set up to pass all Traps to it. Contact the network administrator for this information.

### To configure the router's TRAP destination:

1. Attach to the router via Telnet or through the console port.
2. Log in and enter Enable mode.
3. At the Enable prompt (Hostname#) type **config** and select "terminal".
4. Type

```
SNMP-server host <ip-address> <community-name>
```

The syntax options are:

**<ip-address>**

The IP address of the management station.

**<community-name>**

The Trap community name.

5. Press [CTRL-Z] to exit configuration mode

## Configuring line bandwidth

The Interface Utilization of your Line can be calculated. In order to accomplish this task, the interface's available bandwidth must be able to be retrieved. This variable can be configured on the Cisco router.

### To configure an Interface's Bandwidth:

1. Attach to the router via Telnet or through the console port.
2. Log in and enter Enable mode.
3. At the Enable prompt (Hostname#) type **config** and select "terminal".
4. Type

```
interface serial n
```

The syntax options are:

**n**

The interface you want to configure, e.g., 0, 1, etc.

5. Type

```
bandwidth kb
```

The syntax options are:

**kb**

The speed of the line in kilobits per second.

6. Press [CTRL-Z] to exit configuration mode.

## Configuring SNMP packet size

The Cisco router will accept SNMP packets and respond to them. By default in the router, the largest SNMP packet size is 484 bytes. This value is acceptable for most operations that are performed. However, certain router responses exceed this limit. Therefore, you must change the default SNMP packet size on the Cisco router.

### To change the SNMP Packet Size:

1. Attach to the router via Telnet or through the console port.
2. Log in and enter Enable mode.
3. At the Enable prompt (Hostname#) type **config** and select “terminal”.
4. Type  
**SNMP-server packetsize 4096**
5. Press [CTRL-Z] to exit configuration mode.

## Configuring MIB variables

The Cisco router software allows editing of the MIB II variables **sysContact** and **sysLocation**. These variables are displayed in the top pane of the Boxmap. The sysContact variable should contain the name of the person to call if there is a problem on the router. The sysLocation variable should contain the location of the router.

### To configure the router’s contact and location:

1. Attach to the router via Telnet or through the console port.
2. Log in and enter Enable mode.
3. At the Enable prompt (Hostname#) type **config** and select “terminal”.
4. Type  
**SNMP-server location <location-text>**

**location-text**

The physical location of the router.

5. Type

```
SNMP-server contact <contact-text>
```

**contact-text**

The name of the person to contact if there is a problem.

6. Press [CTRL-Z] to exit configuration mode.

## Special considerations for Novell MPR

NavisAccess requires Novell MPR Software Version 2.11 for the application to operate correctly. In addition, certain router functions must be configured for the application to operate. The router can be configured by using rconsole or by using the system console.

There are three router configuration parameters that must be addressed:

- Configuring SNMP Community Names
- Configuring SNMP Managers for SNMP Traps
- Configuring MIB Variables

## Configuring SNMP Community Names

SNMP validates each message with a password-like mechanism called a Community Name. There are two communities defined: read-only and read/write. Each has a unique password. The default values are public and private, respectively. If there is an existing management station on your network, the community names may have been changed from the default values. Contact the network administrator for this information.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

**To configure the router's Community Names:**

1. Attach to the router via rconsole, or through the system console.
2. Log in to the router.

3. To change the Read Only Community String, at the server prompt type:

### **LOAD INETCFG**

Press [Enter] to display the Internetworking Configuration menu.

4. From the Internetworking Configuration menu, select **Manage Configuration**, then [Enter], to display the Manage Configuration menu.
5. From the Manage Configuration menu, select **Configure SNMP Parameters**, then [Enter] to display the SNMP Parameters window.
6. From the SNMP Parameters window, select **Monitor State**, then press [Enter].
7. From the Monitor State options, select **Specified Community May Read**.
8. Enter a name in the Monitor Community field, then press [Enter]. The community name can be up to 24 characters long.

This is the name of the community that is allowed to read management information. SNMP management stations that belong to this community can read the network management database. **Type "public" if you wish to use the default.**

10. For changing the read-write community string, select **Control State**, then press [Enter].
11. From the Control State options, select **Specified Community May Write**.
12. Enter a name in the Control Community field, then press [Enter].

This is the name of the community that is allowed to *read and write* management information. SNMP management stations that belong to this community can read or modify any value in the network management database. **Type "private" if you wish to use the default.**

## Configuring SNMP managers for SNMP Traps

The Novell MPR router sends alarm messages in the form of SNMP Traps. These Traps are sent to the management station (such as NavisAccess) for logging and interpretation. If there is an existing management station in your network, the router may be set up to pass all Traps to it. Contact the network administrator for this information. If NMS is your sole management station, configure the router to send TRAPs to it.

### To Configure the Router's TRAP Destination:

1. Attach to the router via rconsole, or through the system console.
2. Log in to the router.
3. To add the NMS station as a trap destination, at the server prompt type:  
**LOAD INETCFG**  
Press [Enter] to display the Internetworking Configuration menu.
4. From the Internetworking Configuration menu, select **Manage Configuration**, then [Enter] to display the Manage Configuration menu.
5. From the Manage Configuration menu, select **Configure SNMP Parameters**, then [Enter] to display the SNMP Parameters window.
6. From the SNMP Parameters window, select **Trap State**, then [Enter].
7. From the Trap State options, select **Send Traps With Specified Community**.
8. Enter a name (this must match the read-only community name) in the Trap Community field, then press [Enter].

This enters the community name to be included in trap messages.

## Configuring MIB variables

The Novell MPR router software allows editing of the MIB II variables **sysContact** and **sysLocation**. These variables are displayed in the top pane of the Boxmap. The **sysContact** variable should contain the name of the person to call if there is a problem on the router. The **sysLocation** variable should contain the location of the router.

### To Configure the Router's Contact and Location:

1. Attach to the router via rconsole, or through the system console.
2. Log in to the router
3. To set the **sysContact** or **sysLocation** variable, at the command line type:  
**LOAD INETCFG**

Press [Enter] to display the Internetworking Configuration menu.

4. From the Internetworking Configuration menu, select **Manage Configuration**, then press [Enter] to display the Manage Configuration menu.
5. From the Manage Configuration menu, select the **Configure SNMP Information** option.
6. Select the MIB variable that you want to configure and press [Enter].
7. Modify the selected option and press [ESC]. When asked to save the changes, select [yes].

### Special considerations for Digital Equipment devices

The full line of Digital Equipment routers and switches in production are supported. Each product has different levels of support based on the version of software and the hardware configuration. The following table outlines the product support:

Hardware:	Software supported:
Devices with Router Distributing Software installed	V1.0 and above
DECbrouter 90	V9.1X and above
DECNIS	V3.1.2 and above

In addition, NavisAccess requires certain device functions to be configured for the application to operate correctly with Digital Equipment devices. The device/router may be configured by logging into it via a Telnet session or by connecting to the device's console port.

There are four configuration parameters that must be addressed:

- Configuring SNMP Community Names and Traps
- Configuring SNMP System MIB variables
- Configuring Interface Bandwidth
- Configuring SNMP packet size (DECbrouter 90)

## Configuring SNMP Community Names and traps

SNMP validates each message with a password-like mechanism called a Community Name. There are two communities defined: read-only and read/write. Each has a unique password. The default values are public and private, respectively. If there is an existing management station on your network, the community names may have been changed from the default values. Contact the network administrator for this information.

There are separate procedures outlined below for configuring devices with Distributing Router software, DECNIS devices and the DECbrouter 90.

**NOTE:** The read and write Community Names used by NavisAccess must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

### To configure Community Names and Traps for Distributing Router Software Devices:

1. Connect to the device through the console or via Telnet.
2. Log in to the device. The \* prompt is displayed. Type:  
**talk 6**
3. The **Config>** prompt is displayed. Type:  
**protocol snmp**  
The **SNMP Config>** prompt is displayed.

### Read-only and Trap string

4. To add a read-only and Trap Community String, type:  
**add community *string-name***  
**set Community Access read\_trap *string-name***  
The syntax options are:  
**string-name**  
The name to be used for both the read-only and the Trap Community String.
5. Type **CTRL-P** to exit.

### Read/write and Trap string

6. To add a read/write and Trap community string, type:

```
add community string-name  
set community access write_read_trap string-name
```

The syntax options are:

#### **string-name**

The name to be used for both the read/write and the Trap Community String.

7. Type **CTRL-P** to exit.

### Trap string only

8. To add only a Trap community string, type:

```
add community string-name  
set community access trap-only string-name
```

The syntax options are:

#### **string-name**

The name to be used for the Trap Community String.

9. Type **CTRL-P** to exit.

### To configure Community Names and Traps for DECNIS devices:

**NOTE:** If you have an upgraded Management Processor Board in your DECNIS, you should review the documentation supplied with the upgrade to find out how to modify these parameters.

1. Using the DECNIS Configurator on your DECNIS Console, advance through the DECNIS Configurator menu system by selecting the **DECNIS CONFIG** option, and then selecting the device configuration file to be modified.
2. Continue by selecting the **Modify Configuration** option. Then advance to the DOS Window which is entitled **SNMP Community Names**. At this point, the community names and access rights can be entered.
3. When this is completed, continue through the remainder of the windows

until the option to **Return to the Sections Menu** appears. Select **Return to the Sections Menu**.

4. Choose the option to **Create NCL Script**.
5. Then choose the option to Create an Image/CMIP profile.
6. Start the BOOTP Server on the DECNIS Configurator Console.
7. Perform the BOOTP procedure on the DECNIS whose configuration is to be updated.

### To configure Community Names and Traps for DECbrouter 90:

1. Attach to the router via Telnet or through the console port.
2. Login and enter **Enable** mode.
3. At the Enable prompt (**Hostname#**) type **config** and select **terminal**.
4. Type:  

```
SNMP-server community <read-only com name> RO  
[Read-only]
```
5. Type:  

```
SNMP-server community <read-write com name> RW  
[Read/write]
```
6. Press **CTRL-Z** to exit configuration mode

### To configure Trap destination for DECbrouter 90

1. Attach to the router via Telnet or through the console port.
2. Login and enter **Enable** mode.
3. At the Enable prompt (**Hostname#**) type **config** and select **terminal**.
4. Type:  

```
SNMP-server host <ip-address> <community-name>
```

The syntax options are:

```
<ip-address>
```

The IP address of the management station

**<community-name>**

The TRAP community name.

5. Press **CTRL-Z** to exit configuration mode

## Configuring SNMP system MIB variables

The System MIB variables that can be modified are sysContact (the assigned contact for the device), and sysLocation (the location of the device). Both of these variables are displayed in the top pane of the Boxmap.

### To configure contact and location for Distributing Router Software devices:

1. Attach to the device through the console or via Telnet.
2. The \* prompt is displayed. Type:  
**talk 6**
3. The **Config>** prompt is displayed. To set the device location type:

**set location *string***

The syntax options are:

**<string>**

A text string providing the location of the device.

4. To set the device contact type:

**set contact *string***

The syntax options are:

**<string>**

A text string providing the contact information for the device.

5. Press CTRL-P to exit

### To configure contact and location for DECNIS devices:

**NOTE:** If you have an upgraded Management Processor Board in your DECNIS, you should review the documentation supplied with the upgrade to find out how to modify these parameters.

1. Using the DECNIS Configurator on your DECNIS Console, advance

through the DECNIS Configurator menu system by selecting the **DECNIS CONFIG** option, and then selecting the router configuration file to be modified.

2. Continue by selecting the **Modify Configuration** option. Then advance to the DOS Window where the **SNMP Contact** and **SNMP Location** information can be entered. At this point, the information can be entered.
3. When this is completed, continue through the remainder of the windows until the option to **Return to the Sections Menu** appears. Select **Return to the Sections Menu**.
4. Choose the option to **Create NCL Script**.
5. Choose the option to Create an Image/CMIP profile.
6. Start the BOOTP Server on the DECNIS Configurator Console.
7. Perform the BOOTP procedure on the DECNIS whose configuration is to be updated.

### To configure contact and location for DEChrouter 90 devices:

1. Attach to the router via Telnet or through the console port.
2. Login and enter **Enable** mode.
3. At the Enable prompt (**Hostname#**) type **config** and select **terminal**.
4. To configure the location, type:

```
SNMP-server location <text>
```

The syntax options are:

```
<text>
```

A text string providing the location of the device.

5. To configure the contact, type:

```
SNMP-server contact <text>
```

The syntax options are:

```
<text>
```

A text string providing the location of the device.

6. Press **CTRL-Z** to exit configuration mode.

### Configuring interface bandwidth

Interface utilization is calculated based on the ifSpeed configured for the interface. This variable must be set properly for accurate utilization levels to be reported.

#### To configure interface speed for Distributing Router Software devices:

Please refer to the Configuration Manuals for your Distributing Router Software device since the procedure for configuring the interface speed is dependent on the interface type.

#### To configure interface speed for DECNIS devices:

Please refer to your DECNIS Configuration Manuals for the procedures for configure the interface speed for the specific interface type.

#### To configure interface speed for DECbrouter 90 devices:

1. Attach to the router via Telnet or through the console port.
2. Login and enter **Enable** mode.
3. At the Enable prompt (**Hostname#**) type **config** and select terminal.
4. Type:

```
interface serial n
```

Syntax options are:

```
n
```

The interface you want to configure, e.g., 0, 1, etc.

5. Type:

```
bandwidth kb
```

Syntax options are:

```
kb
```

The speed of the line in kilobits per second. For example, a 128 kb line would have **bandwidth 128**.

6. Press **CTRL-Z** to exit configuration mode.

## Configuring SNMP packet size (DECbrouter 90)

The DECBROUTER 90 will accept SNMP packets and respond to them. By default, the device/router uses a 484 byte packet. Certain device responses exceed this size and result in data not getting displayed. It is important to modify the SNMP packet size on the DECBROUTER 90 to rectify this.

### To change the SNMP packet size for DECBROUTER 90 only:

1. Attach to the router via Telnet or through the console port.
2. Login and enter **Enable** mode.
3. At the Enable prompt (**Hostname#**) type **config** and select terminal.
4. Type:  
**SNMP-server packetsize 4096**
5. Press **CTRL-Z** to exit configuration mode.

## Introduction to device discovery

Discovery gathers SNMP information about the devices on your network and creates a database. There are two ways to run Discovery:

- **Automatic**, which discovers the entire network at one time, using the Explorer applet. The Explorer can be started as needed, or scheduled to run at a preset time.
- **Manual**, which discovers one particular device at a time (using the New Device applet).

Both of these methods gather the following information for each device and store it in a database:





- The sysObjId of the device.
- The sysName, sysLocation and sysDescr of the device.
- The available interfaces for the device.
- The discovered protocols of the device.
- Device specific information.

The information gathered is used by NavisAccess to populate Group Wizard and to create the Internet Map. The Internet Map graphically depicts all devices (access servers, routers, switches) found, as well as the subnetworks linked to these devices and the actual connections. Any device can be managed from the Internet Map or Group Wizard.

After the initial population of the database, use Discovery to update the information in your database. This includes identifying an unknown device or re-establishing contact with an existing device which failed to be discovered during the previous Discovery attempt.

Visual indicators for discovery

The Group Wizard window uses visual indicators to denote a device’s state in the network. The following table summarizes the possibilities:

Indicator	Icon	sysObjID Known	Discovery Attempted	Description
Question mark		No	No	Never attempted to discover the device. Therefore, its type is not known.
Question mark with red ‘X’		No	Yes	Attempted initial discovery, the device failed. Device type remains unknown.
Device icon with red ‘X’		Yes	Yes	The device has been discovered previously. However, the last attempt to discover the device has failed.
Device icon		Yes	Yes	The last attempt to discover the device was successful.

Automatic discovery - the Explorer

Introduction to the Explorer

**Menu Bar:** Tools > Explorer

Explorer is run to automatically discover your network and populate the database. Once the database is populated, you can use Group Wizard and the Internet Map to view your network.

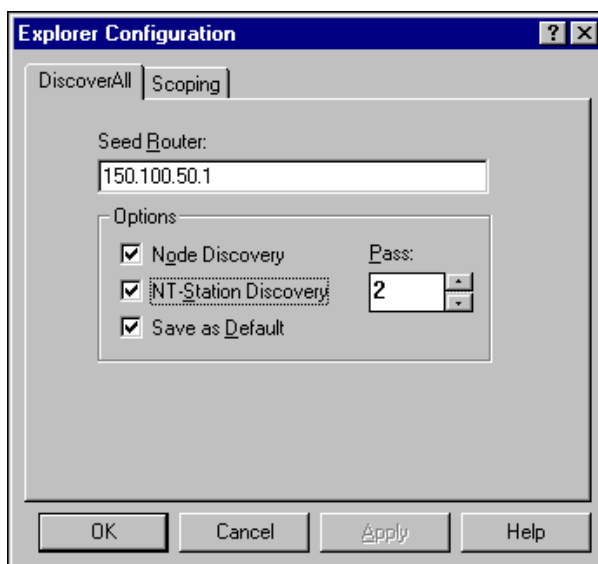
## Device Discovery

---

Explorer can be run manually, or a schedule can be created to run the Explorer at a pre-set time. If your network is frequently changing (new devices, moved devices, swapped cards, etc.), you may want to schedule the Explorer to run on a regular basis at off-hours.

### To run the Explorer

1. Select **Explorer** from the Tools menu. The Explorer Configuration dialog box displays:



2. Configure the settings on the **Discover All** tab.

#### Seed Router

Provide the IP Address for your “Seed Router.” This router is defined as the starting point for discovery of your network. Ascend MAX, MAX TNT and Pipeline devices may be selected as Seed Routers.

#### Node Discovery

Select to have NavisAccess find all system nodes. This option is not recommended for most networks.

#### NT-Station Discovery

Select to have NavisAccess discover all NT workstations and servers. This option is not recommended for most networks.

**NOTE:** To be successfully discovered, the NT machine must have SNMP Service enabled.

### Save as Default

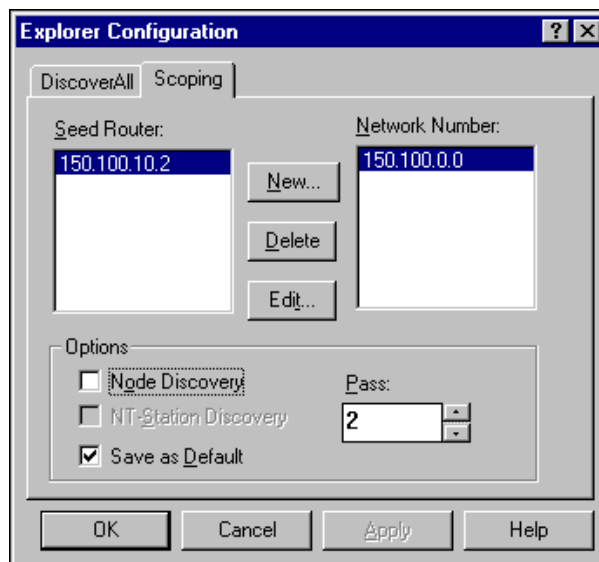
With this option enabled, when Explorer is run for a second time it will begin from the point at which it left off. That is, it will not rediscover devices already discovered. This option is selected by default and is recommended, particularly for large networks.

### Pass

Establish the number of passes which auto discovery will make.

The range for the number of passes is from 1 to 10. Since many devices go down and up, and at times are too busy to respond to SNMP requests, there is the distinct possibility that some may be missed by the Explorer if only one pass is selected. It is therefore recommended that you select at least two passes.

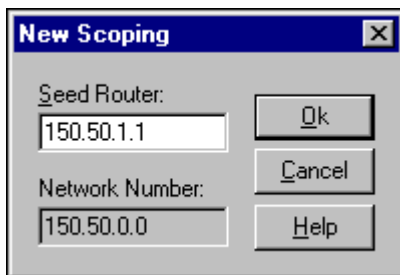
3. If you want to limit the networks which can be discovered, click the **Scoping** tab. In large networks, this can provide a more precise picture of a section of the network. If you are not using Scoping, skip to Step 6.



4. Each network you want to discover requires a seed router. Enter an IP address for each router you wish to use during network discovery. To do this, click the [New] button to open the New Scoping dialog box:

## Device Discovery

---



The Network Number field is automatically filled in. Only devices from the added networks will be discovered.

5. Select Scoping Options. See Step 2 above for definitions.
6. When all the desired options are set, the [Start] button begins the auto detection process. Discovered components will populate Group Wizard and they will also be used to generate the Internet Map.

As devices are added to the database, they are represented by an icon in Group Wizard and shown on a newly rendered Internet Map.

## Manual discovery

### Introduction to manually adding new devices

**Menu Bar:** Select **File > New Device**

The **New Device** feature is used to manually discover your network (that is, discover one device at a time) and populate the database. Once the database is populated, you can use Group Wizard and the Internet Map to view your network.

### To Manually add a new device

1. Select **New Device** from the **File** menu.

This opens the New Device dialog box:

A screenshot of a Windows-style dialog box titled "New Device". The dialog box has a blue title bar with a close button (X) in the top right corner. Inside the dialog, there are four input fields: "IP Address", "Community", "Display Name", and "Comment". The "IP Address" field is a single-line text box. The "Community" field is a single-line text box. The "Display Name" field is a single-line text box. The "Comment" field is a multi-line text box. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

2. Enter a valid IP Address for the device in the IP Address field.
3. Enter an optional, valid, read-only community string for the device in the Community field. If no community string is specified, the default community string defined in System Options Configuration (**Config > System Options**) is used.
4. Enter a Display Name. This is an optional name for the device that can be different than the device's system name (which is set on the device itself).
5. Enter a comment. This can be any information you feel would be useful regarding this device.
6. Click the [OK] button to add the device to the database. Or, click the [Cancel] button to abort.
7. No duplication of IP addresses is allowed throughout the database. If the device IP Address is already in the database, an error message appears.

As devices are added to the database, they are represented by an icon in Group Wizard and shown on a newly rendered Internet Map.

## **Troubleshooting / restarting discovery**

### **Why did discovery fail?**

Discovery may fail for the following reasons:

- The user entered an incorrect community string (or the default in System Options is not correct for this device).
- An incorrect or invalid IP address was entered for a device (or for the Seed Router in Explorer).
- SNMP MIB II is not enabled on the device.
- A filter or firewall blocked communication.

When Discovery fails for a device, it must be restarted for the device to be entered into the database properly.

### **Identifying an unknown device**

If Discovery does not recognize a device, the device is considered **unknown** and the screen displays a question mark in place of an icon for the device.



A yellow question mark indicates that the device was never discovered.



A yellow question mark with a red X indicates that the device failed while it was being discovered.

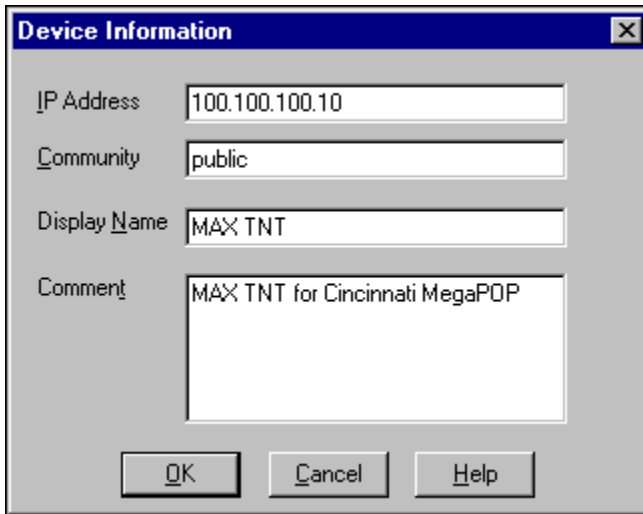
Please see the Visual Indicators table on page 48 for details on what a device display indicates.

### **To restart discovery of a device**

If a device fails to be discovered, you may need to change an IP address or a community string. To restart discovery for an unknown device:

1. Right-click the device icon and select **Device Information**.

The Device Information dialog box displays.



**NOTE:** You may also update the community string using the Configuration applet available via the Boxmap.

2. Enter the correct IP address and Community String for the device, then click [OK].

This automatically updates the device information in the database.

3. Right-click the question mark again and select **Discover Device** to restart discovery.

### To restart discovery of multiple devices

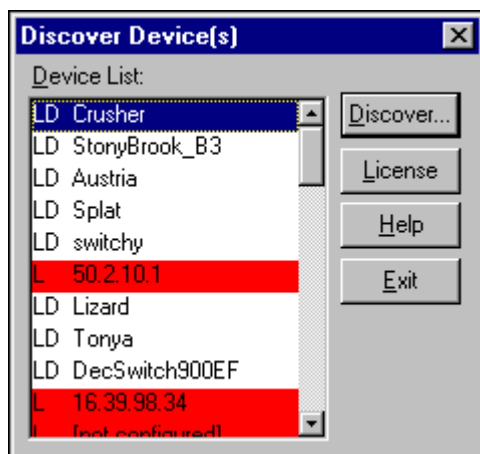
**Menu Bar:** Tools > Discover Devices

1. Select **Discover Devices** from the Tools menu.

The Discover Device(s) dialog box displays:

## Device Discovery

---



2. Highlight the devices you want to rediscover. The standard [SHIFT] and [CTRL] key selection methods apply.
3. Click [Discover].

The device discovery process restarts.

If the discovery completes successfully, the device icon and background color are automatically updated.

## Security: Overview

Three levels of security exist for NavisAccess:

- **Administrator:** complete access to all features and can add and modify users. These Administrative rights are not modifiable or revocable.
- **Managers:** assigned specific devices or groups to open, but cannot add or modify users. Has access to all other features.
- **Operators:** assigned specific devices or groups to open, and may not add or modify users. Has limited access to features.

The Security Levels Table below defines rights granted to each user level.

### Security Levels Table

Specific tasks have been pre-assigned to each security level. The Security Levels Table presents the summary of differences in the three levels:

Operation	Administrator Level	Manager Level	Operator Level
<b>Security Applet</b> User Manager	YES	NO	NO
<b>Group Wizard</b> Create Groups	YES	YES, but only with assigned devices.	NO
Access Watch, viewing	YES	YES	YES
<b>Config Device</b> Download	YES	YES	YES
Database	YES	YES	YES

## Security

---

Operation	Administrator Level	Manager Level	Operator Level
Erase	YES	YES	NO
Write Memory	YES	YES	NO
Upload	YES	YES	NO
<b>Image Upload</b>			
Directory	YES	YES	YES
Download	YES	YES	YES
Erase	YES	YES	NO
Upload	YES	YES	NO
<b>Scheduler</b>	YES	YES	NO
<b>Reporting</b>	YES	YES	NO
<b>Path Finder</b>	YES	YES	YES
<b>Performance Applets</b>	YES	YES	YES
<b>Alarm Monitor</b>	YES	YES	YES
<b>Threshold Manager</b>	YES	YES	NO

## Logging in

The following user level details apply:

- **Administrator**

Upon first using NavisAccess after installation, the default login User Name is “Admin”. The default password is also “Admin”. **Both User Name and Password are case sensitive.**

**SECURITY NOTE:** The Administrator should change the defaults to secure the workstation.

- **Manager**

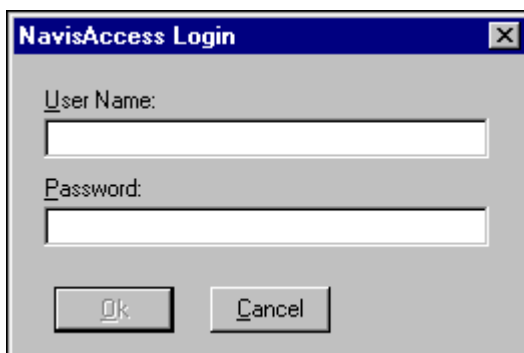
Specific responsibilities are assigned. The device(s)/or group(s) under a Manager's domain have been assigned by the Administrator.

- **Operator**

Specific responsibilities are assigned. The device(s)/or group(s) under an Operator's domain have been assigned by the Administrator.

### To Log in to NavisAccess:

1. From the NavisAccess main menu bar, select **Security > Login**. The Login dialog box opens:

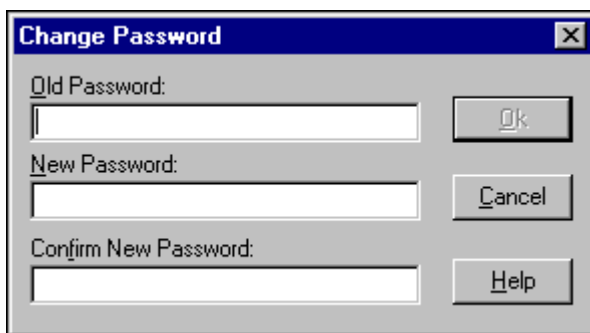


2. Enter a User Name and Password. Any level User can log in over any other User. A login can also be done by starting/restarting the program.
3. Click [Ok] to log in.

### Changing passwords

**To change a password:**

1. From the NavisAccess main menu bar, select **Security > Change Password**. The Change Password dialog box opens:

A screenshot of the 'Change Password' dialog box. The dialog has a title bar with the text 'Change Password' and a close button (X). Inside the dialog, there are three text input fields labeled 'Old Password:', 'New Password:', and 'Confirm New Password:'. To the right of the 'Old Password' field is an 'Ok' button. To the right of the 'New Password' field is a 'Cancel' button. To the right of the 'Confirm New Password' field is a 'Help' button.

2. Enter your Old Password as indicated.
3. Enter and Confirm a new password, as indicated.
4. Click OK.

**NOTE:** Any level user can access the Change Password dialog box when logged in. All users are allowed to change their own password. Only the Administrator can change the default Password “Admin” to secure the workstation initially.

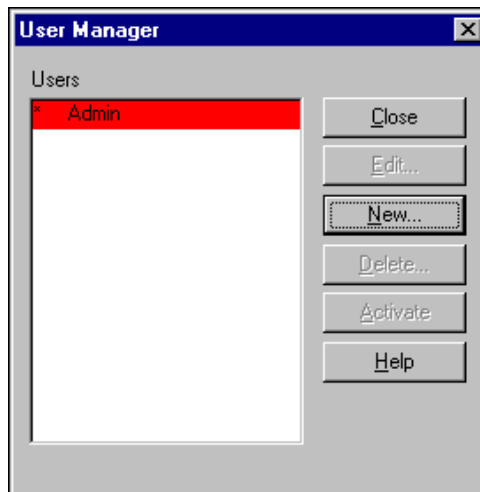
### Adding and deleting users, assigning rights

Users are added, deleted, activated and deactivated through the User Manager.

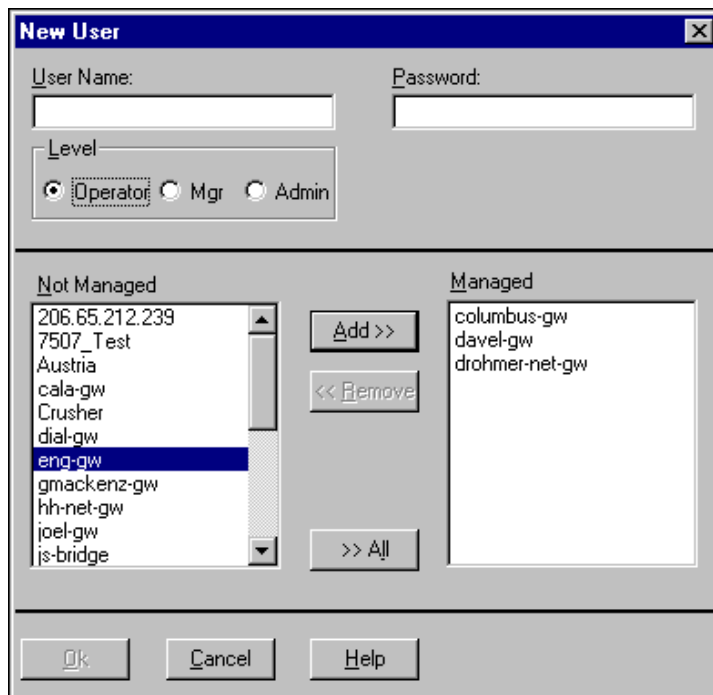
**To add a new user:**

1. From the NavisAccess main menu bar select **Security > Manager**.

**SECURITY NOTE:** The User Manager screen is only available to an Administrator.



2. Click the [New] button to open the New User dialog.



3. Make the necessary field selections.

### User Name

Enter the desired User Name. Remember that it is case sensitive. The User Name can be up to 30 characters in length.

### Password

Enter the desired Password. Remember that it is case sensitive. The Password can be up to 30 characters in length.

### Level

Select the level of security for the User: Operator, Manager or Administrator. See "Security: Overview" (page 57) for details on rights available to each level.

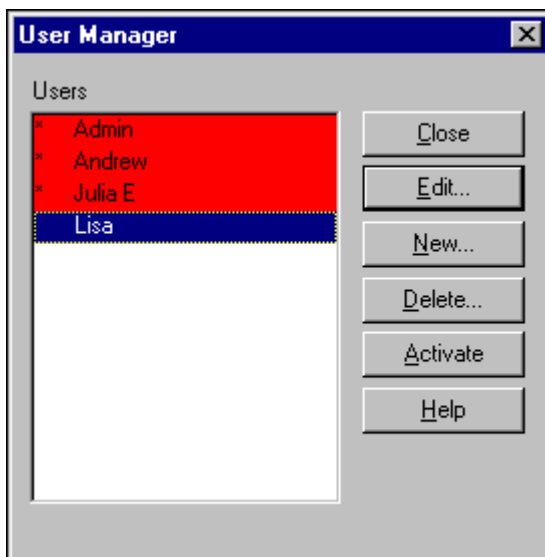
### Management Lists

Used to assign devices for a Manager-level or Operator-level user. To assign a device to a user, highlight a device in the Not Managed window (left pane) and press the [Add] button to place it in the Managed list.

4. Click [OK] to create the new user or [Cancel] to abort.

### To activate or deactivate users:

1. From the NavisAccess main menu bar select **Security > User Manager**.



Any active user is preceded with an asterisk and presented on a red

background. Without activation, the user can not login.

2. To activate a user (e.g. “Lisa”), highlight the user and press the [Activate] button.

Highlight an active user and the [Activate] button becomes a [Deactivate] button. Press the [Deactivate] button to deactivate the user.

### To delete a user:

1. From the NavisAccess main menu bar select **Security > User Manager**.
2. Highlight a user and click the [Delete] button.

**SECURITY NOTE:** Any User can be deleted, with the exception of the last Administrator level user in the system. For practical reasons, one Administrator must be left in the system to insure access to the NavisAccess program.

## Logging out

### To logout from NavisAccess:

1. From the NavisAccess main menu bar, select **Security > Logout**. A message box asks you to confirm the logout decision.
2. Click [Yes] to log out.



## The Group Wizard: Overview

### **Menu Bar: File > Group Wizard**

The Group Wizard is the central window of NavisAccess, providing a view of all network devices and a launching point for many product functions. Group Wizard functionality includes:

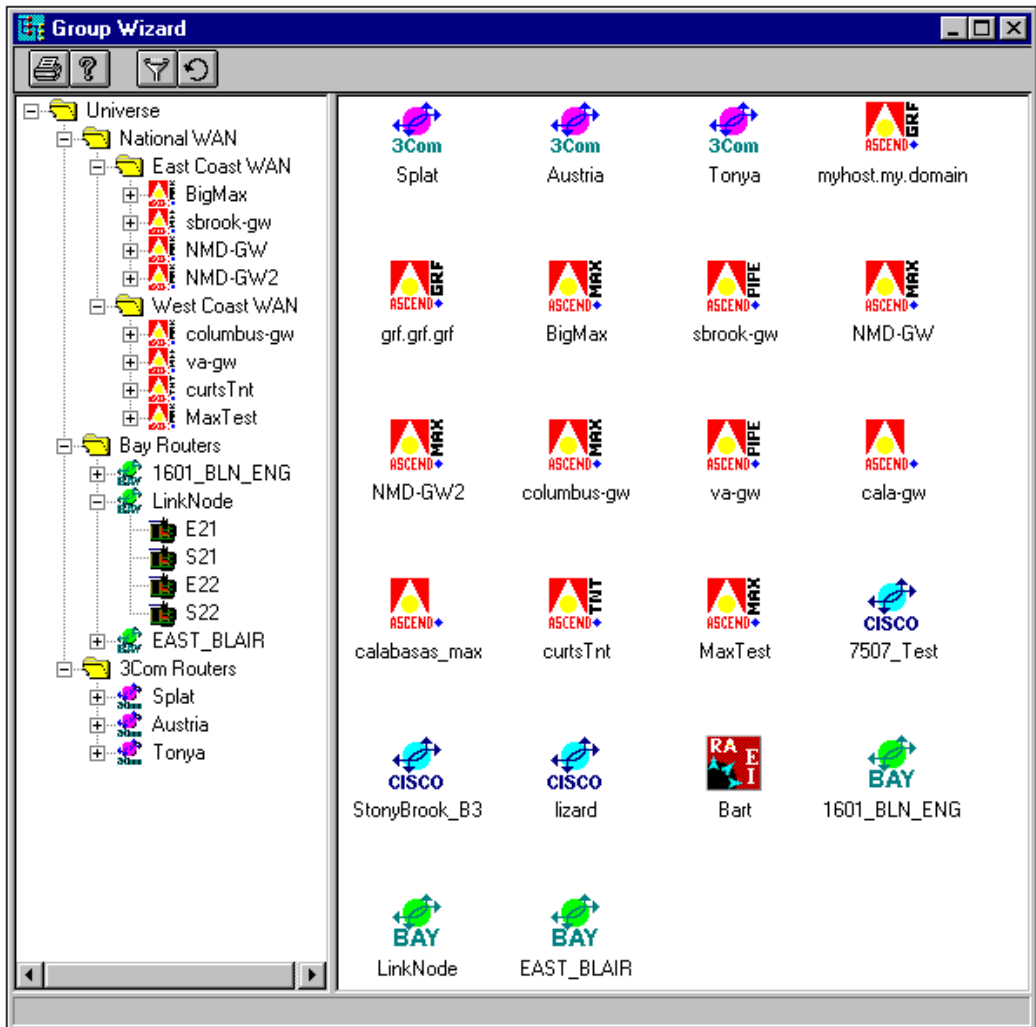
- Displaying all discovered devices, with filtering and finding options available
- Combining devices into logical groups
- Opening the Boxmap of devices
- Launching device-specific applications
- Launching the Access Watch application for remote access statistics

By default, the Group Wizard screen is displayed in the program window when NavisAccess is started. To display the window manually, select **File > Group Wizard**. If you do not want Group Wizard to appear when NavisAccess is started, you can change the startup option through the NavisAccess AutoStart Configuration window.

### **The Group Wizard window**

The Group Wizard is divided into two panes. The right-side displays all devices found by the discovery process or added manually to the NavisAccess database. Devices are identified by manufacturer-specific icons, with device-specific icons for Ascend equipment.

## Group Wizard



Several display options are available for arranging or viewing the icons.

### To arrange the window icons:

1. Right-click on a blank area in the right-window and select **Arrange Icons > option.**

Option choices are:

#### **By Name**

Organizes icons alphabetically based on device names.

#### **By Manufacturer**

Organizes icons based on device manufacturer.

#### **By Address**

Organizes icons in numerical order based on IP address.

### To change the view of the icons:

1. Right-click on a blank area in the window and select **View > option.**

Option choices, which are similar to Windows Explorer options, are:

#### **Large icons**

Displays large image of device icons.

#### **Small icons**

Displays small image of device icons in rows going across the window.

#### **List**

Displays small image of device icons in columns going down the window.



#### **Details**

Displays small icons with additional device information: device IP address, device manufacturer and contact name for the device (taken from the sysContact entry in the device MIB).

The left-pane of the Group Wizard displays the device group tree. The top level group, labeled "Universe," is always present and cannot be moved or renamed. New device groups can be created and devices added by simply dragging-and-dropping devices from the right-pane. See "Creating Device Groups" on page 71 for details.

### Other buttons

In addition to the global toolbar buttons, the Group Wizard has two specialized buttons on the right hand side of the toolbar.

Button	Description
	<b>[Filter Devices] button.</b> Opens the Filter Settings dialog box to set filtering parameters for what kinds of objects are displayed.
	<b>[Rescan Devices from Database] button.</b> Rescans the database and updates device information.

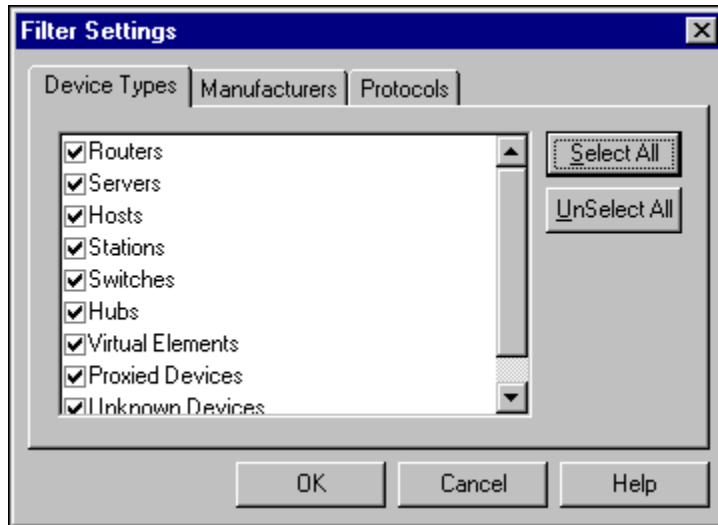
### Filtering and finding devices in Group Wizard

Because the Group Wizard can become populated with a very large number of devices, tools are provided to easily locate the devices you are looking for. There are two ways to do this:

- Device filtering, which lets you configure the Group Wizard to show only the devices you want to see, based on device type, manufacturer, protocol and faults.
- Device searching, a quick way to locate a specific device.

#### Device Filtering

1. To activate device filtering, click the [Filtering Devices] button to open the Filter Settings window.



2. Select filter settings based on the following categories:

**Device Types**

Only the types of devices selected will appear in Group Wizard.

**Manufacturers**

Only devices made by the selected manufacturers will be displayed.

**Protocols**

Only devices running the specified protocols will be displayed.

By default, all categories are selected. Selections may be mixed in any way.

3. Click OK and the Group Wizard will redisplay showing devices that match the selected categories.

**Device Searching**

The Group Wizard window can be searched by simply clicking in the left-pane and typing the name of the device you are looking for. The window will show the device that corresponds to what you are typing. Searching is accumulative, that is, as you type the search will correspond to the each new letter. For example, when you type "A" it will go to the first device beginning with "A." If you continue and type "N," it will go to the first device named "AN..." and so on.

## Group Wizard

---

To search for an IP address, set the window to Detail View.

### Object Status

The device's icon in the Group Wizard window provides information about the current state of the device to the user. See "Visual Indicators for Discovery" on page 48 for details.

## Device grouping: overview

The Group Wizard allows you to combine devices into logical groups. This is a uniquely powerful ability of NavisAccess. Because each device group functions as a separate entity, there is nearly unlimited grouping flexibility: the same device can be included in multiple groups; sub-groups can be created within groups, and the same sub-group can be used within more than one group; groups and sub-groups can be copied or moved easily.

Among the advantages of device grouping are:

- Devices can be grouped based on business or network needs.
- Large networks are far more easily managed by consolidating multiple devices into groups.
- Through use of the Access Watch application, remote access devices can be grouped to report aggregate statistics.
- Schedules can be create to gather historical utilization data for groups of devices.
- Individual interface selection allows you to create and monitor groups based on connection type (PRI, BRI, T1, etc.).

## Ideas for creating groups

While every network will have its individual needs, here are some possible kinds of groups you may wish to create. Remember that with unlimited grouping available you can create as many kinds of groups as you need.

- **Business unit groups:** group devices according to the business units they serve.
- **Geographic groups:** group devices based on office location, regions, states, nations, etc. Remote home office users can also be included.

- **POP groups:** create groups to monitor each Point of Presence in the network.
- **Device type groups:** group devices according to type, such as a MAX group, a Pipeline group, etc. This may be useful on a temporary basis for performance testing and capacity planning.
- **Interface/connection type groups:** create groups of particular interface/connection types, to monitor a specific kind of service, such as T1, BRI, etc.
- **Testing groups:** group devices that will be used for testing purposes. This allows you to separate test data from regular network data.

### Creating device groups

There are several aspects to consider when creating device groups.

- Creating a basic device group.
- Creating a sub-group within a group.
- Selecting specific device interfaces.
- Copying/editing/deleting groups.

#### Device Group Tutorial

In the instructions that follow, we will illustrate Group Wizard functionality by creating sample groups that are used throughout all the instructions. Therefore, understanding a set of instructions may depend on information presented in the previous instructions. For tutorial purposes, you may want to create groups as outlined below.

Before trying this tutorial, you should have discovered several devices.

#### To create a basic device group:

1. In the left-pane of the Group Wizard window, highlight the "Universe" folder, right-click the mouse and choose **New Group**. A New Group folder will appear with a default name of "New Group." You can also press the [Insert] key to create a new folder.
2. Type a name for the group and press [Enter]. Group names should be descriptive of the group's function or purpose. Keep in mind that if you will be creating sub-groups, you may wish to name the top level group in

## Group Wizard

---

an appropriate manner. For illustrative purposes, we will call our group "Group 1."

- 3 Add a device to Group 1 by clicking and holding a device in the right-pane. Drag the device and drop it onto the Group 1 folder. Multiple devices can be added in one operation by using standard Windows [Ctrl] and [Shift] highlighting techniques.

After dragging the device icon, it will appear under the Group 1 folder. It will *not* be removed from the right-pane, and may be reused in other groups, or even within sub-groups of Group 1.

4. Continue to add devices until you have completed the desired group.

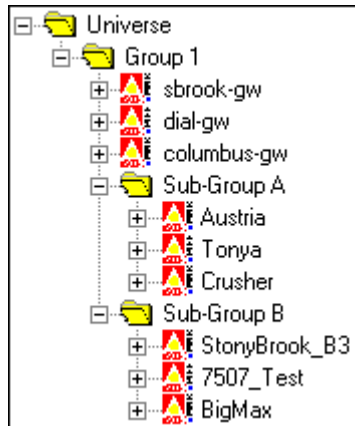
Here is an example of what Group 1 would look like with three Ascend devices added:



### To create a sub-group within a group

1. Right-click on the Group 1 folder and choose **New Group**, or press the [Insert] key. A sub-group folder will appear with the default name of "New Group."
2. Type a name for the sub-group and press [Enter]. We will call our group "Sub-Group A".
3. Add devices to Sub-Group A using the same drag-and-drop procedure as explained above. Note that you may include devices from Group 1 in Sub-Group A if you wish.
4. Create a second Sub-Group called "Sub-Group B".

Here is an example of what Group 1 would look like with sub-groups A and B added.



### Selecting specific device interfaces

NavisAccess allows you to monitor only selected interfaces on a device. To do this, NavisAccess uses a process of elimination approach. After adding a device to a group, you delete all the interfaces you do *not* want to monitor, leaving only those that you do wish to monitor.

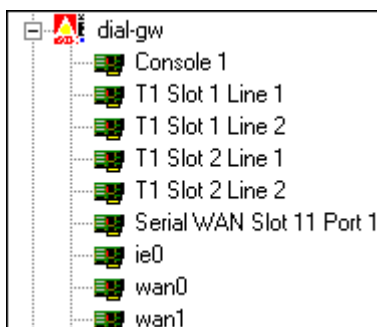
For illustrative purposes, we will create a new group and select only the T1 interfaces.

1. Right-click on the Universe folder and choose **New Group**.
2. Type the name "T1 Group" and press [Enter].
3. Drag and drop the devices you wish to include in the group.
4. Click the plus sign "+" next to the first device in the group. This will open a list of labeled interface icons. What you see will vary with each device. Typical names you will see include: Console, Ethernet, Wan, Serial, BRI, T1 and so on, each with identifying numbers after it.

Here is a portion of a device icon with interfaces:

## Group Wizard

---

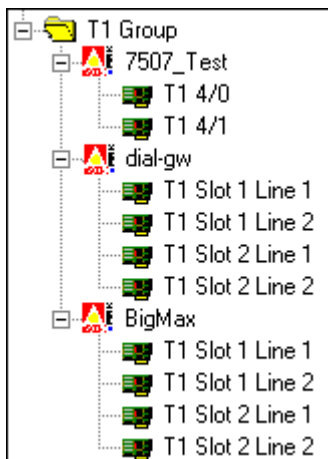


5. To leave only the T1 interfaces, highlight all the interfaces that are *not* T1 interfaces. Standard [Ctrl] and [Shift] selection options apply.
6. After highlighting all non-T1 interfaces, right-click and choose **Remove Items** (or press the [Delete] key). A warning box will appear. Answer "yes" to delete the interfaces.

The interfaces will be deleted, leaving only the T1 interfaces.

7. Repeat this procedure for all devices in the T1 group.

Here is an example of what the T1 Group might look like:



**NOTE:** There are two things to remember when selecting interfaces. First, interface selections will affect only the group you are using. If a device is included in other groups, its interfaces will not be affected. Second, because each group functions as a separate entity, you can create

as many interface-specific groups per device as you wish. This allows you to create separate groups to monitor each specific type of traffic.

### Linking, copying, moving, editing and deleting groups

Groups can be linked, copied, moved, editing and deleted very easily in the Group Wizard. Note the following important distinctions:

**Linking** a group creates an identical group in a new location. The two groups will be permanently linked: i.e., changes made to one group will occur in *all* groups. For example, if you link Group A in three other places (for a total of four groups), when a device is removed from *any* Group A, *all four* Group A groups will have the device deleted.

**Copying** a group creates an identical group in a new location, with the default name "Copy of *Group-Name*". Copied groups are *not linked*: i.e., changes made to one group will have *no effect* on copied groups. Copied groups function independently and can be renamed, reorganized, etc., with no bearing on the original group.

**Moving** a group will delete the group from its original location and place it in a new location.

#### To link a group or device:

1. Right-click and hold the group or device icon in the group tree structure. Drag and drop into the new location.
2. A pop-up menu appears. Select **Link**.

Note the following:

- Any actions performed on one linked group (e.g., deleting devices) will take place in all the groups linked to the source group.
- Linking will create a new version of a group or device, it will *not* move it.
- You cannot drop a device icon onto another device icon.
- Dragging and dropping an upper level group will copy all the subgroups located under the group.

**NOTE:** If you *left-click* on a group and drag-and-drop it, the newly created group will be **linked** with the source group.

## Group Wizard

---

### To copy a group or device:

1. Right-click and hold the group or device icon in the group tree structure. Drag and drop into the new location.
2. A pop-up menu appears. Select **Copy**.

Note the following:

- Copying will create a new version of a group or device, it will *not* move it.
- A copied group will be named "Copy of *Group-Name*," and may be renamed as needed.
- You cannot drop a device icon onto another device icon.
- Dragging and dropping an upper level group will copy all the subgroups located under the group.

### To move a group or device:

1. Right-click on the group or device icon in the group tree structure. Drag and drop into the new location.
2. A pop-up menu will appear. Select **Move**.

Note the following:

- Moving a group or device will delete it from its original location.
- Moving Group B to Group A will carry all devices from Group B and create a Group B sub-group within A.
- You cannot move a device icon onto another device icon.
- Moving an upper level group will move all the subgroups located under the group.

### To edit a group name:

1. To change the name of a group, right-click on it and select **Rename Group**. Enter a new name for the group and press [Enter].
2. The name change will be reflected in any linked groups.

**NOTE:** you cannot change a device name in the Group Wizard. Device names are configured on the device itself though the sysName variable.

### **To delete a group:**

1. Right-click on the group and select **Delete Group**. Or, highlight the group and press the [Delete] button.

### **To delete items within a group:**

1. Right-click on a device or devices in a group and choose **Remove Items**. Deleting devices in a group will also delete them in any linked groups.

## Group Wizard

---

## Access Watch: Remote Access at a Glance

5

### Access Watch: Overview

Access Watch is the focal point for remote-access related information. All vital access statistics are centrally located on one easy-to-read screen. Among the capabilities of Access Watch are:

- Aggregate access statistics reported for groups of devices. Statistics include currently running sessions, total calls, dropped calls, call duration, modem and channel utilization.
- Configurable alert thresholds with alerts reported to screen.
- One-click drill-down from group level view to device level view.
- Drill-down from top level statistics for more specific details.
- Ability to enable/disable/quiesce modems and channels
- Ability to disconnect specific calls/users
- Statistics are continually reported to the NavisAccess database, allowing for the creation of historical trending reports.

**NOTE:** Access Watch functionality is available only for Ascend remote-access devices (MAX, MAX TNT and Pipeline).

Access Watch is launched from already defined groups within the Group Wizard application, or from individual access device icons.

**USAGE NOTE:** For Access Watch to operate correctly, SNMP Call Logging must be enabled on all Pipeline, MAX and MAX TNT devices included in Access Watch groups. See "Special Considerations for Ascend Devices" on page 3 for details.

### Starting and using Access Watch

#### To launch Access Watch:

1. Right-click on a device group in the Group Wizard and select **Access Watch**.

**NOTE:** Only remote access devices (Pipeline, MAX, MAX TNT) will report data to Access Watch. Other devices, while they can be included in groups for other reasons, will not report data in Access Watch.

2. The top-level Access Watch window will open, and statistics will begin to be reported to the screen. Depending on the composition of the group, Access Watch may show individual device information (for a single-level group) or aggregate group data (for a multi-level group).

**NOTE:** Device-specific Access Watch windows can be launched from individual device icons. Right-click on the icon and select **Access Apps > Application**.

#### Using Access Watch

Access Watch utilizes a simple point-and-click drill-down mechanism. Double-clicking in specific window cells opens the next layer of information. The drill-down levels are as follows:

- |                             |   |
|-----------------------------|---|
| <b>1. GROUP LEVEL DATA</b>  | (aggregate call/utilization statistics)     |
| <b>2. DEVICE LEVEL DATA</b> | (single-device call/utilization statistics) |
| <b>3. DATA DETAILS</b>      | (breakdown of call/utilization statistics)  |

Because you can have groups within groups, there may be more than one layer of Level 1 information.

You can also access level 2 and 3 applications directly by right-clicking on a group in the Group Wizard and selecting the specific application.

#### Drill-down from groups to devices:

If you have created a group with subgroups, Access Watch will open showing group level statistics. The Group/Device Name column will show the group name. To view specific devices within that group, double-click the Group/Device Name cell to open a second Access Watch window that will show



the devices in the group.

If the subgroup itself is composed of other groups, the second window will show those groups. Continue to drill-down in the same fashion to reach the device level.

If a group has both devices and other groups, drill-down will show both the individual devices and the groups.

## Reading the Access Watch window: top level

The top level Access Watch window reports both aggregate data (for device groups) and individual device data, depending on what level of group is opened. Data is reported in real-time as a configurable moving average over three separate time intervals.

Access Watch <National WAN>							
							
Group/Device Name	Currently Running Sessions	Calls	Dropped Calls (#/%)	Completed Calls Ave. Duration # / D H:M:S	% Modem Utilization/ Availability	% Channel Utilization/ Availability	
East Coast WAN	27	60min 10	1 / 10%	45 / 0 00:18:33	35% / 100%	31% / 100%	
		15min 10	0 / 0%	23 / 0 00:12:03	36% / 100%	36% / 100%	
		5min 7	0 / 0%	5 / 0 00: 8:13	30% / 100%	37% / 100%	
West Coast WAN	13	60min 3	0 / 0%	45 / 0 00:12:33	31% / 100%	35% / 100%	
		15min 10	1 / 10%	23 / 0 00:18:03	36% / 100%	36% / 100%	
		5min 0	0 / 0%	5 / 0 00: 6:13	37% / 100%	30% / 100%	
Time	Device	Event Details					
10:17:36	columbus-gw	Modem Availability (0%) is below 95% minimum.					
10:17:36	shinjuku	Modem Availability (75%) is below 95% minimum.					

## Access Watch

The following information is displayed in the Access Watch window.

Column Heading	Description	Double-click Action
<b>Group/ Device Name</b>	Indicates the device or device group being reported on. Device groups report aggregate data (i.e., the combined data from all devices in the group).	If a device group is listed, double-clicking in the cell will open a device-level Access Watch screen that will break out the aggregate data into individual devices.
<b>Currently Running Sessions</b>	The total number of sessions currently active in the group or on the device (i.e., the number of users connected).	Double-clicking the cell will open the Active Sessions window, which reports session details such as current service, data rate, user name, WAN and modem slots and lines, etc. The Active Sessions window also allows you to disconnect a user.
<b>Calls</b>	The total number of calls ongoing for the logging period. NavisAccess uses a configurable moving average to present this data. For details, see "Calculating the Moving Average".	Double-clicking the Calls cell opens the Call Monitor window, which displays active call information, providing data on total active calls and a breakdown by call type (analog, digital, Frame Relay) for both inbound and outbound.
<b>Dropped Calls (#/%)</b>	<p>The total number of dropped calls for the monitoring period, and the percentage of dropped calls compared to total calls received for the period. For example, a reading of "8 / 4%" would indicate that 8 calls have been dropped, representing 4% of the total calls received.</p> <p>A dropped call is defined as a call that reported an abnormal disconnect.</p> <p><b>NOTE:</b> Please see the section "More about dropped calls" below for important details on Dropped Call statistics.</p>	None.

Column Heading	Description	Double-click Action
<b>Completed Calls, Ave Duration # D H:M:S</b>	<p>The number of completed calls and the average length of time for each call received in the monitoring period. Time data is shown in D H:M:S format. For example, a reading of "0 06:22:13" would indicate 0 days, 6 hours, 22 minutes, 13 seconds.</p> <p>Note that the number of completed calls <i>includes</i> dropped calls, because a dropped call disconnects <i>after</i> the call is made (and has registered as completed).</p>	None.
<b>% Modem Utilization / Availability</b>	The percentage of modems being utilized and the percentage available for use. A modem is considered not available for use if it is listed as disabled, dead or suspect.	Double-clicking the cell opens the Modem Pools window, which lists modems on a per device basis and displays statistics for available, suspect, disabled, dead and busy modems.
<b>% Channel Utilization / Availability</b>	The percentage of WAN lines in use, and the percentage available for use. Only configured lines are used in the calculations.	Double-clicking the cell opens the Wan Line Table window, which details specific channels and interfaces.
<b>Time, Device, Event Details</b>	The bottom pane of the window reports threshold errors on a per device basis. Threshold levels can be set for factors such as modem availability and utilization, change in active sessions, dropped calls, etc. See "Configuring Access Watch" (page 90) for details on setting threshold levels.	Does not apply.

## Access Watch

Column Heading	Description	Double-click Action
Status Bar	<p>The Status Bar along the bottom of the Access Watch window reports the following items:</p> <p><b>Running Since</b> - The time and date at which the window was first displayed. This indicates when calculations began. Note that any windows opened by drill-down from the top level window will show the time that the drill-down window was opened. However, calculations will have started at the time the first window was originally opened.</p> <p><b>Elapsed Time</b> - The time that has passed since the Access Watch window was opened.</p> <p><b>Calls Processed</b> - The total number of calls processed since the window was opened. This includes all devices at all drill-down levels.</p>	Does not apply.

### More about Dropped Calls

Please exercise caution when evaluating Dropped Call statistics. A dropped call is defined as a call that returns an abnormal disconnect. However, an abnormal disconnect does not necessarily indicate a problem condition. A large number of dropped calls may only be a reflection of the way in which users are hanging up.

In order to fully understand the reasons that calls are being dropped, it is necessary to look at the Disconnect Cause Codes and Progress Codes for the dropped calls. NavisAccess provides an Account Disconnect report that will list the Disconnect Cause and Progress Codes, the number of times each was received, and the percentage of each code in relation to the total codes received.

NavisAccess considers the following Disconnect Codes to be normal: that is, they will *not* report as a Disconnect in AccessWatch.

**Disconnect Code 11, with Progress Code 60**

**Disconnect Code 20, regardless of Progress Code**

**Disconnect Code 21, regardless of Progress Code**

**Disconnect Code 22, regardless of Progress Code**  
**Disconnect Code 24, regardless of Progress Code**  
**Disconnect Code 45, regardless of Progress Code**  
**Disconnect Code 100, regardless of Progress Code**  
**Disconnect Code 102, regardless of Progress Code**

If you are receiving a large number of dropped calls which you determine are *not* abnormal, please contact Ascend Communications technical support for assistance.

The following tables list both Disconnect Cause Codes and Progress Codes.

**NOTE:** These tables are continuously updated. Please consult your Ascend device documentation and release notes for the latest updates to the tables if you cannot find a number below.

**Disconnect Cause codes**

Disconnect Code	Explanation
0	No reason.
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.
3	The call has disconnected.
4	CLID authentication has failed.
These codes can appear if a disconnect occurs during the initial modem connection.	
10	The modem never detected DCD.
11	The modem detected DCD, but became inactive.
12	the result codes could not be parsed.
These codes are related to immediate Telnet and raw TCP disconnects during a terminal server session	

## Access Watch

Disconnect Code	Explanation
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process ended because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process ended because the user typed Ctrl-C.
28	The terminal server session has ended.
29	The user closed the virtual connection.
30	The virtual connection has ended.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The user has insufficient resources for the terminal server session.
<b>These codes concern PPP connections.</b>	
40	PPP LCP negotiation timed out while waiting for a response from a peer.
41	There was a failure to converge on PPP LCP negotiations.
42	PPP PAP authentication failed.
43	PPP CHAP authentication failed.
44	Authentication failed from the remote server.
45	The peer sent a PPP Terminate Request.

Disconnect Code	Explanation
46	LCP got a close request from the upper layer while LCP was in an open state.
47	LCP closed because no NCPs were open.
48	LCP closed because it could not determine to which MP bundle it should add the user.
49	LCP closed because it could not add any more channels to an MP session.
<b>These codes are related to immediate Telnet and raw TCP disconnects, and contain more specific information than the Telnet and TCP codes listed earlier in this table.</b>	
50	The Raw TCP or Telnet internal session tables are full.
51	Internal resources are full.
52	The IP address for the Telnet host is invalid.
53	The hostname could not be resolved.
54	A bad or missing port number detected.
<b>The TCP stack can return these disconnect codes during an immediate Telnet or raw TCP session.</b>	
60	The host reset the TCP connection.
61	The host refused the TCP connection.
62	The TCP connection timed out.
63	A foreign host closed the TCP connection.
64	The TCP network was unreachable.
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.

## Access Watch

Disconnect Code	Explanation
<b>These are additional disconnect codes.</b>	
<b>100</b>	The session timed out because there was no activity on a PPP link.
<b>101</b>	The session failed for security reasons.
<b>102</b>	The session ended for callback.
<b>120</b>	One end refused the call because the protocol was disabled or unsupported.
<b>150</b>	RADIUS requested the disconnect.
<b>160</b>	The allowed retries for V.110 synchronization have been exceeded.
<b>170</b>	PPP authentication has timed out.
<b>180</b>	The call disconnected as the result of a local hangup.
<b>185</b>	The call disconnected because the remote end hung up.
<b>190</b>	The call disconnected because the T1 line that carried it was quiesced.
<b>195</b>	The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter.

## Progress Codes

Progress Code	Explanation
<b>0</b>	No progress.
<b>1</b>	Not applicable.
<b>2</b>	The progress of the call is unknown.
<b>10</b>	The call is up.
<b>30</b>	The modem is up.
<b>31</b>	The modem is waiting for DCD.

Progress Code	Explanation
32	The modem is waiting for result codes.
40	The terminal server session has started up.
41	Establishing the TCP connection.
42	Establishing the immediate Telnet connection.
43	The user has established a raw TCP session with the host. This code does not imply that the user has logged into the host.
44	The user has established an immediate Telnet connection with the host. This code does not imply that the user has logged into the host.
45	The user is establishing an Rlogin session.
46	The user has established an Rlogin session with the host. This code does not imply that the user has logged into the host.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
69	LCP is in the Initial state.
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.

## Access Watch

---

Progress Code	Explanation
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.
80	IPXNCP is in the Open state.
90	V.110 is up.
91	V.110 is in the Open state.
92	V.110 is in the Carrier state.
93	V.110 is in the Reset state.
94	V.110 is in the Closed state.

## Configuring Access Watch

**Menu Bar:** Config > System Options

The Access Watch tab allows you to customize the moving average, default secret and threshold limits used by the Access Watch application.

**NavisAccess Configuration**

Boxmap | Alarm Monitor | INTERNET | WebReport  
CommStr | SNMP | Color | Applet | AutoStart | Access Watch

Moving Average Durations (hh:mm)

Interval 1: 00:05 × 3 = Interval 2: 00:15 × 4 = Interval 3: 01:00

Default Secret: ascend

Threshold Limits (warn user if:)

Percent change in Active Sessions (>): 5	Percent Modem Utilization (>): 95
Percent change in Calls (>): 5	Percent Modem Availability (<): 95
Percent Dropped Calls (>): 3	Percent Channel Utilization (>): 95
Average Call Duration (<): 00:14	Percent Channel Availability (<): 95

OK Cancel Apply Help

### Moving Average Durations

Sets the three Moving Average intervals. Intervals are defined as multiples of the previous interval and are in HH:MM format. For example, to set Interval 2 at 15 minutes, you would set Interval 1 at 00:05 minutes with a multiplier of 3 (5 x 3 = 15). The default intervals are 5 minutes, 15 minutes and 60 minutes.

For details on how moving averages are calculated, see "Calculating the Moving Average" on page 93.

### Default Secret

The keyword which enables NavisAccess to receive data from an access device. This field sets a default value for use on all devices. Individual devices can

have unique secrets entered through the Configuration screen.

The secret entered from within NavisAccess, either individually or through the default setting, *must be the same* as that entered on the device itself. See "Enabling Call Logging on the MAX and Pipeline" (page 6) and "Enabling Call Logging on the MAX TNT" (page 14) for details.

### Threshold Limits

The levels used for determining Access Watch warning messages. Whenever a call or utilization category passes a threshold limit, a message is generated and sent to the Access Watch window.

Configurable threshold levels and their defaults are:

- **Percent change in Active Sessions Greater Than (>) 5**  
Warning issued if Active Sessions changes (up or down) by more than 5 percent.
- **Percent change in Calls Greater Than (>) 5**  
Warning issued if number of calls changes (up or down) by more than 5 percent
- **Percent Dropped Calls Greater Than (>) 3**  
Warning issued if the percentage of dropped calls rises above 3 percent of total calls.
- **Average Call Duration Greater Than (>) 14 minutes**  
Warning issued if the average call time rises above 14 minutes per call.
- **Percent Modem Utilization Greater Than (>) 95**  
Warning issued if the utilization level of modems rises above 95 percent.
- **Percent Modem Availability Less Than (<) 95**  
Warning issued if the number of available modems decreases to less than 95 percent of the total number of modems.
- **Percent Channel Utilization Greater Than (>) 95**  
Warning issued if the utilization level of channels rises above 95 percent.
- **Percent Channel Availability Less Than (<) 95**  
Warning issued if the number of available channels decreases to less than 95 percent of the total number of channels.

Note that values shown above are defaults, and may be configured to suit the needs of your network.

## Calculating the moving average

NavisAccess calculates moving averages through the use of three additive queues. This is best explained by looking at an example using the default values.

Each queue corresponds to the interval settings on the Access Watch Configuration screen. By default, the values are:

- Interval 1: 5 minutes
- Interval 2: 15 minutes
- Interval 3: 60 minutes

Intervals are defined as multiples of the previous interval, in HH:MM format. For example, to set Interval 2 at 15 minutes, Interval 1 is set at 00:05 minutes with a multiplier of 3 ( $5 \times 3 = 15$ ).

When Access Watch is first started, data is delivered based both on the polling interval (for SNMP data, each device is polled once per minimum interval) and as calls are received (for Call Logging data).

For the first 5 minutes, each interval will display the same statistics. When five minutes passes, Call Logging data in Interval 1 is reset to a value of zero. Intervals 2 and 3, however, continue to accumulate data.

When a second 5 minutes passes, Interval 1 again returns to zero, but the next five minutes of data continues to accumulate in Intervals 2 and 3.

Another 5 minutes passes, and 5 more minutes of data accumulate in Intervals 2 and 3, and Interval 1 is again zeroed. However, when the fourth 5 minute interval begins, Interval 2 (a 15 minute interval) drops the first 5 minutes of collected data in order to accumulate the upcoming 5 minutes of data. In other words, at the 15 minute mark, Interval 2 will drop back to showing the last 10 minutes of data (displayed numbers will correspondingly reduce), and begin accumulating new data for 5 more minutes going forward. Generically speaking, Interval 2 will drop “Interval 1” worth of data every time Interval 1 passes.

A similar process takes place for Interval 3 after 60 minutes passes. In that case, Interval 3 drops back 15 minutes (the size of Interval 2) and begins to accumulate from 45 minutes to 60 minutes.

The moving average process ensures that you are always seeing an average of the most recently available data.

Access Watch drill-down levels

Access Watch: the Active Sessions window

The Active Sessions window provides detailed session information for access devices being monitored by the Access Watch application. It also allows you to disconnect any listed call.

Active Sessions <slc-max>								
Device Name	Current Service	Data Rate	User Name	Wan (sl/ln/ts)	Modem (sl/unit)	Login Duration (H:M:S)	IP Address	Subnet Mask
slc-max	mpp	64000	Homer	1/2/20	0/0	0 17:03:36	204.253.164.217	255.255.255.248
slc-max	mpp	56000	TomsPipe75	1/2/23	0/0	0 17:03:18	0.0.0.0	255.255.255.255
slc-max	mpp	64000	Homer	1/2/2	0/0	0 17:02:44	204.253.164.217	255.255.255.248
slc-max	mpp	64000	Homer	1/2/3	0/0	0 17:02:37	204.253.164.217	255.255.255.248
slc-max	ppp	14400	kvigor	1/2/11	4/5	0 16:42:12	204.253.164.60	255.255.255.255
slc-max	mpp	56000	p50	1/2/14	0/0	0 16:33:18	204.253.164.253	255.255.255.255
slc-max	mpp	56000	p50	1/2/15	0/0	0 16:33:10	204.253.164.253	255.255.255.255
slc-max	mpp	64000	ConniesPipe75	1/2/8	0/0	0 13:50:31	0.0.0.0	255.255.255.255
slc-max	mpp	64000	CraigsPipe75	1/2/4	0/0	0 00:54:52	204.253.164.209	255.255.255.248

The following information is displayed in the Active Sessions window:

Column Heading	Description
Device Name	The name of the device.
Current Service	The type of service the session is using, such as PPP, MPP or Frame Relay.
Data Rate	The connection speed of the session, in Kbps.
User Name	The user name that has logged in for the session.
WAN (sl/ln/ts)	The WAN slot, line and channel numbers for the session.
Modem (sl/unit)	The Modem slot and unit numbers for the session.
Login Duration	The length of time the session has been running, in Days:Hours:Minutes:Seconds format.
IP Address	The IP address assigned to the session.
IP Mask	The IP mask used by the session.

All fields are sortable by clicking on the column heading. The Active Sessions window also uses standard toolbar buttons.

### Disconnecting a caller

To disconnect a caller in the Active Sessions window, right-click on the caller in question to bring up the Disconnect *User-Name* menu. User-Name will be the same as that listed in the Active Sessions window. After selecting the option, you will receive a warning message asking if you are sure you wish to disconnect the caller. Choosing [Yes] will disconnect the caller.

### Launching the Active Sessions window

Active Sessions is launched by double-clicking the Currently Running Sessions cell in the Access Watch application. It can also be launched by right-clicking on a device or group in the Group Wizard and choosing Active Sessions.

## Access Watch: the Call Monitor window

The Call Monitor window provides call details for access devices being monitored by the Access Watch application.

Group/Device Name	Total Active Calls	Active Calls Analog	Active Calls Digital	Active Calls Frame Relay
<b>SF Group</b>	<b>High: 5 Cur: 2</b>	<b>In : 0 Out: 0</b>	<b>In : 0 Out: 1</b>	<b>In : 0 Out: 1</b>
shinjuku	High: 5 Cur: 2	In : 0 Out: 0	In : 0 Out: 1	In : 0 Out: 1
Jimi	High: 1 Cur: 0	In : 0 Out: 0	In : 0 Out: 0	In : 0 Out: 0
mlw-gw	High: 0 Cur: 0	In : 0 Out: 0	In : 0 Out: 0	In : 0 Out: 0
Homer	High: 0 Cur: 0	In : 0 Out: 0	In : 0 Out: 0	In : 0 Out: 0

The following information is displayed in the Call Monitor window:

Column Heading	Description
Group/Device Name	Indicates the device or device group being reported on. Device groups report aggregate data (i.e. the combined data from all devices in the group) and are displayed in bold face type.

## Access Watch

Column Heading	Description
	You cannot drill-down into a group directly through the Call Monitor window. You must drill-down through the Access Watch window and then open the Call Monitor at the group level.
<b>Total Active Calls</b>	The total number of calls currently active on the device or in the group (the Cur figure). The High figure indicates the highest total active calls reported at any time during the monitoring period.
<b>Active Calls Analog</b>	Lists the number of currently active analog calls, both incoming and outgoing, on the device or in the group.
<b>Active Calls Digital</b>	Lists the number of currently active digital calls, both incoming and outgoing, on the device or in the group.
<b>Active Calls Frame Relay</b>	Lists the number of currently active Frame Relay calls, both incoming and outgoing, on the device or in the group.

All fields are sortable by clicking on the column heading. The Call Monitor window also uses standard toolbar buttons.






### Launching the Call Monitor window






Call Monitor is launched by double-clicking the Calls cell in the Access Watch application. It can also be launched by right-clicking on a device or group in the Group Wizard and choosing **Call Monitor**.






## Access Watch: the Modem Pools window

The Modem Pools window provides modem utilization details for access devices being monitored by the Access Watch application.

The screens below show Modem Utilization as aggregate data for a group (top), as individual devices within a group (middle) and for a single device (bottom).

Modem Pools <National WAN>						
    						
Group/Device Name	Available	Suspect	Disabled	Dead	Busy	
East Coast WAN	72	0	0	0	0	
West Coast WAN	12	0	0	0	0	
<b>Total</b>	<b>84</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	

Modem Pools <East Coast WAN>						
    						
Group/Device Name	Available	Suspect	Disabled	Dead	Busy	
BigMax	24	0	0	0	0	
sbrook-gw	0	0	0	0	0	
NMD-GW	24	0	0	0	0	
NMD-GW2	24	0	0	0	0	
<b>Total</b>	<b>72</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	

Modem Pools <dial-gw>		
    		
Modem Pools	Number Of Modems	
Available Modems	11	
Suspect Modems	0	
Disabled Modems	0	
Dead Modems	4	
Busy Modems	1	

## Access Watch

The following information is displayed in the Modem Pools window:

Column Heading	Description	Double-click Action
<b>Group/Device</b>	The name of the group or device being reported on. This field is not applicable to the single-device view.	Double-clicking on a group entry will open a window showing a breakdown by device.
<b>Available</b>	The total number of available modems for the group or device. An available modem is defined as a modem that is functioning properly and is waiting for a call to be made or received.	Double-clicking in the Available cells opens the Available Modem Pool window, showing available modem details: slot number, port number, used count, and bad count.
<b>Suspect</b>	The total number of suspect modems for the group or device. A suspect modem is defined as a modem that has dropped a set number of calls.	Double-clicking in the Suspect cells opens the Suspect Modem Pool window, showing suspect modem details: slot number, port number, used count, and bad count.
<b>Disabled</b>	The total number of disabled modems for the group or device. A disabled modem is defined as one that has been administratively disabled by an operator.	Double-clicking in the Disabled cells opens the Disabled Modem Pool window, showing disabled modem details: slot number, port number, used count, and bad count.
<b>Dead</b>	The total number of dead modems for the group or device. A dead modem is defined as a modem that has failed a power-on self-test, or that is not responding at all electronically.	Double-clicking in the Dead cells opens the Dead Modem Pool window, showing dead modem details: slot number, port number, used count, and bad count.
<b>Busy</b>	The total number of busy modems for the group or device. A busy modem is defined as a modem that is making or receiving a call.	Double-clicking in the Busy cells opens the Busy Modem Pool window, showing busy modem details: slot number, port number, used count, and bad count.

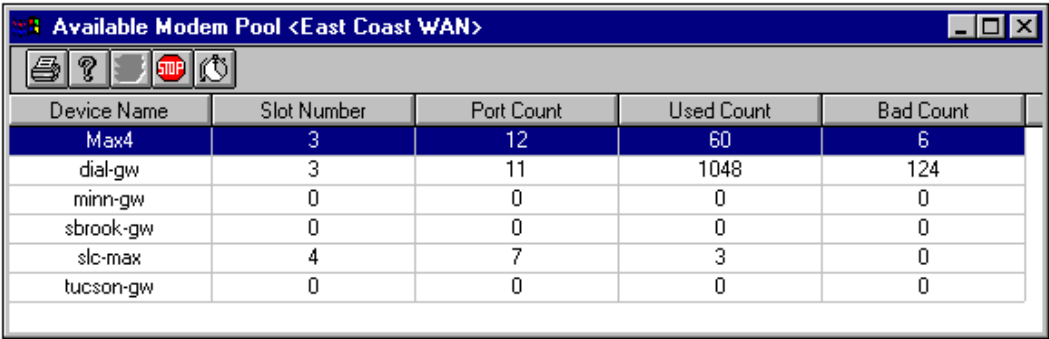
All fields are sortable by clicking on the column heading. The Modem Pools window also uses standard toolbar buttons.

**Launching the Modem Pools window**

Modem Pools is launched by double-clicking the % Modem Utilization/Availability cell in the Access Watch application. It can also be launched by right-clicking on a device or group in the Group Wizard and choosing **Modem Pools**.

**Access Watch: the Modem Pool window**

The Modem Pool window breaks down modem details for Available, Suspect, Disabled, Dead and Busy modems. Each category is reported in a separate window with a corresponding title bar. The screen below shows the Available Modem Pool window.



Device Name	Slot Number	Port Count	Used Count	Bad Count
Max4	3	12	60	6
dial-gw	3	11	1048	124
minn-gw	0	0	0	0
sbrook-gw	0	0	0	0
slc-max	4	7	3	0
tucson-gw	0	0	0	0

The following information is displayed in the Modem Pool window:

Column Heading	Description
Device Name	The name of the device being reported on.
Slot Number	The slot number for the modem.
Port Number	The port number on the modem.
Used Count	The number of times modems in the modem pool were used.
Bad Count	The number of times modems in the modem pool failed.

All fields are sortable by clicking on the column heading. The Modem

## Access Watch

---

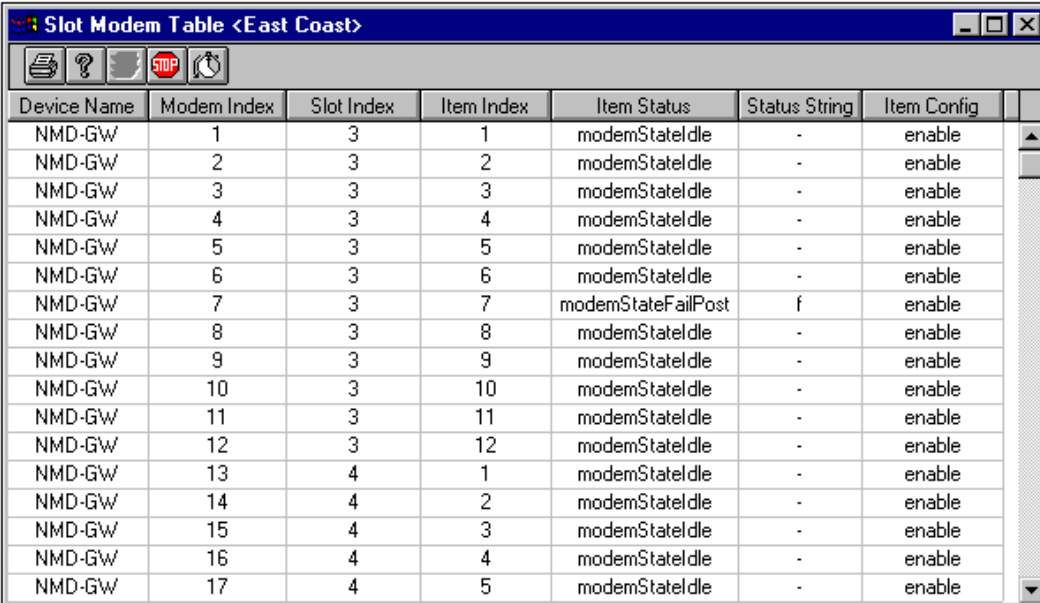
Utilization window also uses standard toolbar buttons.

### Launching the Modem Pool windows

The Modem Pool window is launched by double-clicking an Available, Suspect, Disabled, Dead or Busy cell in the Modem Utilization window. You can open a Modem Pool window for a group (as seen above) or for a single device.

## Access Watch: the Slot Modem Table window

The **Slot Modem Table** window displays status information for each modem on a device. The Slot Modem Table also allows you to change the usage state of any displayed modem.



Device Name	Modem Index	Slot Index	Item Index	Item Status	Status String	Item Config
NMD-GW	1	3	1	modemStateIdle	-	enable
NMD-GW	2	3	2	modemStateIdle	-	enable
NMD-GW	3	3	3	modemStateIdle	-	enable
NMD-GW	4	3	4	modemStateIdle	-	enable
NMD-GW	5	3	5	modemStateIdle	-	enable
NMD-GW	6	3	6	modemStateIdle	-	enable
NMD-GW	7	3	7	modemStateFailPost	f	enable
NMD-GW	8	3	8	modemStateIdle	-	enable
NMD-GW	9	3	9	modemStateIdle	-	enable
NMD-GW	10	3	10	modemStateIdle	-	enable
NMD-GW	11	3	11	modemStateIdle	-	enable
NMD-GW	12	3	12	modemStateIdle	-	enable
NMD-GW	13	4	1	modemStateIdle	-	enable
NMD-GW	14	4	2	modemStateIdle	-	enable
NMD-GW	15	4	3	modemStateIdle	-	enable
NMD-GW	16	4	4	modemStateIdle	-	enable
NMD-GW	17	4	5	modemStateIdle	-	enable

The following information is displayed in the Slot Modem Table window:

Column Heading	Description
Device Name	The name of the device being reported on.
Modem index	The index number of the modem.

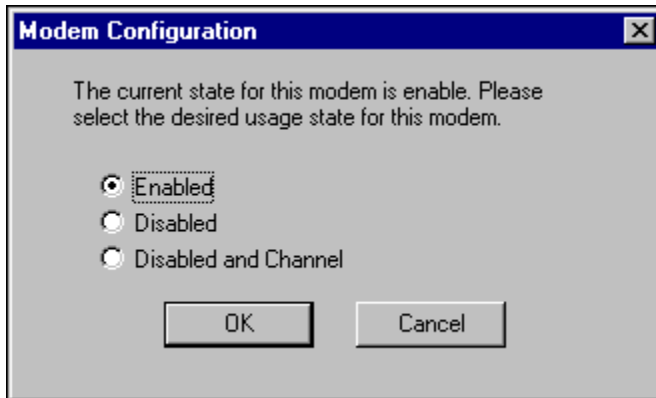
Column Heading	Description
Slot Index	The slot number of the modem.
Item Index	The item number of the modem.
Item Status (Status String values in parentheses)	<p>The status of the modem. Possible values include:</p> <p><b>modemStateNonExist (.)</b> This modem is non-existent.</p> <p><b>modemStateFailPost (f)</b> Failed. This modem failed the POST (Power-On Self Test). The modem is unavailable for use.</p> <p><b>modemStateIdle (-)</b> The modem is not in use.</p> <p><b>modemStateAwaitingRlsd (a)</b> Waiting to go active. The modem has been instructed to dial or answer a call, and the unit is waiting for RLSD (Received Line Signal Detector) to go active.</p> <p><b>modemStateAwaitingCodes (A)</b> Active. RLSD has already gone active and the unit is waiting for result codes to be decoded. This state is entered only if RLSD precedes the codes.</p> <p><b>modemStateOnline (*)</b> Connected. A call is connected and the unit is monitoring RLSD.</p> <p><b>modemStateInit (i)</b> Initializing. The modem is re-initializing after being reset.</p> <p><b>modemStateInitOpenQueued (q)</b> Open request. The modem is re-initializing after being reset and an open request is waiting to be processed when re-initialization completes.</p> <p><b>modemStateInitOpenQueuedVC (Q)</b> Open request for virtual connection. The modem is re-initializing after being reset and an open request for Virtual Connection is waiting to be processed when re-initialization completes.</p> <p><b>modemStateInitDialStr2 (d)</b> Dialing. The first part of the dial string has been sent. This unit is</p>

## Access Watch

Column Heading	Description
	<p>pausing for the modem to read and process the second part before sending it.</p> <p><b>modemStateVirtualConnect (v)</b> Virtual connection. A virtual connection session is active on the modem. No call is active yet.</p> <p><b>modemStateDisabled (o)</b> Out of service in interface. The user has disabled the modem from the configuration interface. The modem is unavailable for calls.</p> <p><b>modemStateDisabledChan (O)</b> Out of service. The user has disabled the modem from the configuration interface. The modem is unavailable for calls and a B-channel is set to OutOfService.</p>
Status String	The status of the modem as displayed in the menu system. Status string values are shown in parentheses in the Item Status field above.
Item Config	<p>Displays the current usage state of the modem. Possible values are:</p> <p><b>enable</b> Modem is available for use.</p> <p><b>disable</b> Modem is on the disabled modem list and not available for use.</p> <p><b>disable and channel</b> An arbitrary B channel is out of service along with the disabled modem.</p>

### Changing the usage state

To change the usage state of a modem, right-click on a modem in the Slot Modem Table window to bring up the Set Usage menu. Select this to open the Modem Configuration dialog box:



The current modem state is indicated in the window. Select one of the following options to change the usage state for the modem:

**Enabled**

Enables a modem currently on the disabled list and makes it available for use.

**Disabled**

Places the modem on the disabled modem list, indicating it is not available for use.

**Disabled and Channel**

An arbitrary B channel is taken out of service along with the disabled modem. The B channel appears on a disabled-channel map, and the device polls all channels on the map with Out-of-Service messages until the associated modem is re-enabled.

**Launching the Slot Modem Table window**

The Slot Modem Table window is launched by right-clicking on a device or device group in the Group Wizard and selecting **Slot Modem Table**.

**Boxmap access**

The Modem Configuration application can also be accessed from the Modem Utilization icon in the Boxmap. Right-click on the icon and choose **Slot Modem Table**.

## Access Watch: the Wan Line Table window

The Wan Line Table window provides channel utilization details for access devices being monitored by the Access Watch application. It also allows you to change the digital line configuration to one of three states (trunk, quiesced, disabled).

For a breakdown of access information by channel, click on any cell to open the corresponding Wan Line Channel Table for that interface.

Device	IfIndex	Name	Type	Channels	State	State String	Line Usage	Active Channels	Available Channels
NMD-GW	2	Factory	1.3.6.1.4.1.529.4.2	24	Is-active	LA	lu-trunk	0	23
NMD-GW2	2	Factory	1.3.6.1.4.1.529.4.2	24	Is-active	LA	lu-trunk	0	23
NMD-GW2	4	Factory	1.3.6.1.4.1.529.4.2	24	Is-loss-of-sync	RA	lu-trunk	0	0
NMD-GW2	5	Factory	1.3.6.1.4.1.529.4.2	24	Is-disabled	DS	lu-disabled	0	0
NMD-GW	9	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0
BigMax	7	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0
NMD-GW	10	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0
NMD-GW2	6	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0
NMD-GW	11	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0
BigMax	2	Factory	1.3.6.1.4.1.529.4.2	24	Is-disabled	DS	lu-disabled	0	0
NMD-GW	12	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0
NMD-GW2	7	Factory	1.3.6.1.4.1.529.4.5	2	Is-no-physical	X	lu-enabled	0	0

The following information is displayed in the Wan Line Table window:

Column Heading	Description
Device	The name of the device being reported on.
IfIndex	The interface index number.
Name	The name of the interface. This is user-configurable on the Ascend device and may or may not be changed from the default setting.
Type	The object ID of the WAN type.
Channels	The number of DS0 channels supported by the interface.

<b>State</b>	<p>The state of the WAN line. Possible values are:</p> <p><b>ls-unknown(1)</b> The state is not known.</p> <p><b>ls-does-not-exist(2)</b> The line does not exist.</p> <p><b>ls-disabled(3)</b> The line is disabled.</p> <p><b>ls-no-physical(4)</b> There is no physical link available.</p> <p><b>ls-no-logical(5)</b> There is no logical link available.</p> <p><b>ls-point-to-point(6)</b> The line is point-to-point.</p> <p><b>ls-multipoint-1(7)</b> The line uses a multipoint-1 connection.</p> <p><b>ls-multipoint-2(8)</b> The line uses a multipoint-2 connection.</p> <p><b>ls-loss-of-sync(9)</b> There has been a loss of synchronization on the line.</p> <p><b>ls-yellow-alarm(10)</b> A warning condition has been received for the line.</p> <p><b>ls-ais-receive(11)</b></p> <p><b>ls-no-d-channel(12)</b> There is no D channel available.</p> <p><b>ls-active(13)</b> The line is active.</p> <p><b>ls-maintenance(14)</b> The line is administratively down for maintenance reasons.</p>
--------------	---

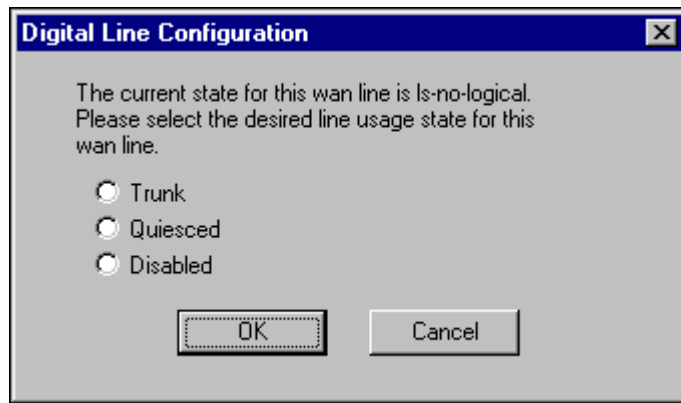
## Access Watch

<b>State String</b>	<p>An indication of the link status. Possible values are:</p> <p><b>LA</b> Link active. The line is active and physically connected.</p> <p><b>RA</b> Red Alarm/Loss of sync. The line is not connected, improperly configured, experiencing a very high error rate, or is not supplying adequate synchronization.</p> <p><b>YA</b> Yellow Alarm. Indicates that one end of the line cannot recognize the signals the other line is transmitting.</p> <p><b>DF</b> D-channel failure. The D channel for a PRI line is not currently communicating.</p> <p><b>1S</b> Keep alive (all ones). A signal is being sent from the T1 PRI network to the device to indicate that the T1 PRI line is currently inoperative.</p> <p><b>DS</b> Disabled link. The line is physically connected but has been disabled in the Line profile.</p>
<b>Active Channels</b>	The number of active DS0 channels on the line.
<b>Available Channels</b>	The number of channels on the line configured but not connected. This variable counts the number of channels with the Channel State of bs-idle(7) for all the entries in its Wan Line Channel table. You can drill-down into this table by double-clicking the cell.
<b>Configured Channels</b>	The number of configured channels on the line. This variable counts the number of channels with any Channel State, except bs-unused(3) and bs-connected(11) for all the entries in its Wan Line Channel table.
<b>Disabled Channels</b>	The number of disabled channels on the line. This variable counts the number of channels with the Wan Line Channel State of bs-unused(3) for all the entries in its Wan Line Channel table.
<b>Hunt Group 1-3 Phone Number</b>	The hunt group phone number associated with the line. This entry is manually entered in the line configurations options.

All fields are sortable by clicking on the column heading. The Modem Utilization window also uses standard toolbar buttons.

### Changing the digital line configuration

To change the configuration of a digital line, right-click on a line in the Channel Utilization window to bring up the Change WAN Line Usage menu. Select this to open the Digital Line Configuration dialog box:



The current line state is indicated in the window. Select one of the following options to change the line state:

#### **Trunk**

Enables the line.

#### **Quiesced**

Disables the line without dropping active calls. All modems not actively used are immediately added to the disabled list. Active calls are not dropped. When an active call drops, the modem is added to the disabled list. This continues until all modems are on the disabled list. At this point, incoming calls receive a busy signal.

#### **Disabled**

Disables the line. All active calls are dropped.

### Boxmap access

Digital Line Configuration application can also be accessed from the Individual Interface icon in the Boxmap for any T1 or E1 interface. Right-click on the

Access Watch

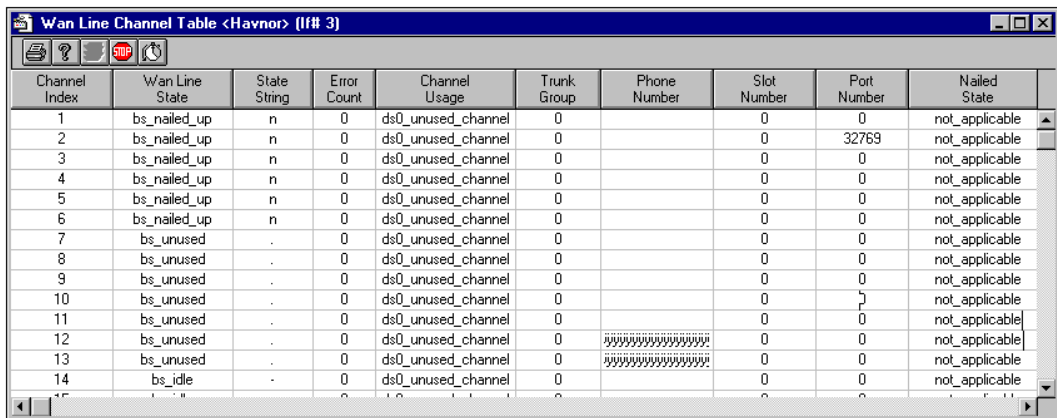
icon and choose **Set WAN Line Usage**.

Launching the Wan Line Table

The Wan Line Table is launched by double-clicking the Channel Utilization cell in the Access Watch application. It can also be launched by right-clicking on a device or group in the Group Wizard and choosing **Access Apps > Wan Line Table**.

Access Watch: WAN Line Channel Table window

The WAN Line Channel Table window provides WAN line details for access devices being monitored by the Access Watch application. The Channel Table is launched for specific interfaces by double-clicking an interface cell in the Channel Utilization window.



Channel Index	Wan Line State	State String	Error Count	Channel Usage	Trunk Group	Phone Number	Slot Number	Port Number	Nailed State
1	bs_nailed_up	n	0	ds0_unused_channel	0		0	0	not_applicable
2	bs_nailed_up	n	0	ds0_unused_channel	0		0	32769	not_applicable
3	bs_nailed_up	n	0	ds0_unused_channel	0		0	0	not_applicable
4	bs_nailed_up	n	0	ds0_unused_channel	0		0	0	not_applicable
5	bs_nailed_up	n	0	ds0_unused_channel	0		0	0	not_applicable
6	bs_nailed_up	n	0	ds0_unused_channel	0		0	0	not_applicable
7	bs_unused	.	0	ds0_unused_channel	0		0	0	not_applicable
8	bs_unused	.	0	ds0_unused_channel	0		0	0	not_applicable
9	bs_unused	.	0	ds0_unused_channel	0		0	0	not_applicable
10	bs_unused	.	0	ds0_unused_channel	0		0	0	not_applicable
11	bs_unused	.	0	ds0_unused_channel	0		0	0	not_applicable
12	bs_unused	.	0	ds0_unused_channel	0	xxxxxxxxxxxxxxxx	0	0	not_applicable
13	bs_unused	.	0	ds0_unused_channel	0	xxxxxxxxxxxxxxxx	0	0	not_applicable
14	bs_idle	-	0	ds0_unused_channel	0		0	0	not_applicable

The following information is displayed in the WAN Line Channel Table window:

Column Heading	Description
Channel Index	The DS0 channel number.
Wan Line State	The state of the WAN line. Possible values are:  bs-unknown bs-unavailable

Column Heading	Description
	<p><b>bs-unused</b></p> <p><b>bs-out-of-service</b></p> <p><b>bs-nailed-up</b></p> <p><b>bs-held</b></p> <p><b>bs-idle</b></p> <p><b>bs-clear-pending</b></p> <p><b>bs-dialing</b></p> <p><b>bs-ringing</b></p> <p><b>bs-connected</b></p> <p><b>bs-signaling</b></p> <p><b>bs-cut-through</b></p> <p><b>bs-current-d</b></p> <p><b>bs-backup-d</b></p> <p><b>bs-maintenance</b></p> <p><b>bs-spc-up</b></p>
State String	<p>A textual representation of the WAN Line Channel State as displayed by the menu system.</p> <p><b>.</b> [dot] Not available. The channel is not available because the line is disabled, has no physical link, or does not exist, or because the channel is marked Unused in the channel usage parameter of the Line profile.</p> <p><b>*</b> [asterisk] Current. The channel is connected in a current call.</p> <p><b>-</b> [hyphen] Idle. The channel is currently idle (but in service).</p> <p><b>d</b> Dialing. The device is dialing from this channel for an outgoing call.</p> <p><b>r</b></p>

## Access Watch

Column Heading	Description
	<p>Ringing. The channel is ringing for an incoming call.</p> <p><b>m</b> Maintenance. The channel is in maintenance/backup (ISDN only).</p> <p><b>n</b> Nailed. The channel is marked Nailed in the Line profile.</p> <p><b>o</b> Out of Service. The channel is out of service (ISDN only).</p> <p><b>s</b> ISDN D-channel. The channel is an active D channel (ISDN only).</p>
<b>Error Count</b>	The error count for the specific channel.
<b>Channel Usage</b>	<p>The use for the DS0 channel. Possible values are:</p> <p><b>ds0-unused-channel</b> <b>ds0-switched-channel</b> <b>ds0-cut-through</b> <b>ds0-clear-64</b> <b>ds0-pri-d-channel</b> <b>ds0-nfas-prime-d</b> <b>ds0-nfas-sec-d</b> <b>ds0-cas-channel</b> <b>ds0-spc-channel</b></p>
<b>Trunk Group</b>	The trunk group assigned to this channel.
<b>Phone Number</b>	The phone number of this channel. This is the number sent to the far end in an inverse multiplexed call when instructing the far end to add more bandwidth. The number should contain the minimum number of digits to identify the channel. If the channel is part of a hunt group, the phone number should be blank.
<b>Slot Number</b>	A slot number for routing incoming calls associated with the channel. A slot-port number zero means calls arriving on this channel can be routed to any port.

Column Heading	Description
Port Number	A port number for routing incoming calls associated with the channel. A slot-port number zero means calls arriving on this channel can be routed to any port.
Nailed State	The nailed group associated with the channel.

All fields are sortable by clicking on the column heading. The Wan Line Channel Table window also uses standard toolbar buttons.

## **Access Watch**

---

## The Boxmap

Double-clicking on an icon in the Group Wizard or from the Internet Map opens the Boxmap for that specific device.

There are two ways of looking at the Boxmap:

- Physical View - Depicts a backpanel image of the device, with all slot cards in place.
- Application View - Multiple icons provide access to device-specific applications.

**NOTE:** Physical view is available only for Ascend devices (Pipeline, MAX, MAX TNT, GRF) and certain Cisco routers.

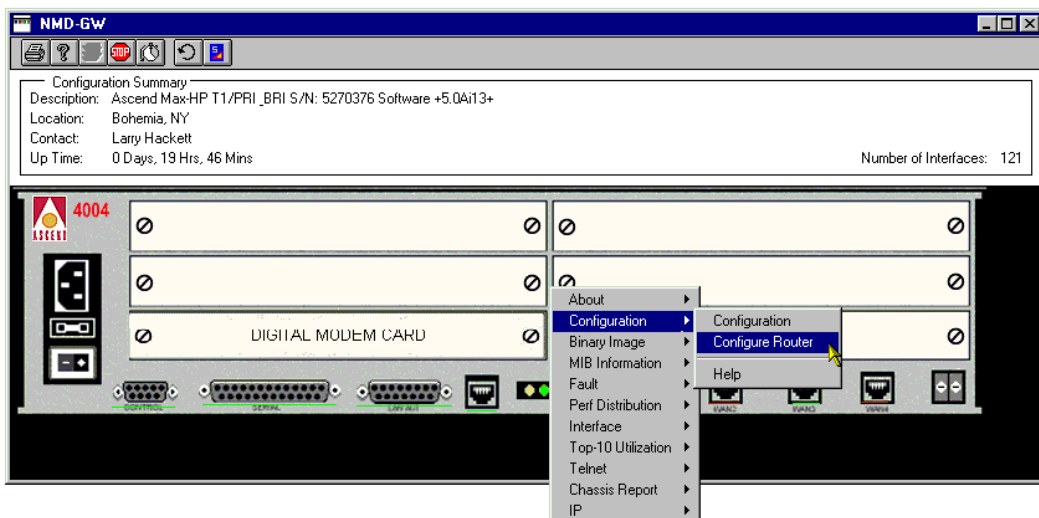
By default, the Boxmap will open as Physical View whenever available. To toggle from physical view to application view, double-click on a blank area of the Boxmap window.

### Physical view

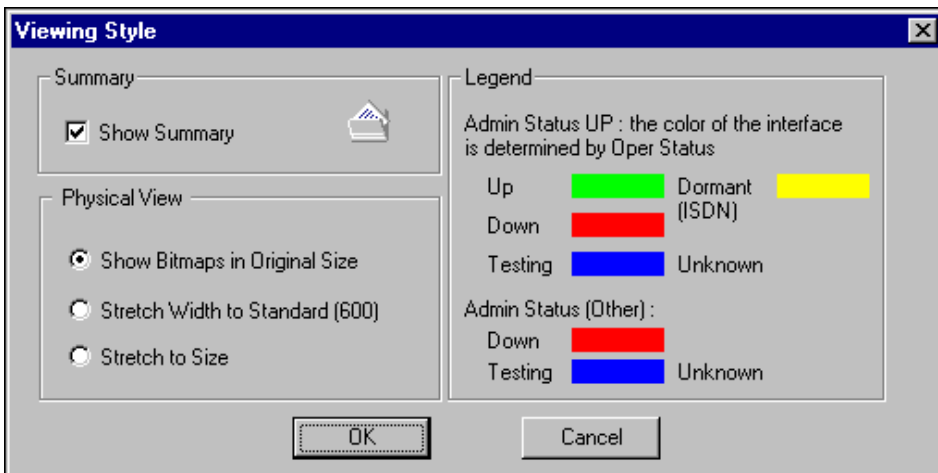
The Physical view depicts the device backpanel, dynamically displaying all slot cards currently on the device. Right-clicking on a blank area of the physical view provides menu access to all device-specific applications.

Right-clicking on individual interfaces provides menu access to interface-specific applications.

## Boxmap



Interfaces status is indicated on the physical view by a colored line under the interface. Click the [Style] button to view the Legend for what each color signifies.



Other items on the Viewing Style window are:

### Show Summary

Toggles the Summary pane on and off. The Summary pane is the top pane in the Boxmap that displays configuration information. By default, this is on.

### **Physical View**

Alters the way the Physical View is presented. Options are:

#### **Show Bitmaps in Original Size**

Physical view backpanels are displayed in their original size, and cannot be resized. This is the default view. Every time you open a Boxmap, this view is displayed.

#### **Stretch Width to Standard (600)**

Sets backpanels at a standard size. With this option selected, all backpanels will display at the same width.

#### **Stretch to Size**

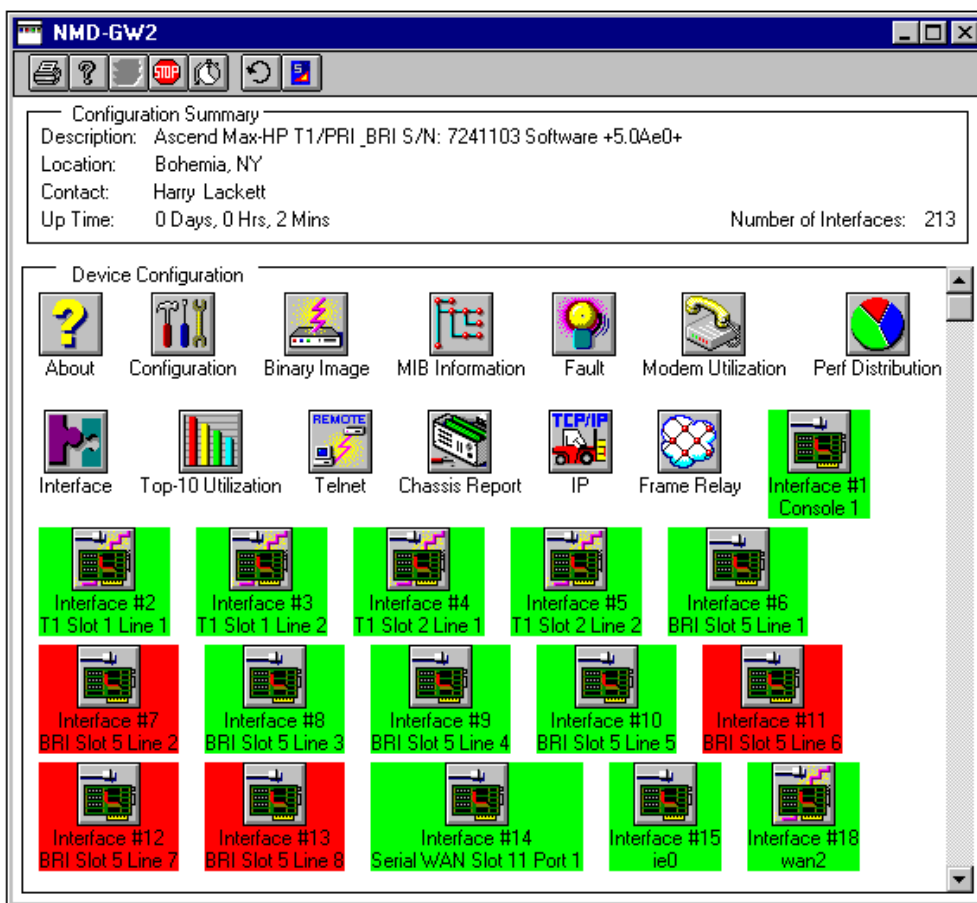
Sets the backpanel to fill the entire Boxmap window. As the window is resized, the backpanel is resized.

### Application view

The Application View displays icons that launch related application menus. For example, by right-clicking the IP icon, you will access a menu for IP-related applications.

Interface icons provide access to interface-specific applications. For example, by right-clicking on an interface icon, you can access the Utilization applet which provides utilization data for that interface.

The icons displayed in the Application View will vary based on the device, manufacturer, and software level. Each icon also has a help option which opens a help topic detailing all the options available from the icon.



## The Internet Map: Overview

### **Menu Bar:** File > Internet Map

The Internet Map provides a graphical depiction of the entire network, including network devices and connection types.

Among the capabilities provided by the map are:

- Launching of device-specific applications
- Launching of link/connection-specific applications
- Launching of protocol/service-specific applications
- Grouping of map icons into logical entities (LAN, POP, Corporate Office, etc.)
- Manually creating links between devices
- Drill-down into smaller submaps, circuit maps and segment maps
- Reporting of device alarms
- Color-coding of network link status (up, down, degraded)
- Filtering and finding tools

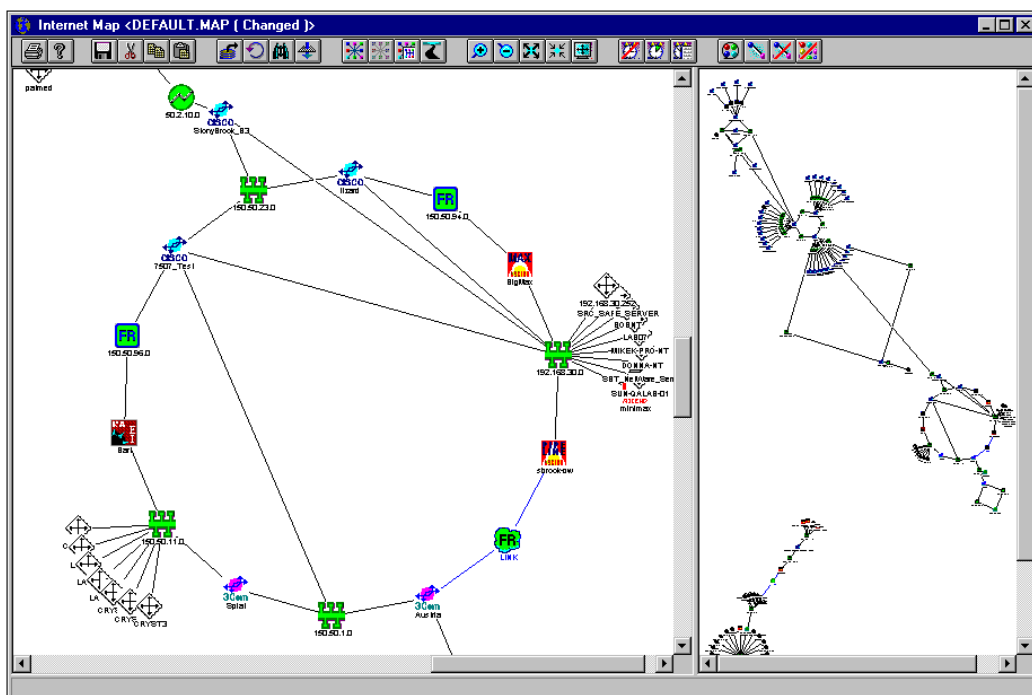
### **Launching the Map**

When first launched by selecting **File > Internet Map**, the map takes a few moments to build itself from the database. The map building action takes place on screen. Map information is automatically saved as file DEFAULT.MAP. If your database has changed, rescan the map to update the devices on screen.

Changes you make to the original map can be saved by using the Save icon in the Internet Map toolbar, and retrieved by selecting Map List from the File menu (**File >Map List**).

## The Internet Map

Below is a sample Internet Map.



## Reading the Internet Map

The Internet Map is composed of several types of icons.

- Device icons, which represent specific types of network devices (MAX, Pipeline, Cisco router, etc.)
- Segment icons, which represent types of connections (serial, Frame Relay, Token Ring, etc.)
- Group icons, which are user-created logical groupings of device and segment icons. When a group icon is created, the individual icons that comprise the group are no longer shown on the map.
- Links, which are the lines drawn between devices, segments and groups.
- Circuit icons, which represent individual circuits of a Frame Relay, X.25, FDDI or ISDN connection.

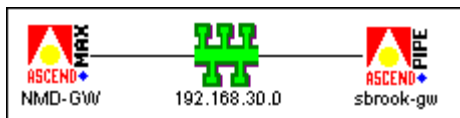
- Alarm icons, which appear above device icons to report alarm information.

It is important to understand the relationships between map elements.

Typically, a device icon will be linked to another device icon, and the link will pass through a segment icon.

### One-to-one connection

The map section below shows an Ascend MAX (named **NMD-GW**) connecting to an Ascend Pipeline (named **sbrook-gw**).



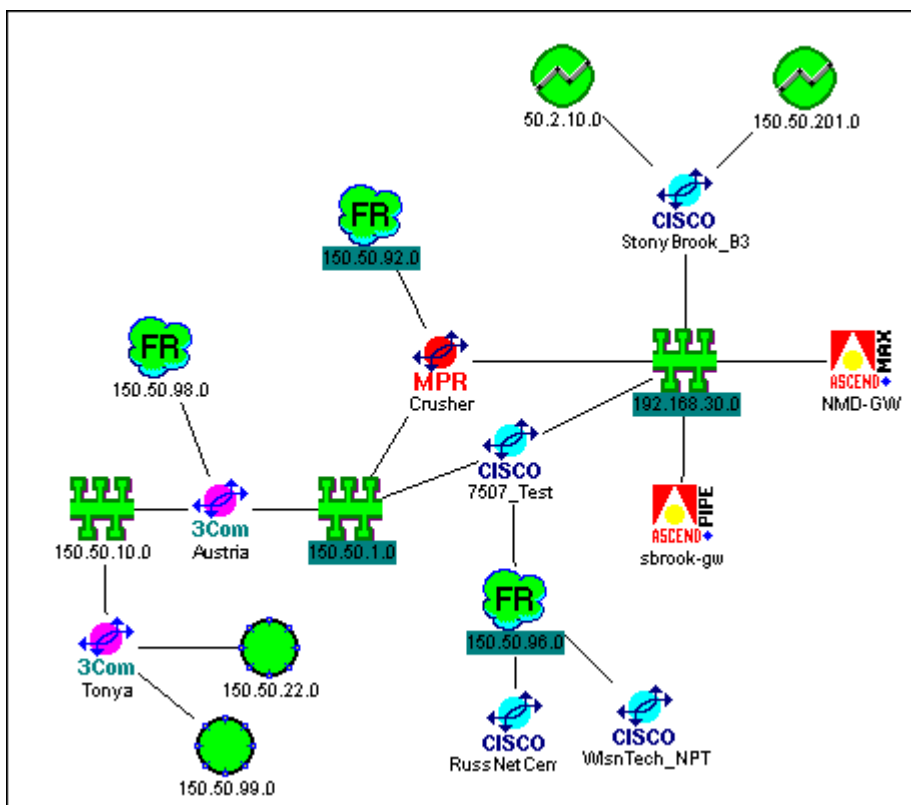
The connecting link passes through an Ethernet icon, indicating that the two devices "talk" to each other via an Ethernet connection. The Ethernet icon is labeled with the IP address of the network segment. In the example, the MAX and Pipeline are connected along the 192.168.30.0 network segment.

Note that segment icons always have IP addresses ending in zero. This is because they represent a network segment, not a physical device with a specific IP address on the network.

### Multiple device connections

A device may connect to many other devices, using many connection types. For example:

## The Internet Map



There are many things to note in the map section above. Looking at the map from left-to-right, we begin with the 3Com router **Tonya**. The map shows two Token Ring icons connecting to Tonya, with subnets 150.50.22.0 and 150.50.99.0. Tonya is also connected via Ethernet to 3Com router **Austria**.

Austria has a Frame Relay cloud connected to it, indicating a Frame Relay interface. You can right-click on the Frame Relay cloud and access an array of applications for information such as specific interfaces, Top 10 talkers, Alarm and Event Reports, and more. Similarly, you could right-click on the 3Com icon to access more applications, including the device Boxmap.

Austria connects via Ethernet to both the MPR router **Crusher** and the Cisco router **7507\_Test**. Note the Ethernet link's IP subnet (150.50.1.0) is shown in a green box. This indicates a consolidated link.

7507\_Test connects via Frame Relay to two other Cisco routers, and via

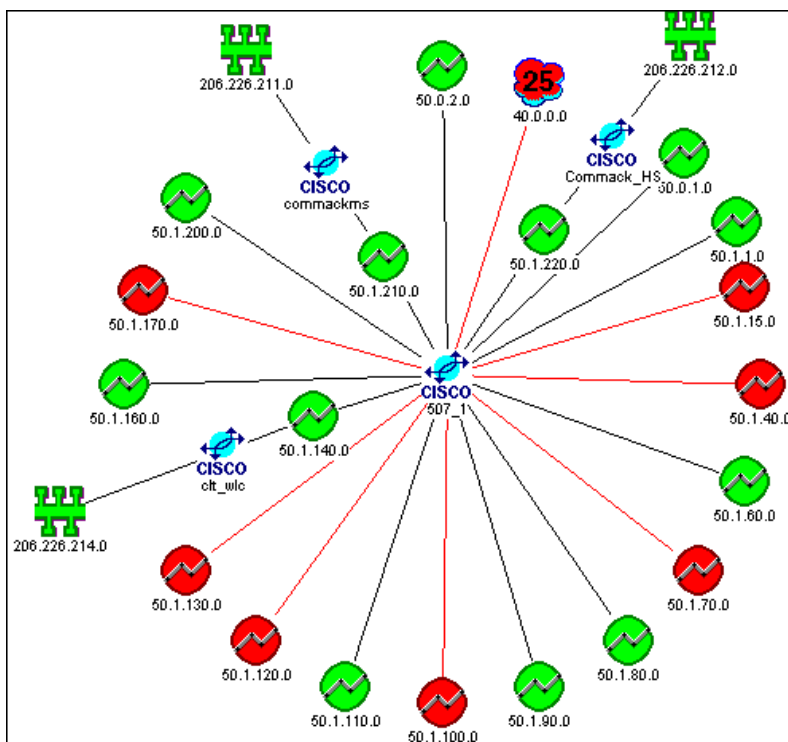
Ethernet to another Cisco router (**StonyBrook\_B3**), an Ascend MAX (**NMD-GW**) and an Ascend Pipeline (**sbrook-gw**). The Cisco router StonyBrook\_B3 has two serial interfaces.

The two Ascend devices are clearly at the edge of the network, as you would expect for access devices. You can easily drill-down into them from the map to see precisely what kinds of lines they connect to, the utilization on the lines, etc.

Note that this diagram is only a section of a map used for illustrative purposes and is not meant to be complete.

### Multiple network segments

In the example below, the router in the center has many segment icons connecting to it. They are all point-to-point interfaces, except for one X.25 cloud, showing that one interface on the router is configured for X.25 services.



The point-to-point, or serial, icons each indicate a physical connection between

## The Internet Map

---

two nodes. Many of the serial icons have no link lines on the side away from the router. This may be because there are no other network devices on the given segment, or that the devices were not discovered (possibly because of incorrect community strings). Also, the segments may contain only PCs or file servers, and not network devices (routers, access servers, etc.).

Three of the links to the center router connect to other routers. These connections are then passed along by the other routers through an Ethernet icon. On the full map, the link lines continue from the Ethernet icon, but in this example they have been truncated.

### Status color codes

The Internet Map uses color coding to indicate the status of segments and links.

For segment and circuit icons, the following color codes are used:


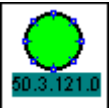
Segment Icon Color	Status	Description
Red	Down	All devices on the segment/circuit are down
Yellow	Degraded	Some devices on the segment/circuit are down
Green	Up	All devices are up

Links use the following color codes:

Link line Color	Status	Description
Red	Down	The link between devices is down.
Black	Up	The link between devices is up.

### Grouping color codes

The Internet Map uses color coding of icon text to identify icons that represent groups of devices or segments. The following color codes are used:

Color of icon text	Sample icon	Description
Black text Gray background		Indicates a user-created rollup group.
Black text Green background		Indicates a segment icon that has been consolidated.

### Alarm Reports on the Map

The Internet Map uses alarm-bell icons to indicate that an alarm has been received for a device. When an alarm is reported, an icon appears over the network device in question.

## Map navigation and manipulation

The Internet Map is very flexible, both in ways to navigate the map and ways to display it.

### Navigating the Map

Because the Internet Map initially displays all devices discovered on the network, it can be very highly populated with icons, making it difficult to find particular devices. There are two tools which help you locate devices on the map.

- The Map Navigator
- The Search Node function

### Manipulating the Map

When first generated, the Internet Map displays a picture of the network based on its default settings. However, there are many options available for modifying the map as desired. Options include:

## The Internet Map

---

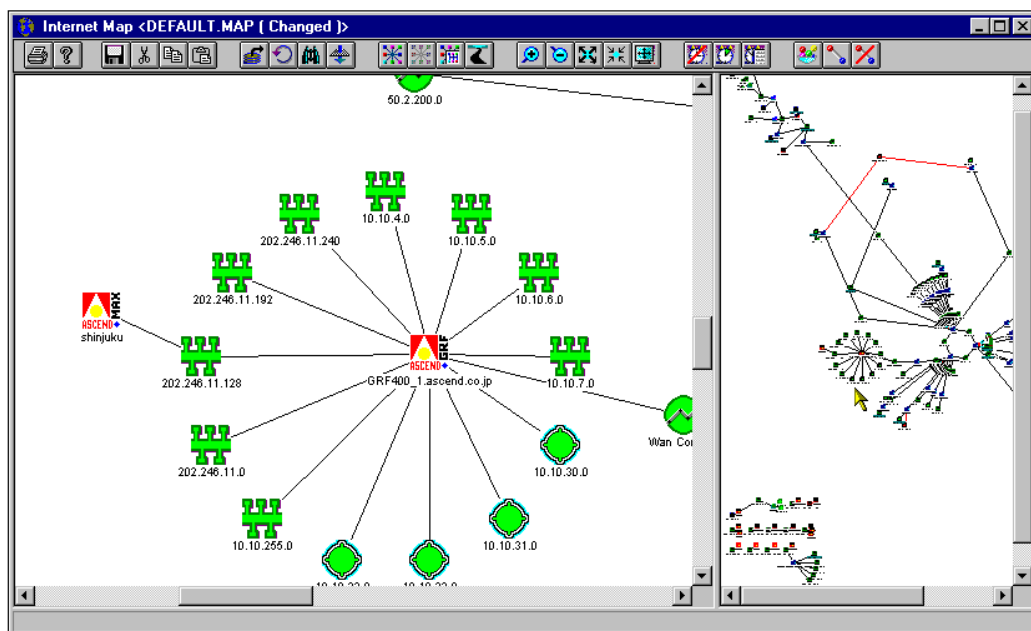
- Movement of map components
- Scaling the map
- Cut/paste/copy
- The Network Filter function
- The Consolidate option
- Grouping of map icons
- Manual linking of devices

When you have finished modifying a map, you can save the map for reuse at a later time.

## The Internet Map Navigator

The Internet Map is divided into two panes. The left pane is the working map, from which applications are launched and the map's appearance manipulated. The right pane is the Map Navigator, which shows a condensed, bird's-eye-view of the map. When you click the mouse anywhere within the Map Navigator, the working map will move to view that portion of the map.

This provides an easy means to jump quickly from one end of the map to another. In the illustration below, you can see the mouse pointer in the right-hand pane, and the corresponding map section in the left.



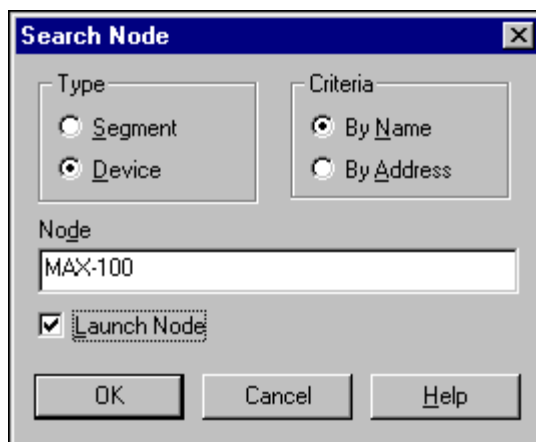
### Search Node function

The Search Node function quickly locates a specific device or segment on the map, moves the map to where the device icon is, and highlights the name or IP address in black.

**To use the Search Node function:**



1. Click the [Search Node] button to display the Search Node dialog box:



2. Select the search options.

### Type

Indicates the type of map item you are searching for, either a Device icon or a Segment icon.

### Criteria

Choose if you want to identify the device by the device Name or IP Address. This option does not apply when Segment is selected.

### Node

Enter the name or IP address of the device/segment you wish to locate.

### Launch Node

Select to automatically open the Boxmap for a device or the Subnet map for a segment when the item is located.

3. Click [OK] to launch the search node.

## Moving and Scaling Map Icons

Any icon on the Internet Map can be moved by holding the left mouse button on it and dragging it to a new location.

Multiple icons can be moved together or rotated in place.

### To move or rotate multiple icons:

1. To select icons, use one of the following:

- a. Hold down the [Ctrl] key and click on as many icons as you wish to manipulate. Highlighted icons will show their names with white text on a black background.
- b. Click and hold your mouse on a blank spot in the map. Drag the mouse cursor, which will generate a box behind it. Drag the box until all the icons you wish to highlight are included.

**NOTE:** After highlighting using the mouse-drag method, you may select additional icons by holding the [Ctrl] key and clicking. However, if you use the [Ctrl] key to make selections first, and then use the mouse drag, the [Ctrl] key selections will be de-selected.

2. After making your selections, you can move the icons by holding down the mouse button and dragging. A box outline will appear on the map. Drag the box to new location. When you release the mouse button, the icons will move. Icons will remain highlighted, so to move them again, simply re-click and hold the mouse, and drag again.
3. To rotate the icons, after making your selections, right-click on any of the selected icons and choose **Rotate Selected Nodes**. A box will appear which you can turn by moving the mouse. Move to the desired position and re-click to move the icons.

### Select all or none



The Internet Map allows you to select or deselect all icons through the toolbar [Select All] and [Unselect All] buttons. Simply click the appropriate button for the desired action.



**NOTE:** The [Select All] feature is not recommended for use with large maps. It is more appropriate for smaller submaps and subnet maps.

### Scaling the map icons






The Internet Map allows you to increase and decrease the size of the icons through a number of toolbar button options. Scaling options apply only to the left-pane, or working side, of the map.

The options are:

Toolbar	Description
---------	-------------

## The Internet Map

---

button icon	
	<b>[Increase Scale] button</b> Increases the map scale one level each time it is clicked.
	<b>[Decrease Scale] button</b> Decreases the map scale one level each time it is clicked.
	<b>[Biggest Scale] button</b> Switches to the largest scale map.
	<b>[Smallest Scale] button</b> Switches to the smallest scale map.
	<b>[Best Fitting] button</b> Provides the best fit for the current screen size.

## Cutting, pasting and copying in the Internet Map

Frequently, NavisAccess users will customize their Internet map to meet their needs, often creating and saving a number of different maps, each serving a different purpose.

One means of creating customized maps is using the cut, copy and paste options. This allows you to cut or copy items from one map and paste them into another. Or, you can simply cut objects out of a map and then save the map under a new name.

**NOTE:** You cannot cut items permanently from the Default Map. If you cut objects, you must save the map under a new name. The Default Map will always show the full database when it is opened.

### To cut/copy and paste a map:

1. Highlight the icons you wish to cut/copy. It is preferable to select a small number of icons that are linked, or an independent group of devices. Selecting separate devices from many locations on the map is not an effective means of copying.
2. Click the [Cut Map] or [Copy Map] toolbar buttons.

3. Open or switch to a different map, and click the [Paste Map] button.

The copied icons will be placed at the top of the map, with their links intact. They can then be moved within the map to a desired location, or you can click the [Re-layout Map] button to automatically re-layout the map.

### Notes about cut/copy paste

Be aware of the following:

- NavisAccess stores only the most recently cut/copied objects. If you cut a group of devices and then cut a second group before pasting the first group, the first group will no longer be available.
- You cannot cut/copy a single device icon. You must select at least one device icon and one segment or circuit icon connecting to it (i.e., a complete link).

## The Network Filter

The Network Filter allows you to view only devices from a specific subnetwork or multiple subnetworks.

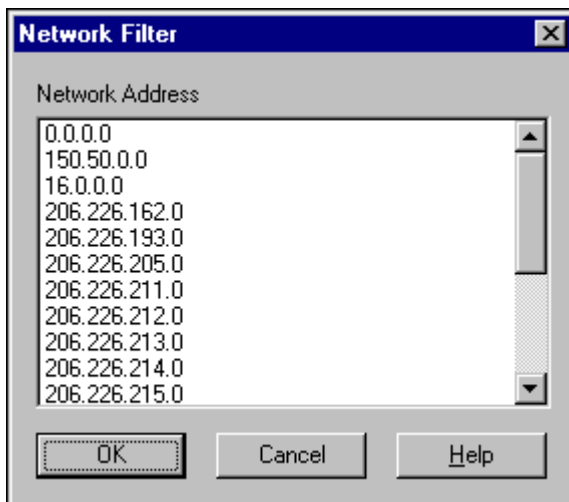
### To use the Network Filter:



1. Click the [Internet Filter] button to open the dialog box.

## The Internet Map

---



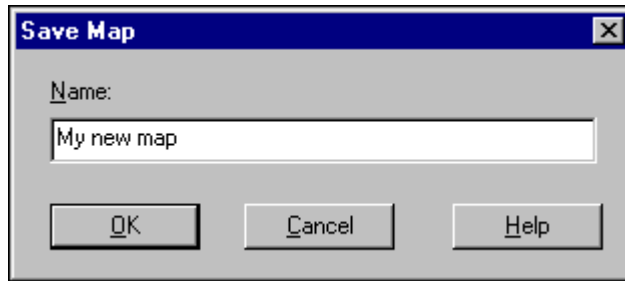
2. Select the network addresses you wish to include in the submap by clicking them on or off.
3. Click OK. A new map will open, showing only the devices and segments found in the chosen addresses.
4. You can continue to filter within the submap. The Network Filter will show only the addresses contained within the submap, and you may further narrow down the selection and launch another submap.

## Saving an Internet Map

After modifying an Internet map, you can save it for reuse at a later time. You can also save submaps, subnet maps and circuit maps.

### To save a map:

1. With the map window open and selected, click the [Save Map] button to open the dialog box.



2. Enter a name for the map and click OK.

### To retrieve a saved map:

1. Select **File > Map List** from the main menu bar to display the Internet Map List screen.
2. Double-click the icon for the map you want to retrieve.

## Launching applications from the Map

The Internet Map provides quick access to the full array of powerful NavisAccess management tools. Different tools are accessible from different types of icons. To access applications, simply right-click on any map icon and make the appropriate selections.

### From device icons, you can:

- Open the Boxmap, which provides access to all tools for that device
- Configure the device information
- Discover the device
- View the IP Route Table for information on destination, next hop, etc.
- View the Interface Table for details on all device interfaces
- Access the Alarm Monitor and Event Report
- Launch remote access applications
- Telnet to the device
- Access tools for Frame Relay

## The Internet Map

---

### From segment icons, you can:

- Open a subnet net, which shows all devices on the segment and reports interface utilization
- Open the Alarm Monitor and Event Report. This is particularly useful because when you open these applications from the segment icon they report only on the devices on the segment.
- View the Top 10 Talkers on the segment
- View the Group Interface table for the segment
- For Frame Relay, X.25 and ISDN clouds you can also view the circuit map

### From a link line, you can:

- Open the interface utilization monitor for the interface being used on the link

## Grouping map items into logical entities

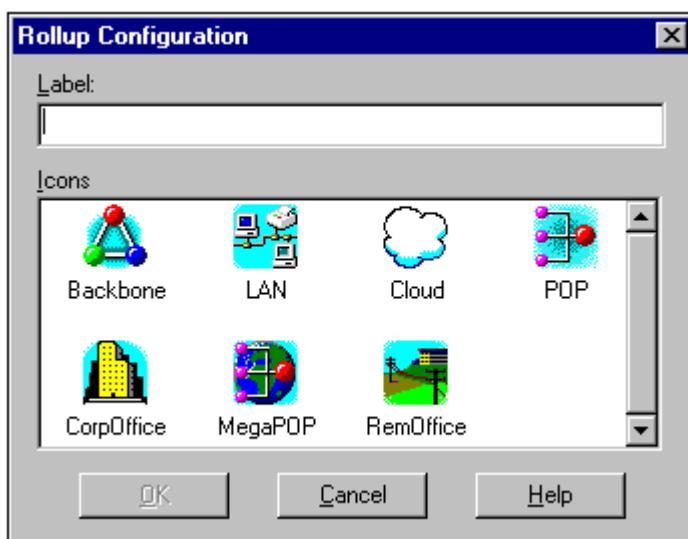
One of the most powerful features of the Internet Map is the ability to group map icons into logical entities. Any device and segment icons can be selected and "rolled up" into a group, which is given a user-defined name and icon. A number of identifying Rollup icons are available to choose from, to help identify the purpose of the group.

Group-based applications can be launched from the Rollup icon.

### To create a Rollup group:

1. Highlight the map icons you wish to include in your group. Devices should be grouped for logical reasons, such as they are the devices that form a LAN, a POP, or a network backbone.
2. Click the [Roll Up Nodes] button to open the dialog box:





3. Enter a label name for the Rollup icon. The name should be descriptive of the group's purpose, location, etc.
4. Select an appropriate Rollup icon by clicking on one in the Icons window. Rollup icons are identifiable by their common blue-background color, and icon labels on the map are gray with black text.
5. Click [OK]. The selected devices will disappear from the map, replaced by the Rollup icon.

## Rollup Functionality

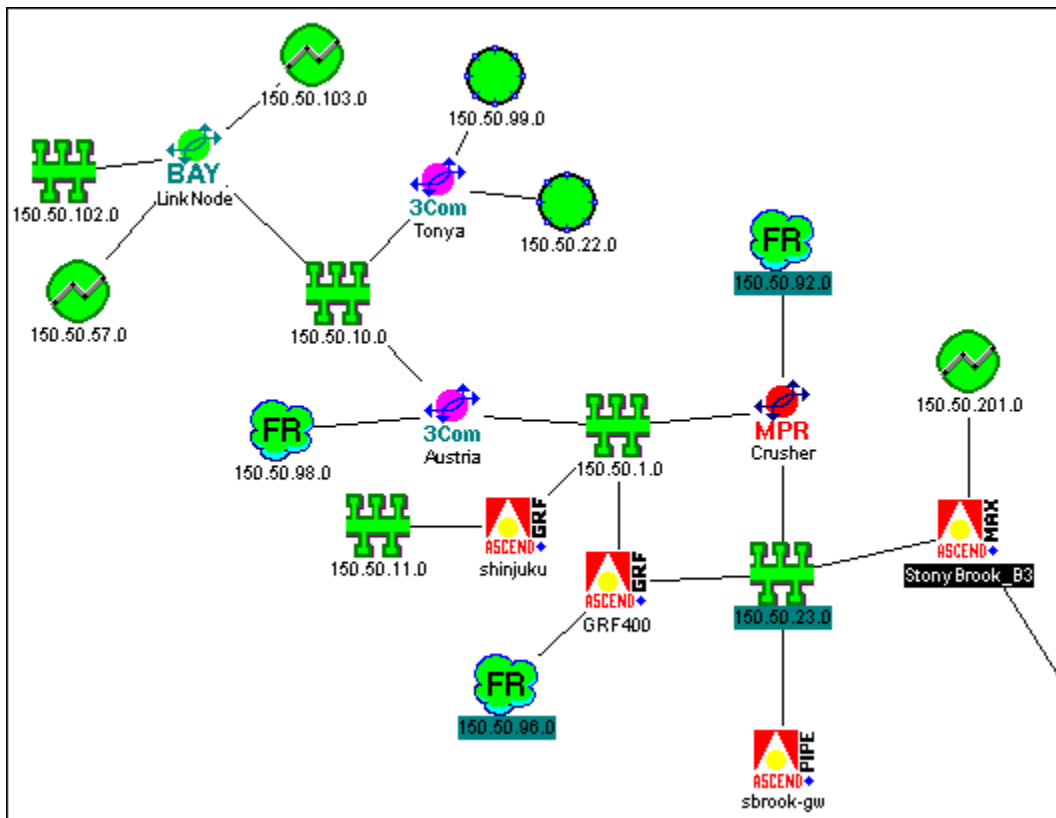
Once a group of devices is collected into a Rollup group, there are various available functions you can perform on the group. To illustrate Rollup functionality, we will illustrate an actual example.

### Example Rollup

1. We begin with a section of an Internet Map that shows a corporate office network, including the access devices (Ascend MAX and Pipeline), routers (Ascend GRF, Novell MPR, 3Com and Bay) and various segment icons.

## The Internet Map

Because this is only one portion of a very large map, we would like to consolidate it to make the map less crowded.

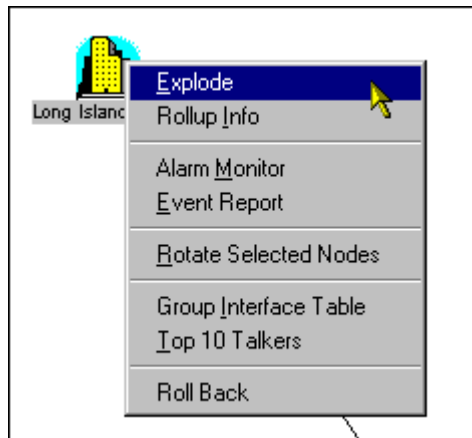


2. The process begins very simply. We highlight all the devices by clicking and holding the mouse pointer and dragging the rectangle over all the icons. Then we click the [Rollup Nodes] button, name the group "Long Island Office," choose the Corporate Office icon and click [Ok]. The map section above now looks like this:



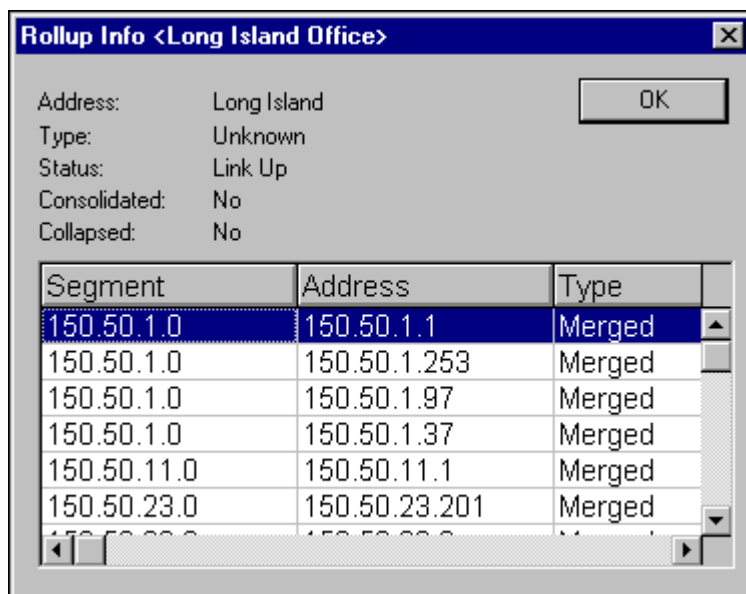
As you can see, the complexity of the map is greatly reduced.

3. By right-clicking on the Long Island Office icon, we can access a number of applications.



The first of these is the **Explode** option. By selecting Explode, we will open a second Internet Map window which will re-display the original icons that made up the Long Island Office group (i.e., it will look like the map in Step 1). This allows you to quickly view the component devices of the group, and access the individual device applications for them. If you wish, you can save the Exploded group as a separate map.

4. The **Rollup Info** option displays a list of all the network segments in the Rollup group, and the specific IP addresses on those segments.



5. The **Alarm Monitor** and **Event Report** options will launch those applications, which will display only data related to the devices in the Rollup group.
6. **Rotate Selected Nodes** allows you to rotate icons around a central point. You must have two or more icons selected for this to function.
7. **Group Interface Table** and **Top 10 Talkers** will launch those applications for all segments contained within the Rollup Group, and for the device or devices connecting to the group.
8. **Rollback** will "unroll" the group and return the individual devices to the map. After a rollback, the devices will be displayed along the top of the map. You need to click the [Re-layout Map] button to return the map to its original state.



## Adding a link to the Map

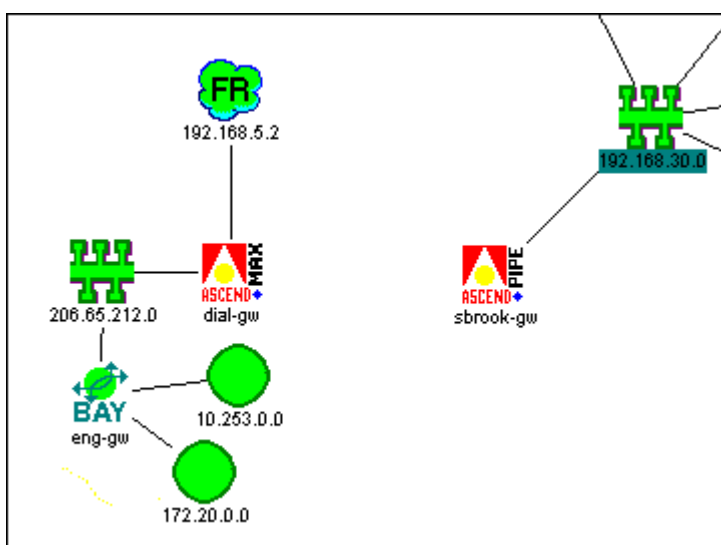
The Internet Map allows you to manually create a link between two devices. This can be used in situations where two devices are known to be connected but the map did not represent them as such because they are not connected via the IP protocol. Or, it can be used for appearance purposes.

A manually created link has limited functionality, and you cannot create a link between two devices that are already linked on the map.

### To manually create a map link:

1. Highlight two devices in the Internet Map by holding the [Ctrl] key and clicking each one.

For example, in the map section below, we want to connect Ascend MAX **dial-gw** to Ascend Pipeline **sbrook-gw**. Both devices should be highlighted.



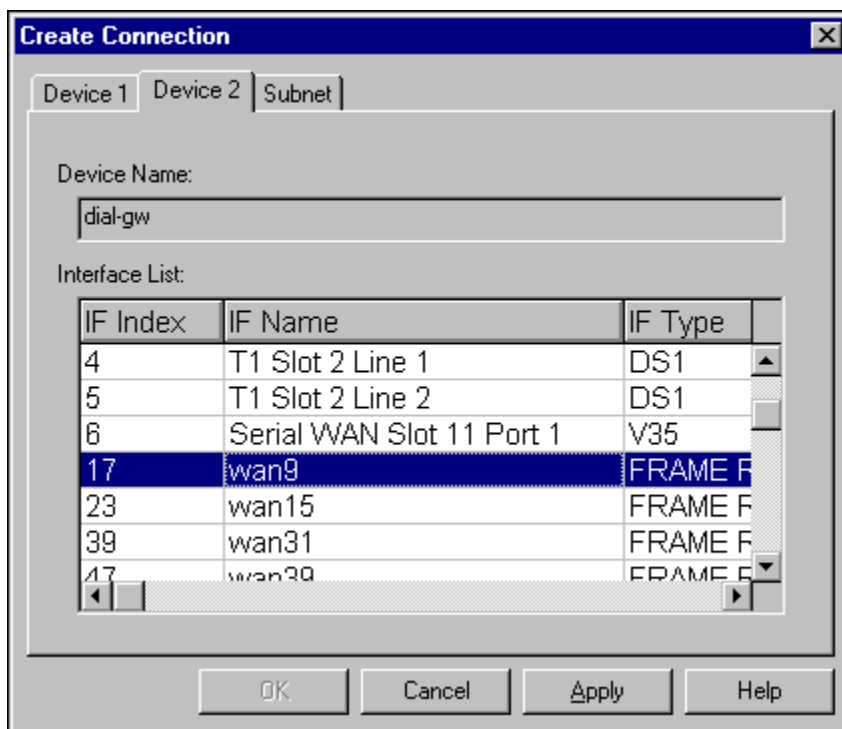
2. Click the [Add Link] button to open the Create Connection dialog box.

The dialog box is used to select the interfaces that will connect the two

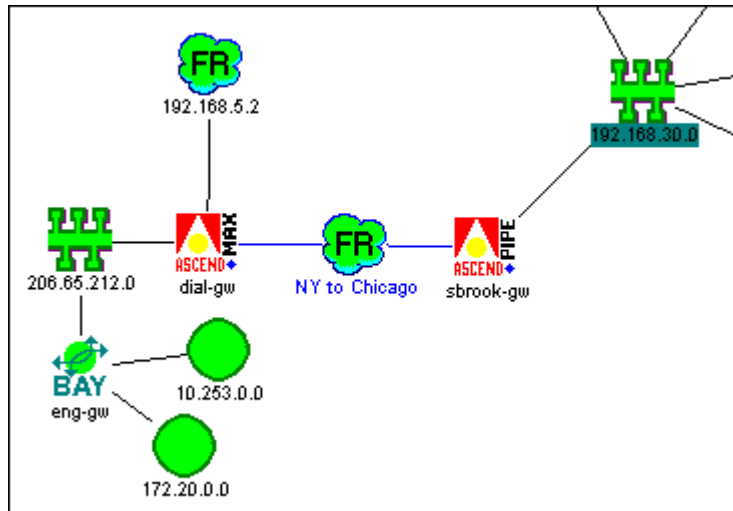
## The Internet Map

---

devices. Interfaces are displayed by index, name and type. The dialog box lists only interfaces that are not currently used on the devices. Therefore, if a device has no unused interfaces, the dialog box may be blank and a link cannot be created.



3. Click the Device 1 tab and select an interface.
4. Click the Device 2 tab and select an interface.
5. Click the Subnet tab and enter a name for the link you are creating. In our example, one device is in the New York office and another in Chicago, so we name the link "NY to Chicago."
6. Click [Apply], then click [OK]. The new link will appear on the map. For example, our sample link now looks like this:



Note that manually created links and link text are colored blue. Also, in this case, because the link was created by selecting two Frame Relay interfaces, the connection icon is a Frame Relay cloud. The icon used will depend on the interfaces selected.

### Deleting a link



1. To delete a link, highlight all three link components (two devices and the joining link icon) and click the [Delete Links] button.

### Cutting nodes from the Map

The Internet Map allows you to quickly remove any segment icons that are either not connecting two or more devices or not consolidated. After cutting the nodes, you can save the map and reopen it with the cuts still in place.

#### To cut segment icons:

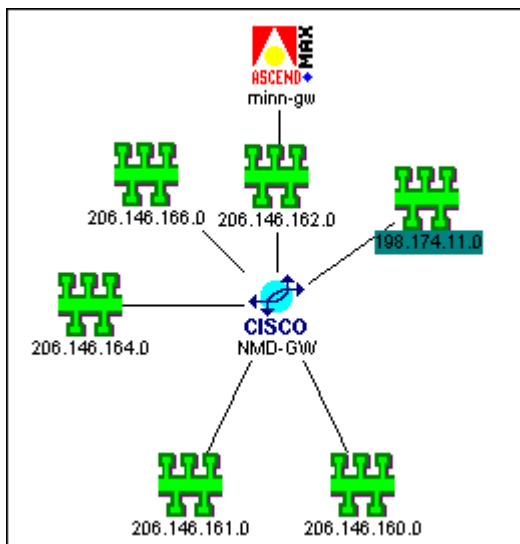


1. Open an Internet Map.
2. Click the [Cut Lead Nodes] button. Non-connected and non-consolidated nodes will be deleted.

For example, the illustration below shows a map before nodes are cut.

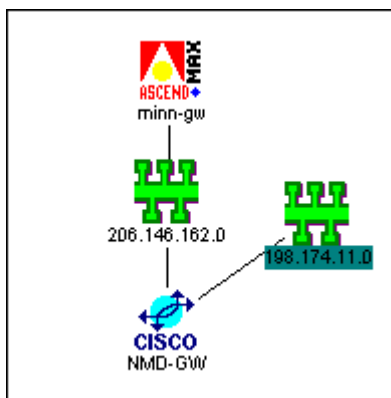
## The Internet Map

---



Note that only one segment icon is connecting two devices, and one is consolidated. Cutting the nodes would eliminate all but these two nodes.

After clicking the [Cut Leaf Nodes] button, the map looks like this:



3. You can now save the map. When you reopen the map, the cuts will be in place. Note, that cutting nodes does *not* affect the Default Map, which cannot be overwritten and is always generated from the current database.

**To restore cut nodes**

1. After cutting nodes, click the [Paste] button. Nodes will be restored along the top of the map window.
2. Click the [Re-layout Map] button to re-draw the map.

**NOTE:** You can only paste the most recent cut. If you cut the nodes and then cut nodes in another map, the nodes from the first cut will be lost.

### Internet Map drill down levels

The Internet Map has three additional levels you can drill-down into.

- Subnet Map
- Segment Map
- Circuit Map

### Subnet Maps

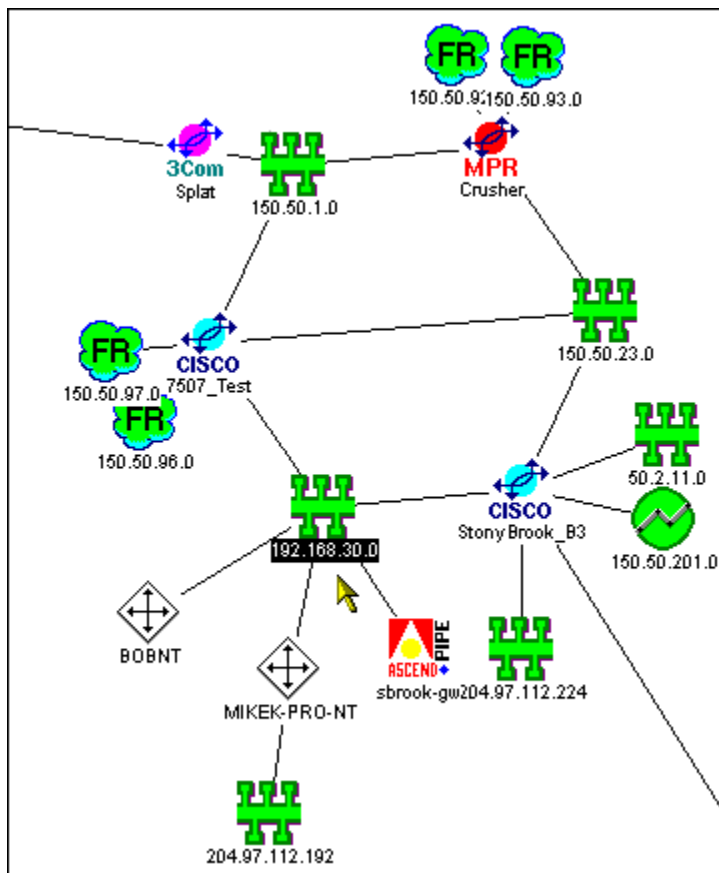
Subnet Maps display all routing devices that are part of a specific IP subnet. In addition, depending on the devices selected, they can display the Interface Utilization graph for a device you specify using the [Subnet Configuration] button.

Open a Subnet Map by right-clicking a segment icon in the Internet Map and selecting Subnet.

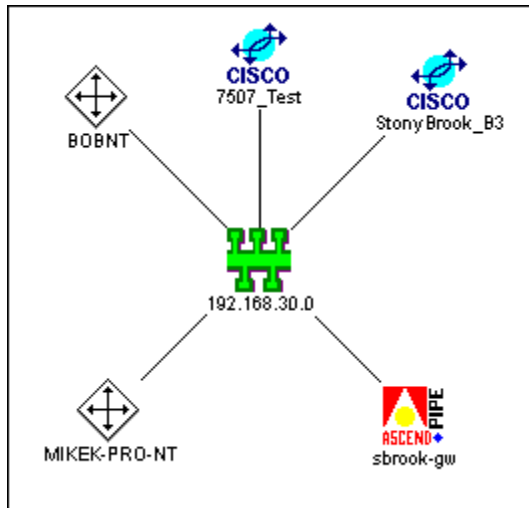
For example, the illustration below shows a section of an Internet Map. A little below the center of the picture, the mouse is pointing at an Ethernet icon, subnet 192.168.30.0.

## The Internet Map

---



If you right-click on this icon and select Subnet, you would launch a new map similar to the following:



Note that this map shows only the single Ethernet segment, and only the devices connected to it. Included in the map window would be a utilization graph allowing you to track line utilization between devices in the subnet map.

### To display Subnet utilization information:

1. Click the [Subnet Configuration] button.
2. Specify if you want the device displayed by Address or by Name.
3. Specify the polling interval.
4. Select the device you wish to monitor.
5. Click [OK].
6. Start the monitoring by clicking the [Start Utilization] button. A utilization graph will display line utilization for the selected device.

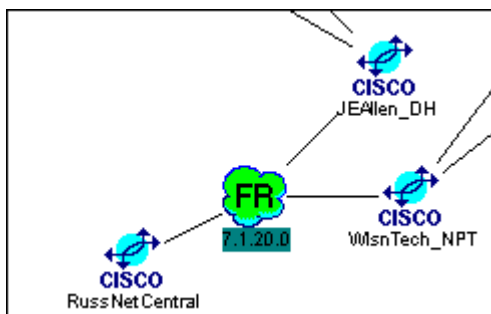
## Segment Map

A Segment Map displays all devices, including known workstations, that are part of a specific segment. A Segment Map is opened from within a Subnet map. Click on the segment icon within the subnet map and select **Segment Map**.

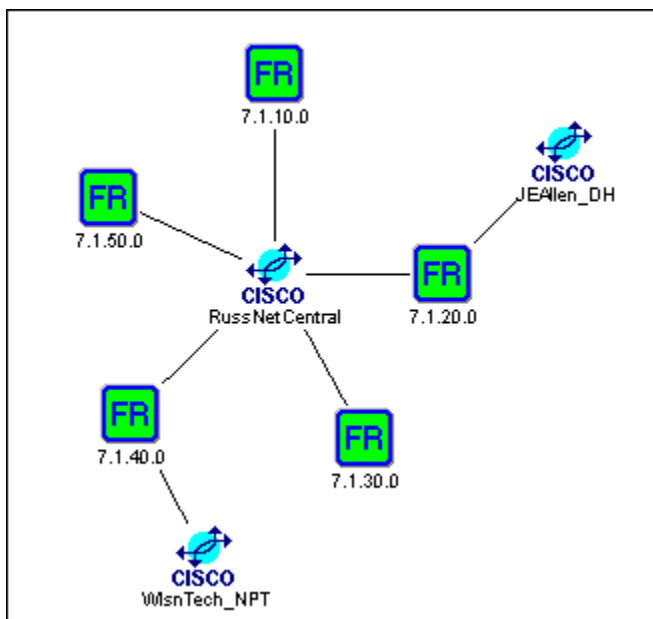
### Circuit Map

A Circuit Map displays individual circuits for Frame Relay, ISDN, FDDI or X.25. The regular Internet Map will, by default, consolidate multiple circuits into one map icon. The Circuit Map expands this view and shows each circuit individually. This also allows you to configure a Virtual Circuit link between two devices.

For example, below is part of a map showing three routers connecting over a Frame Relay link. The Frame Relay icon is consolidated, as indicated by the green background of the segment address.



To view the Circuit Map, right-click on the Frame Relay icon and select **Circuit Map**. Doing so with the illustration above would open a Circuit Map that looked similar to this:



There are now five separate Frame Relay circuits, rather than just one consolidated icon. You can now configure the link between devices by right-clicking on any icon that is connected to two devices and choosing **Configuration**.

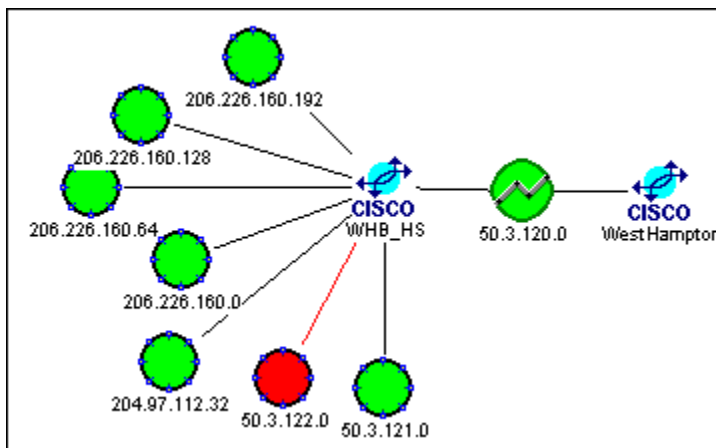
**NOTE:** If you do not have the Consolidate option selected, the map will display individual circuit icons.

### The Consolidate Map option

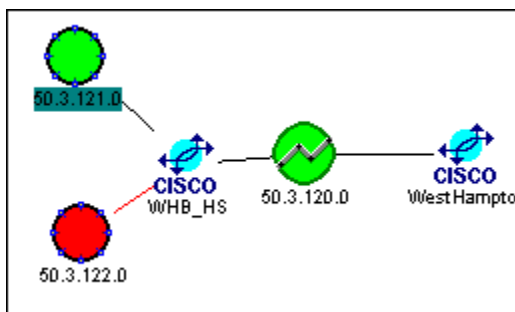
The Consolidate option reduces the number of segment icons on the Internet map by combining sub-interfaces on the same interface into one icon. For example, the following map illustration shows a router (WHB\_HS) with seven Token Ring icons. In fact, there are only two Token Ring interfaces on this router. The rest are sub-interfaces. However, a map that is not consolidated will show each sub-interface as a separate icon.

## The Internet Map

---

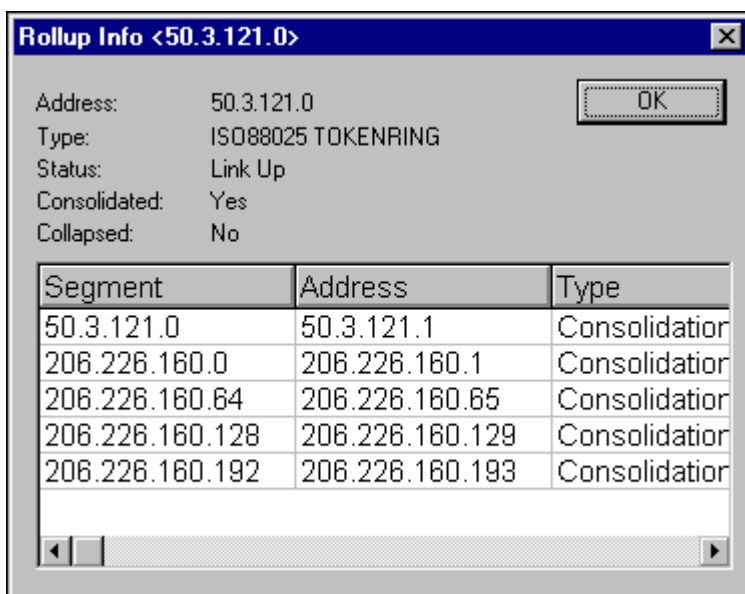


If we change the map option and turn Consolidate on, the same section of map now looks like this:

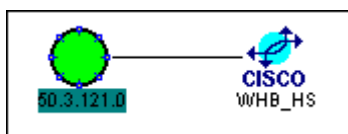


The seven icons have been reduced to two: matching the actual number of interfaces. The top Token Ring icon shows its sub-net address (50.3.121.0) on a green background, indicating that this is a consolidated segment icon.

To see the other segments that have been consolidated into one icon, right-click on the icon and choose **Subnet Info**. The Rollup Info screen will display the segments and addresses that are consolidated into the icon.



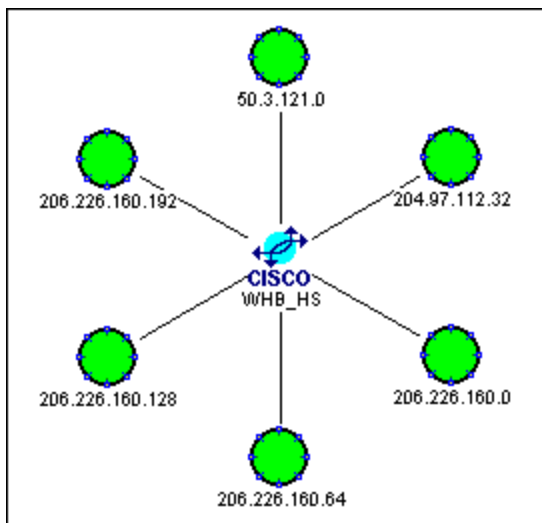
In addition, you can right-click on the consolidated icon and choose **Subnet**, which opens a subnet map for the segment. Note that here the Token Ring icon is still consolidated.



You can then expand the icon by right-clicking and selecting **Expand Subnet**, which opens an expanded subnet map, again showing all the sub-interfaces.

## The Internet Map

---



### Turning Consolidate on and off

The Consolidate option is turned on and off through the NavisAccess system options Internet tab. To change the option:

1. From the NavisAccess main menu, choose **Config > System Options**.
2. Click the Internet tab.
3. Select or de-select the Consolidate check-box as desired.
4. Click [OK] to apply the new setting. To view the new settings on the Internet Map, either close and reopen the map, or click the [Rescan from Database] button.

### Zooming in with submaps

Submaps allow you to view a selected portion of the full Internet Map. By selecting one or more devices, you can launch a second, smaller Internet Map containing only the selected devices and their segment icons. These submaps can then be saved. This is an effective way to break a large Internet map into several smaller segments.

Submaps encompass the full functionality of the Internet Map.

### To open a submap for one device:



1. Select (highlight) a device, then click the [Launch Sub Internet Map] button.

### To open a submap for multiple devices.

1. Drag-select a portion of the Internet Map, then click the [Launch Sub Internet Map] button.

## Alarm functions from the Map

When any component of the Map is licensed, Alarm Monitoring can be activated for it. A component can be monitored as part of a group, or as a single object.

### To launch the Alarm Monitor:



1. Highlight one or more devices in the map.
2. Click the [Alarm Monitor] button to launch the Alarm Monitor for all selected devices.

### To clear an alarm icon:

When an alarm is received, an alarm-bell icon is displayed over the device on the Internet map. To clear the icon:



1. Highlight a device with an alarm-bell icon over it.
2. Click the [Clear Alarm] button to remove the alarm icon.

### Viewing the Event Report

You can also access the Event Report for one or more devices. To do so:



1. Highlight one or more devices in the map.
2. Click the [View Event Report] button to launch the Event Report for all selected devices.

### Virtual Elements

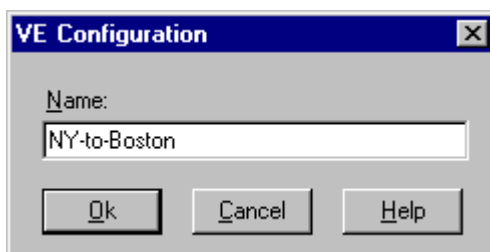
Virtual Elements represent dynamic groups of devices connected through either Frame Relay, X.25, or ISDN services. The Virtual Element is an icon in the Group Wizard that provides quick access to applications specific to the services and devices for which it is configured.

Virtual Elements can be created in the Internet Map wherever a services cloud icon is found.

### Configuring Virtual Elements

#### To configure a Virtual Element:

1. Right-click a services cloud icon in the Internet map and select **Configuration**. The Virtual Element Configuration window appears:



2. Enter a name for the virtual element. The name should be descriptive of the devices involved.
3. Click [OK]. The cloud icon in the Internet Map will be renamed with the name entered above. In the Group Wizard, a Virtual Element icon will appear, indicating the type of service and including the user-defined name. For example:



By right-clicking on the Virtual Element icon in the Group Wizard, you can launch applications specific to the devices that were used to created

the Virtual Element.











## Using Virtual Elements

There are four features available from a Virtual Element. To access these features, right-click on the Virtual Element icon. Available features are:








- **Circuit Map:** An Internet Map that displays individual circuits for Frame Relay, ISDN or X.25.
- **Configuration:** Used to create a Virtual Element or change the name of a Virtual Element.
- **Group Interface Table:** Displays interface information for each device associated with to the Virtual Element.
- **Top 10 Talkers:** Displays the ten busiest interfaces associated with the Virtual Element.

## Table of device icons

The following icons are used to represent devices in the Group Wizard and the Internet Map. For Digital Equipment devices, see the next section.







Device	Icon	Device	Icon
Ascend MAX Family		Ascend SA Broadband	
Ascend MAX TNT		3Com Router	
Ascend Pipeline Family		Cisco Router	
Ascend GRF Family		Cisco Switch	
Ascend B-STDx		Bay/Wellfleet Router	

## The Internet Map










Device	Icon	Device	Icon
Frame Relay			
Ascend CBX ATM		Novell MPR Router	
Generic Ascend icon		Generic symbol for non-SNMP device	
Windows NT Node		A host computer	
A server computer			

## Table of Digital Equipment device icons




The following icons are used to represent Digital Equipment devices in the Group Wizard and the Internet Map.

Icon	Digital Device	Icon	Digital Device
	Generic Digital Device icon. This icon is displayed when a device is identified as a Digital device, but no further information can be obtained. In most cases, a more precise icon is used.		DEC Gigaswitch
	DECswitch 900 EE		DEC Gigaswitch/ATM 14-slot DEC Gigaswitch/ATM 5-slot
	DECswitch 900 EF		DECbridge 90 DECbridge 900EE DECbridge 900MX DECbridge 90FL

## The Internet Map






















			RoamAbout
	DECswitch 900 ET		DECbrouter 90T1 DECbrouter 90T2 DECbrouter 90T2a
	RouteAbout Access EI		DECconcentrator 900FH DECconcentrator 900MX DECconcentrator 900TH
	RouteAbout Access TW		DEChub 90
	RouteAbout Access EW		DEChub 900
	RouteAbout Central EI		DECmau 900 <sup>TH</sup> DECmau 900TL
	RouteAbout Central EW		DECpacketprobe 90 DECpacketprobe 90+
	DECrepeater 900FL DECrepeater 900SL DECrepeater 900TL		DECwanrouter 90
	DECrepeater 900FP DECrepeater 900GM DECrepeater 900TM DECrepeater 90C DECrepeater 90FA DECrepeater 90FL DECrepeater 90FS DECrepeater 90T DECrepeater 90T+ DECrepeater 90T-16 DECrepeater 90TS		DECswitch 900EE DECswitch 900EF DECswitch 900FO PEswitch 900TX VNswitch 900AE VNswitch 900EE VNswitch 900FE VNswitch 900XE

The Internet Map

	PORTswitch 900CP PORTswitch 900FP PORTswitch 900TP		DECserver 900GM DECserver 900TM DECserver 90L DECserver 90L+ DECserver 90M DECserver 90TL
	DECpacketprobe 900RR		











## Segment icons - Internet Map

The following icons represent network segments on the Internet Map. There are three colors for each icon (green, red and yellow) representing up, down and degraded, respectively.

	Ethernet	Token Ring	FDDI	Frame Relay	X.25	ISDN	Serial, Point to Point
UP Green							
DOWN Red							
DEGRADED Yellow							

## Circuit icons - Internet Map

The following icons represent individual circuits for Frame Relay, X.25, ISDN and FDDI services on the Internet Map. There are three colors for each icon (green, red and yellow) representing up, down and degraded, respectively.

	Frame Relay	X.25	ISDN	FDDI
UP Green				
DOWN Red				
DEGRADED Yellow				

# Device Management: Configuration Tools

## 8

### Device Configuration: overview

A major component of network management is device configuration. This includes maintaining and keeping track of configuration files, updating software, tracking device chassis contents and more. NavisAccess provides the following tools to manage device configuration:

- **Configuration applet** - Used to edit device parameters, such as community strings and polling intervals, in the NavisAccess database.
- **Configure Router applet** - Used to download, store, edit and upload a device's configuration information. Also performs a differences operation, a line-by-line comparison of a downloaded file with a file stored in the configuration database.
- **Device software tools** - Used to upload and/or download software from devices. Available for Ascend, 3COM, Cisco and Bay/Wellfleet devices.
- **Ascend-specific tools** - There are two applets for Ascend devices:
- **System Reset** - Used to reset an Ascend MAX, MAX TNT or Pipeline device.
- **Radius Server applet** - Used to retrieve the remote configuration from the RADIUS server and update the selected parameters..
- **TFTP Server** - Used to monitor the status of TFTP downloads and uploads, maintain historical data about them, and set parameters such as maximum retry and timeout.
- **Telnet applet** - Uses the TCP/IP Telnet protocol to establish a terminal connection to the selected router.
- **Chassis Report** - Displays the hardware configuration for the device, such as slot numbers, slot types and slot contents.

---

## **The Configuration applet**

The **Configuration** applet is used to edit the parameters for a device which has been added to the database.

**To use the Configuration applet:**

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Configuration**. From the application view, right-click the Configuration icon and select **Configuration**. The Configuration window opens.

**Configuration**

Name: StonyBrook\_B3

Display Name:

IP Address: 150.50.23.254

Call Logging Secret:

Read Community Name:

Write Community Name:

Polling Interval: 60   Sec

Timeout: 1   Sec

Retries: 2

Comment:

**NOTE:** Novell MPR will not show the [Configure Device] button.

3. Enter a new Display Name if desired. By default, NavisAccess assigns the device system name (the name configured on the device) as the Display

Name. You can alter or add to the name if you wish. For example, you may want to identify a device as belonging to a particular office or region, so you might change device "ABC" to "ABC - Chicago office".

The Display Name has no impact on the device itself and will *not* change the system name.

4. Select an IP address. The IP Address combo box lists all IP addresses known for the device. An IP address can be selected (or changed) for monitoring.
5. Enter the Call Logging secret, Read and Write Community Names.

### **Call Logging Secret**

The keyword which enables NavisAccess to receive data from Ascend access devices (MAX, MAX TNT, Pipeline). This is not needed for other kinds of devices.

### **Read Community Name**

The password put into an SNMP get request.

### **Write Community Name**

The password put into an SNMP set request

To insure security, as characters are typed, asterisks will be displayed on the screen instead of the passwords themselves.

**NOTE:** The Call Logging Secret, Read and Write Community Names must match what is specified by (on) the device. Otherwise, communication cannot be established with the device.

6. Set Polling Interval, Timeout and Retry numbers.

### **Polling Interval**

The interval between each SNMP get request. The interval selected will also display in the Applet Parameters dialog box presented for most applets.

### **Timeout**

The amount of time the device will be polled.

### **Retries**

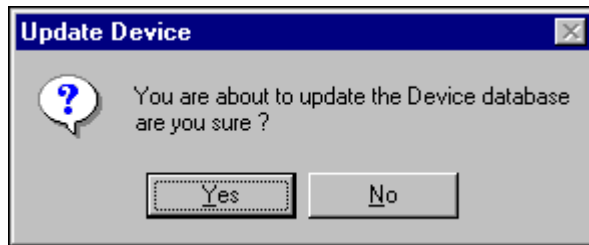
The number of times the SNMP get request will be made.

7. Enter text in the Comment field, if desired. The Comment box can be used to add any additional information you wish. It has no impact on the

device.

8. Click [OK] when done.

Any changes entered into the Configuration dialog box will prompt the following message:



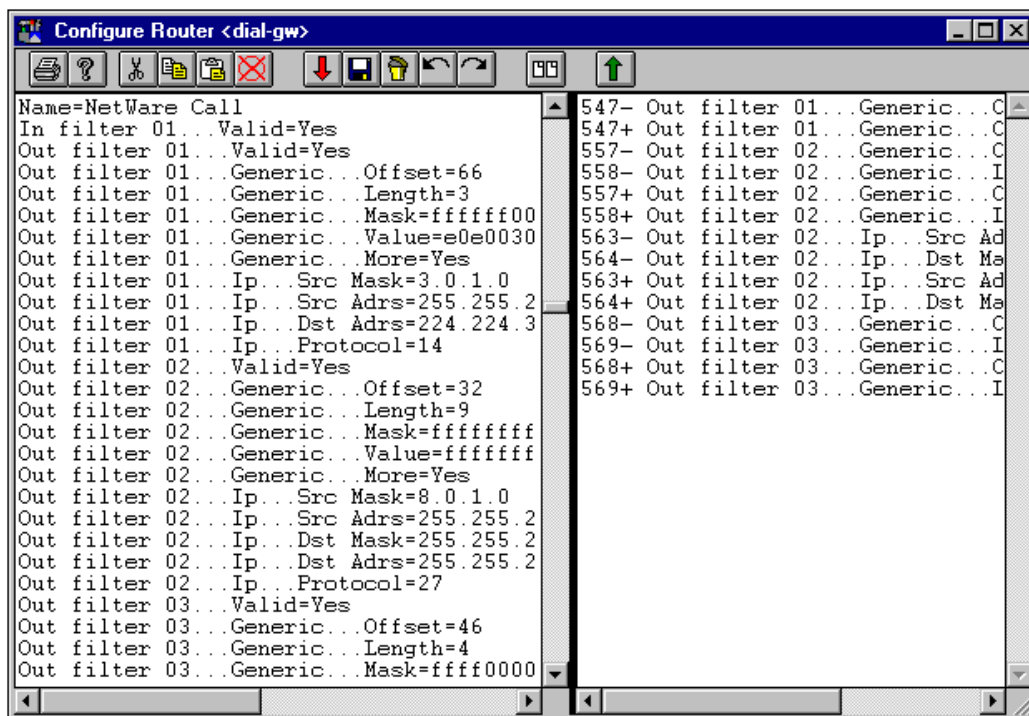
## The Configure Router applet

The **Configure Router** applet is used to download, store, edit and upload a router's configuration information. It is an easy-to-use substitute for Telnet sessions and error-prone command-line operations. In addition, the applet can perform a differences operation, a line-by-line comparison of a downloaded file with a file stored in the configuration database.

Other functions of the Configure Router applet are:

- Storing configuration files in the database for later retrieval or comparison.
- Exporting to an ASCII file.
- Importing from an ASCII file.

While the Configure Router applet is designed for one-device-at-a-time configuration, NavisAccess also performs multiple-device configuration. See the Schedule Wizard (page 213) for details.



**PRINTING NOTE:** To print a configuration file, click in the window pane you wish to print and then click the Print button.





## Starting the Configure Router applet

To start the Configure Router applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Configure Router**. From the logical view, right-click the Configuration icon and select **Configure Router**. The Configure Router window opens.
3. You may choose from the following operations:
  - Downloading a configuration file from a device

- Saving a configuration file in the NavisAccess database
- Deleting a configuration file from the NavisAccess database
- Retrieving a configuration file from the NavisAccess database
- Editing a configuration file
- Exporting a configuration file
- Importing a configuration file
- Comparing files: performing a Differences operation
- Uploading a configuration file
- Write a file to memory: Cisco routers only
- Erase a file from memory: Cisco routers only

In addition to the above operations, the following operations are available from the Configure Router toolbar:

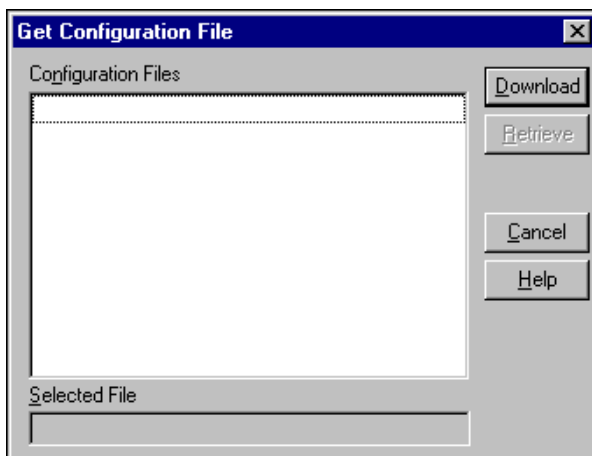
Button	Description
	<b>[Cut Text to Clipboard] button</b> Cut the currently selected text to the windows clipboard.
	<b>[Copy Text to Clipboard] button</b> Copy the currently selected text to the windows clipboard.
	<b>[Paste Text from Clipboard] button</b> Paste the text in the windows clipboard to the current insertion point.
	<b>[Clear Configuration] button</b> Clears text from the configuration screen.

## Downloading a configuration file from a device

This function downloads a configuration file from a device for viewing, saving or comparing.

### To download a configuration file:

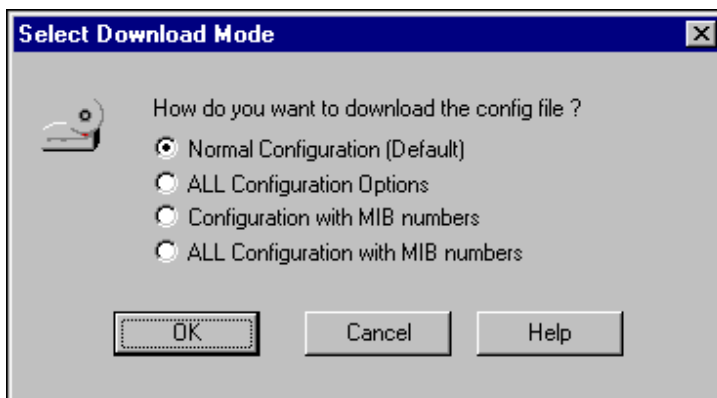
1. Open the Configure Router applet.
2. Click the [Retrieve Configuration File] button in the toolbar to open the Get Configuration File window.



3. Click on the [Download] button.

### Ascend devices only:

If you are downloading from an Ascend MAX, Pipeline or MAX TNT device, the Select Download Mode options window appears:



Select one of the following options. **Please read all options before**

selecting.

**Normal Configuration**

Downloads the configuration file with details only for parameters that have been set by the user. The file is presented in user-readable format, that is, parameters listed as text.

**ALL Configuration Options**

Downloads the configuration file with details for all parameters, including default parameters (i.e., parameters that have not been set by the user). This option will typically download a far larger file and take more time.

**Configuration with MIB numbers**

Same as Normal Configuration download, but file is presented with MIB numbers, rather than user-readable. That is, parameters are displayed with MIB numbers, rather than text entries. For example, a normal download may show a parameter as "Active=Yes," while a MIB number download would present it as "65.2=Yes". This format is designed for machine processing, rather than user-readability.

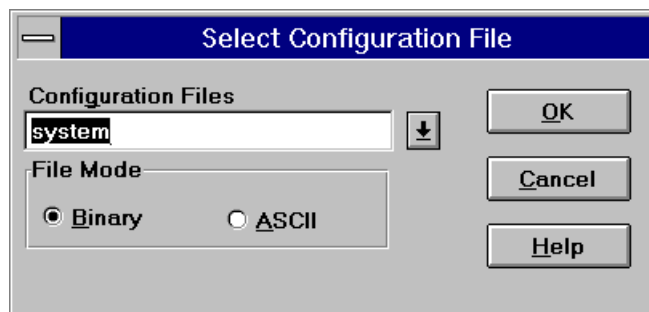
**ALL Configuration with MIB numbers**

Downloads with all parameters, and displays MIB numbers.

**NOTE:** A MIB download should be used for upgrading Ascend devices. This is because text entries may change between configuration files and cause file incompatibilities. MIB numbers will not change and will be properly processed by the device.

For a visual comparison of download options, see "Select Download Mode options window" in the next section.

4. If applicable, the Select Configuration File dialog box will appear asking for the name of the configuration file on the device.



## Device Management

---

5. Select File Mode of ASCII or Binary.

Wellfleet/Bay 5.XX will have a save as default button on the bottom of the screen.

6. Type or highlight the correct file name and click on the [OK] button.

The download process will begin. When complete, the configuration file will appear in the left-hand pane of the Configure Router applet when it can be edited, saved and/or uploaded.

File downloads are performed through the TFTP server.

### Select Download Mode options window

There are four options available when downloading configuration files from Ascend devices (MAX, MAX TNT and Pipeline).

**Please read all options before selecting.**

Following is a visual comparison of download types:

Normal Configuration	
Note that unset (default) parameters are displayed only as START and END points. For example, the first parameter of SAPFILT shows only <b>START=SAPFILT=200=0</b> and <b>END=SAPFILT=200=0</b> . None of the intervening parameters are displayed. See below for a comparison with the ALL option.	
Note also that defined parameters are displayed in full, such as Name=domestic-frame.	
	<div>START=SAPFILT=200=0 END=SAPFILT=200=0 START=SAPFILT=200=1 END=SAPFILT=200=1 START=IPXROUTE=200=0 END=IPXROUTE=200=0 START=IPXROUTE=200=1 END=IPXROUTE=200=1 START=FRELAY=200=0 Name=domestic-frame Active=Yes Data Svc=56KR Link Mgmt=T1.617D END=FRELAY=200=0</div>

<p><b>ALL Configuration Options</b></p> <p>Here all the possible values are displayed. Note that the SAPFILT parameter now displays many specific parameter options between the START and END points, and all are blank or set to 0 (i.e. because they have not been user-defined).</p>	<pre>START=SAPFILT=200=0 Name= In SAP filter 01...Valid=No In SAP filter 01...Type=Exclude In SAP filter 01...Server Type=0000 In SAP filter 01...Server Name= In SAP filter 02...Valid=No In SAP filter 02...Type=Exclude In SAP filter 02...Server Type=0000 In SAP filter 02...Server Name= Out SAP filter 01...Valid=No Out SAP filter 01...Type=Exclude Out SAP filter 01...Server Type=0000 Out SAP filter 01...Server Name= Out SAP filter 02...Valid=No Out SAP filter 02...Type=Exclude Out SAP filter 02...Server Type=0000 Out SAP filter 02...Server Name= END=SAPFILT=200=0</pre>
<p><b>Configuration with MIB numbers</b></p> <p>This displays the same information as a Normal Configuration download, but the parameters are listed with MIB numbers rather than as user-readable text. For example, the parameter listed here as <b>65.2=Yes</b> is displayed in the normal download as <b>Active=Yes</b>.</p>	<pre>START=SAPFILT=200=0 END=SAPFILT=200=0 START=SAPFILT=200=1 END=SAPFILT=200=1 START=IPXROUTE=200=0 END=IPXROUTE=200=0 START=IPXROUTE=200=1 END=IPXROUTE=200=1 START=FRELAY=200=0 65.1=domestic-frame 65.2=Yes 65.7=56KR 65.11=T1.617D END=FRELAY=200=0</pre>

## Device Management

<b>ALL Configuration with MIB numbers</b> <p>This option displays a full download with MIB numbers. In other words, it is a combination of the "ALL Configuration Options" and "Configuration with MIB Numbers" choices.</p> <p>For comparison purposes, note for example that the <b>In SAP filter 01...Valid=No</b> parameter seen in "ALL Configuration Options" is here displayed as <b>1 : 53. 2, 52.1=No</b>.</p>	<pre>START=SAPFILT=200=0 53.1= 1:53.2.52.1=No 1:53.2.52.2=Exclude 1:53.2.52.3=0000 1:53.2.52.4= 2:53.2.52.1=No 2:53.2.52.2=Exclude 2:53.2.52.3=0000 2:53.2.52.4= 1:53.3.52.1=No 1:53.3.52.2=Exclude 1:53.3.52.3=0000 1:53.3.52.4= 2:53.3.52.1=No 2:53.3.52.2=Exclude 2:53.3.52.3=0000 2:53.3.52.4= END=SAPFILT=200=0</pre>
---	--

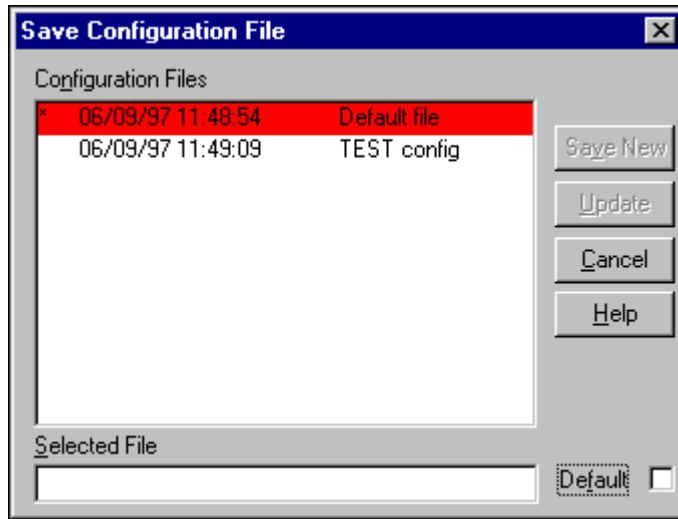
## Saving a configuration file

Configuration files can be saved to the database, either as originally downloaded, or after changes have been made.

### To save a configuration file:

1. Download a file from a device.
2. Click the [Save Configuration File] button on the toolbar.
3. Enter up to 30 characters to describe the configuration file. It will be saved under this name and displayed in the Configuration Files List.





4. To specify this as the default configuration file, click on the Default box in the lower right-hand corner of the dialog box. *There can be only one default configuration file at a time, and it is displayed in red, preceded by an asterisk.* Attempting to create a new default file when one already exists will trigger a prompt asking for confirmation and a warning that the old file will be over-written.
5. If applicable, the [Update] button will be available on the right hand side of the Save Configuration File dialog box. Select the desired file to make changes to, and press on the [Update] button. The file will appear in the Configuration Device edit space. When the edits (changes) are completed, press on the [Save] button, and then on the [Update] button to update the configuration file.

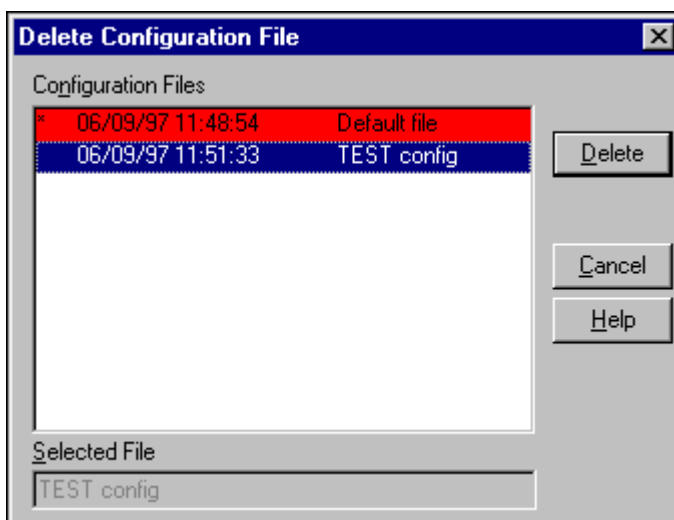
### Deleting a configuration file from the database

Any configuration file saved in the configuration database can be deleted.

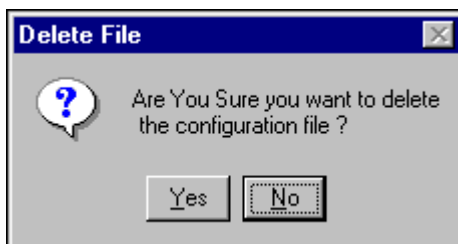
#### To delete a file:



1. Click the [Delete Configuration File] button in the Configure Router applet to display the Delete Configuration File dialog box:



2. Select the desired file to be deleted from the list displayed. It will appear in gray in the Selected File edit space.
3. Click the [Delete] button to remove the selected configuration file, or click the [Cancel] button to abort the operation.
4. The following message displays for confirmation of the operation.



5. Click [Yes] to delete the file.

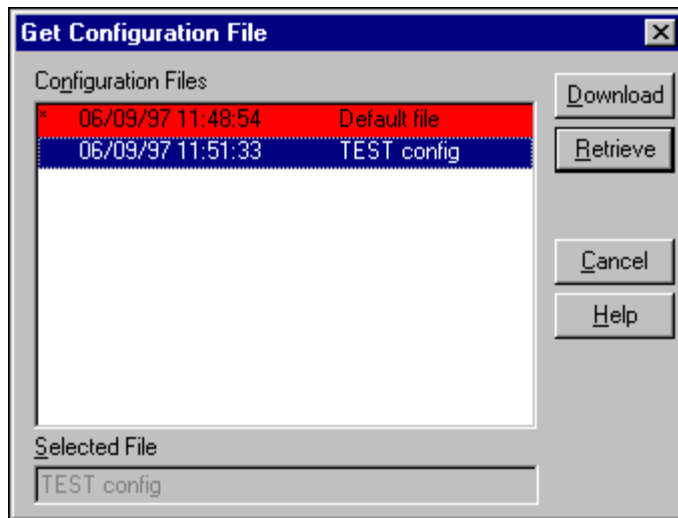
## Retrieving a configuration file from the database

You can retrieve a configuration file from the NavisAccess database in order to view it in the Configure Router edit window.

### To retrieve a file:



1. Click on the [Retrieve Configuration File] button in the Configure Router applet toolbar.
2. Select the desired file in the Configuration Files list.



3. Click on the [Retrieve] button to retrieve the file from the configuration database. Or, click on the [Cancel] button to exit.

Once the configuration file has been retrieved, it is displayed in the edit workspace area of the Configure Router applet.

## How to edit a configuration file

Once the file is displayed in the Configure Router edit workspace, it can be edited. The workspace uses standard Windows editing keys.

## Device Management

---

These are:

### Cursor Movement Keys

The following keys move the cursor or insertion point in the edit workspace:

Press	To Move
<b>UP ARROW</b>	Up one line
<b>DOWN ARROW</b>	Down one line.
<b>RIGHT ARROW</b>	Right one character.
<b>LEFT ARROW</b>	Left one character.
<b>CTRL+RIGHT ARROW</b>	Right one word.
<b>CTRL+LEFT ARROW</b>	Left one word.
<b>HOME</b>	To the beginning of the line.
<b>END</b>	To the end of the line.
<b>PAGE UP</b>	Up one screen.
<b>PAGE DOWN</b>	Down one screen.
<b>CTRL+HOME</b>	To the beginning of the document
<b>CTRL+END</b>	To the end of the document.

### Text Editing Keys

The following keys edit text in the edit workspace:

Press	To
<b>BACKSPACE</b>	Delete the character to the left of the insertion point. Or delete selected text.
<b>DEL</b>	Delete the character to the right of the insertion point. Or delete selected text.
<b>CTRL+INS, CTL+C</b>	Copy the selected text and place it into the Clipboard.
<b>SHIFT+DEL, CTL+X</b>	Delete the selected text and place it onto the Clipboard
<b>SHIFT+INS, CTRL+V</b>	Paste text from the Clipboard into the active window.
<b>CTRL+Z, ALT+BKSPACE</b>	Undo the last editing action.

### Text Selection Keys

The following keys select text in the edit workspace. All of the following selections begin at the insertion point. Once the text has been selected, pressing the same key cancels the selection:

Press	To Select
<b>SHIFT+LEFT or RIGHT ARROW</b>	One character at a time to the left or right.
<b>SHIFT+UP or DOWN ARROW</b>	One line of text up or down.
<b>SHIFT+PAGE UP</b>	All text, one screen up.
<b>SHIFT+PAGE DOWN</b>	All text, one screen down.
<b>SHIFT+HOME</b>	Text to the beginning of the line.
<b>SHIFT+END</b>	Text to the end of the line.

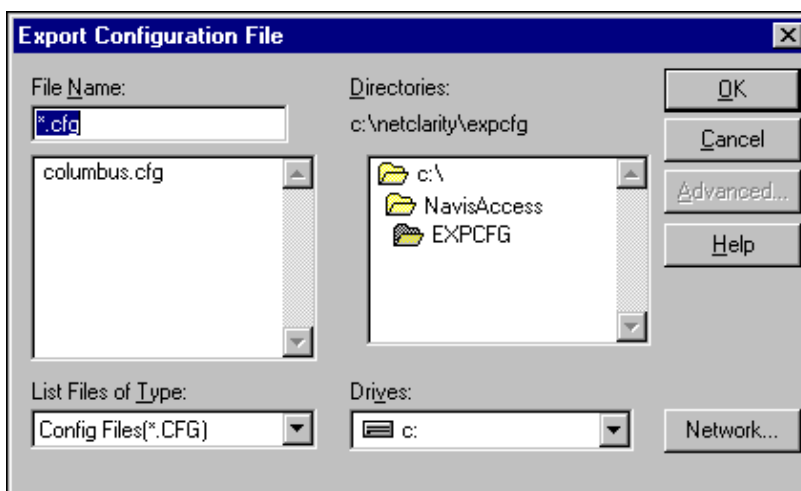
<b>CTRL+SHIFT+LEFT ARROW</b>	The previous word.
<b>CTRL+SHIFT+RIGHT T ARROW</b>	The next word.
<b>CTRL+SHIFT+HOME</b>	Text to the beginning of the document.
<b>CTRL+SHIFT+END</b>	Text to the end of the document.

### Exporting a configuration file

The configuration file displayed in the Configure Router applet can be exported to an ASCII file.

#### To export the configuration file to an ASCII file:

1. With a file opened in the edit workspace, click the [Export Configuration File] button.
2. In the Export Configuration File window, enter a unique name in the File Name edit space (change the file extension if desired).



3. In the Directories space, specify the destination path for the file to be saved. By default, files are saved to the EXPCFG directory under the NavisAccess home directory.

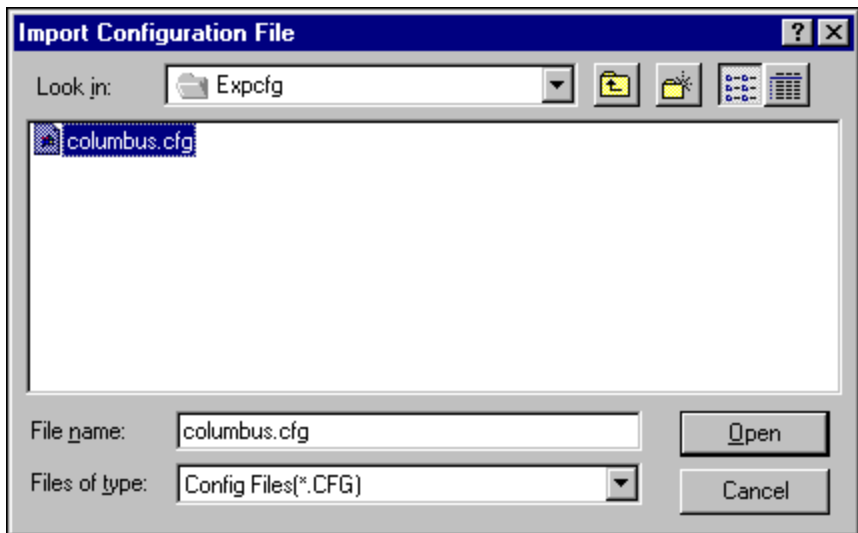
4. Click on the [OK] button to export the file.

## Importing a configuration file

Any ASCII file can be imported into the Edit Workspace.

### To import an ASCII file into the edit workspace:

1. After clearing the edit workspace, click the [Import Configuration File] button.
2. Select the desired configuration file from those listed in the Import Configuration File dialog box.



3. Click on the [OK] button to import the ASCII file or double-click on the file name.

## Comparing files: performing a differences operation

The Differences feature allows for comparison of two configuration files. Files can either be downloaded from a device or retrieved from the NavisAccess database.

The first file downloaded or retrieved is displayed in the left-pane of the

window. The second file used for comparing will not be displayed. Rather, the differences between the first and second file are displayed in the right-pane.

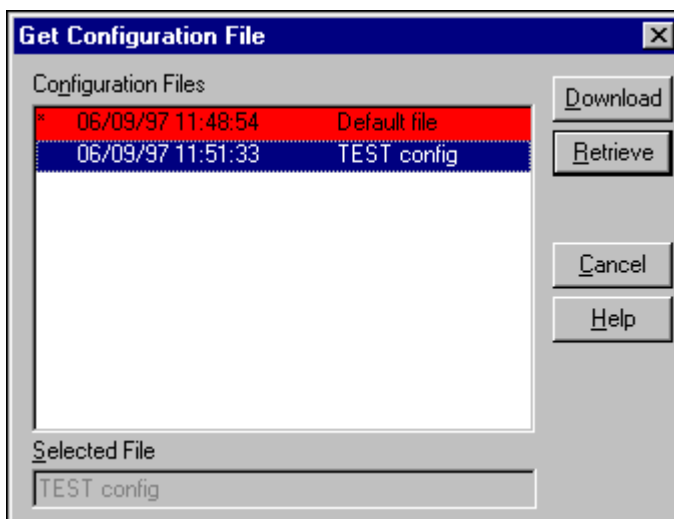
All comparisons are measured from the primary configuration file. The information displayed contains what needs to be done to transform the primary configuration file into the secondary configuration file. A minus (-) sign identifies a line from the primary configuration file (i.e., a line that does not match the secondary file). A plus (+) sign identifies a line from the secondary file (i.e., the primary file must be changed to match this setting).

The number in front of the plus or minus signs indicates the line number in the configuration file.

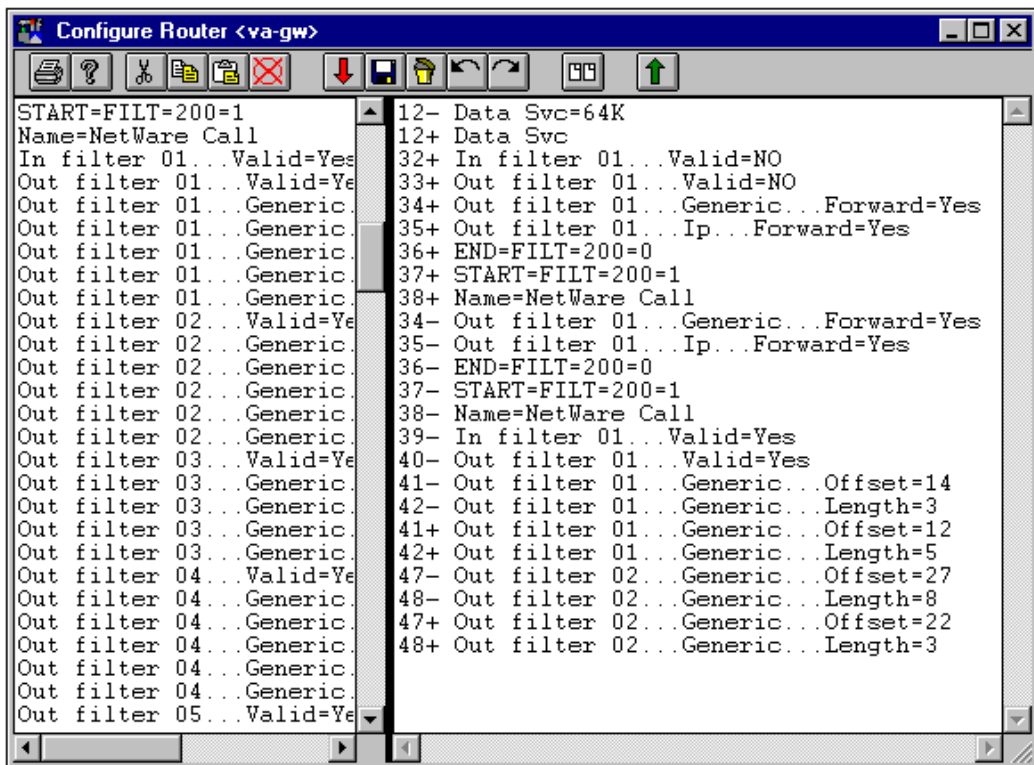
Text can be copied and pasted between the Differences Space and Edit Workspace using either the toolbar or the editing keys which are described in "How to edit a configuration file" (page 169).

### To perform a Differences operation:

1. Download or retrieve a file into the primary window (left-pane) of the Configure Router applet.
2. With the primary file displayed in the left-pane, click on the [Perform Differences Operation] button to display the Get Configuration File dialog box



3. To download the file currently on the device, click [Download]. To retrieve the file from the NavisAccess database click [Retrieve]. When the download or retrieve is complete, the differences between the primary and secondary file will be displayed.



You may continue to perform differences operations using alternate secondary files.

### Comparing files from different devices

You may want to compare a configuration file from one device with a file from another. To do this, one of the files must be downloaded/retrieved and then exported to a directory. This file must then be imported into the left-pane of the Configure Router window. From this point, follow the procedures outlined above.

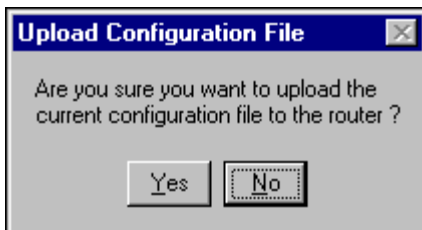
### Uploading a configuration file

This function sends the configuration file displayed in the edit workspace to the device. The file uploaded becomes the active device configuration file. Uploads are performed using the TFTP Server.

**Note for Cisco routers:** While the uploaded configuration file will become active, it will not survive a device reboot unless it is written to memory. See "Write Memory: Cisco Specific" for details.

#### To Upload the configuration file:

1. Open the desired file in the left-pane of the Configure Router applet.
2. Click on the [Upload Configuration File] button.
3. Confirm the decision in the prompt box shown below:



4. Click the [Yes] button to upload the file, or click on the [No] button to end the operation.

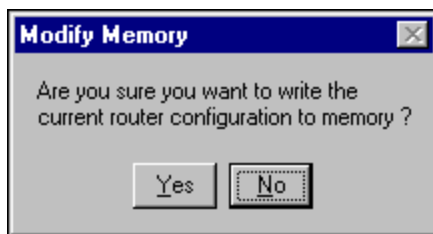
**NOTE:** Make certain you are uploading the correct file before proceeding with the upload operation. An incorrect file can adversely affect the network (device) operation.

## Cisco specific tools

### Write Memory: Cisco specific

**NOTE:** This feature is only available for Cisco routers.

Changes made to a Cisco router's configuration become active immediately; however, they will not survive a reboot of the device. In order for the changes to become permanent, they must be written to the device's non-volatile memory. Clicking on the [Write Configuration File] button in the Configure Router applet toolbar makes the configuration changes permanent. When the [Write Configuration File] button is pressed, a message is displayed asking for confirmation of the operation.



Click the [Yes] button to write the changes made to the device's configuration file to non-volatile memory. To abort the operation, click on the [No] button.

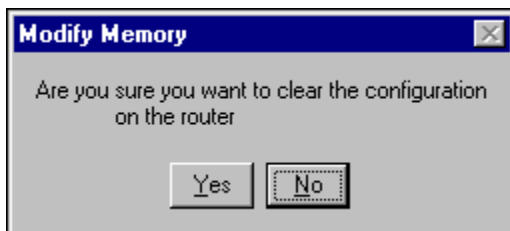
### Erase Memory: Cisco specific

**NOTE:** This feature is only available for Cisco routers.

It is possible to clear the contents of the Cisco router's non-volatile memory. Clicking on the [Erase Configuration File] button in the Configure Router applet toolbar erases the device's non-volatile memory. When the button is pressed, a message is displayed asking for confirmation of the operation.

## Device Management

---



Click the [Yes] button to erase the device's non-volatile memory. To abort the operation click on the [No] button.

**NOTE:** Be certain that another image is going to be uploaded immediately, because if the device reboots, it will have no bootable image.

## **Device software tools**

### **Binary Image applet: Ascend specific**

The **Binary Image** applet uploads software to Ascend MAX, MAX TNT and Pipeline devices, making error-prone Telnet sessions unnecessary.

In addition, following the upload the device is reset, and then it is polled to verify that the upload and reset was successful. Upon completion, a status message is delivered to the console, and an event (with date and time stamp) is posted to the Event Viewer.

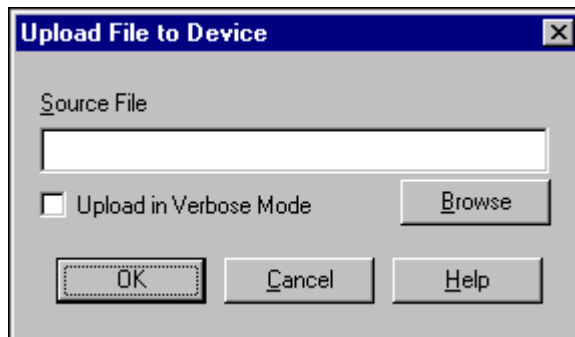
#### **Automating software updates**

Binary Image uploads can be scheduled to be performed on multiple devices in succession. For details, see "Creating an Image Uploader schedule" on page 235.

### **Using the Binary Image applet**

#### **To start the Binary Image applet:**

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, click on a blank area of the screen and select **Binary Image > Binary Image Upload**. From the application view, right-click the Binary Image icon and select **Binary Image Upload**. The Upload File to Device window opens.



## Device Management

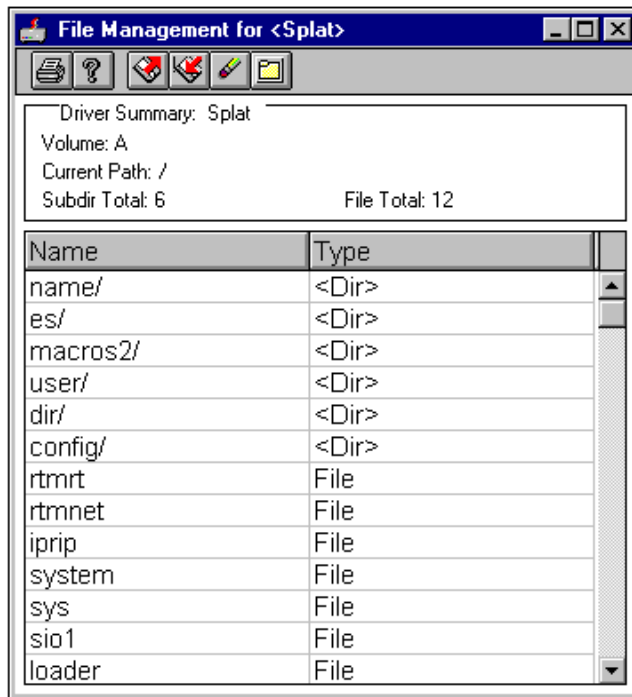
---

3. Enter the name and location of the file to be uploaded to the device in the Source File window. Pressing the [Browse] button displays the standard file Browse dialog box, which allows for easy selection of the file.
4. Choose the Upload in Verbose Mode option to generate detailed Event Viewer messages.
5. Click [Ok] to start the file transfer.

## The File Manager applet: 3Com specific

The **File Manager** applet displays a list of files and directories in the device's file system. 3Com supports downloading, uploading and deleting of files using this applet. Downloads and uploads are performed using the TFTP Server.

The top pane contains a directory summary displaying information about the entire file system. The bottom pane contains a table with all the directories and files in the device's file system.



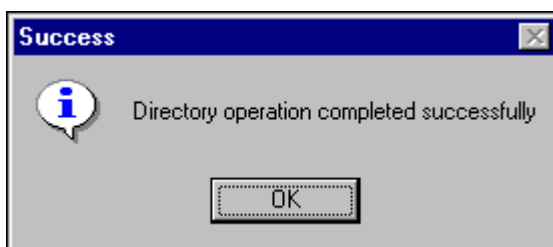
## Using the File Manager applet

The File Manager for 3Com can be used to download, upload or erase a file from the floppy disk.

**To start the File Manager applet:**

1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click the File Manager icon and select **File Manager**. The File Manager window opens.

Initially, the contents (name and type) are being updated, and are not in view. As the update is completed, the following message appears:

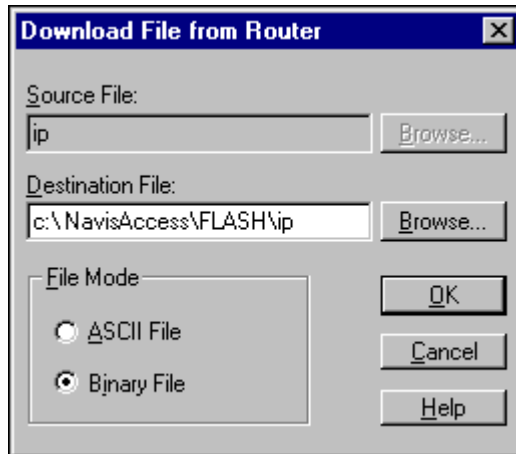


### To change a directory:

1. To change the current directory, double-click on a directory entry (Type Dir). The contents of the list will be updated with the new directory information. In addition, the Current Path field displayed at the top of the File Manager applet will reflect the newly displayed directory.

### To download a file:

1. Select the desired file to download from the list displayed in the bottom pane of the 3Com File Manager applet.
2. Click on the [Download] button on the toolbar. The Download File from Router dialog box displays:



The following fields are displayed:

**Source File**

Contains the file name to transfer from the device's file system to the PC. The Source File edit space is automatically filled in with the file name (the full path information is stripped off). The [Browse] button is not available for the Source File edit space.

**Destination File**

Contains the name and location of the file to be written to the PC. Pressing the [Browse] button displays the standard file Browse dialog box, which allows for easy selection of the destination directory. This field can be accessed and renamed.

**File Mode**

Selects the file type to transfer. If the file being transferred is binary, select the Binary File radio button. Otherwise select the ASCII File radio button.

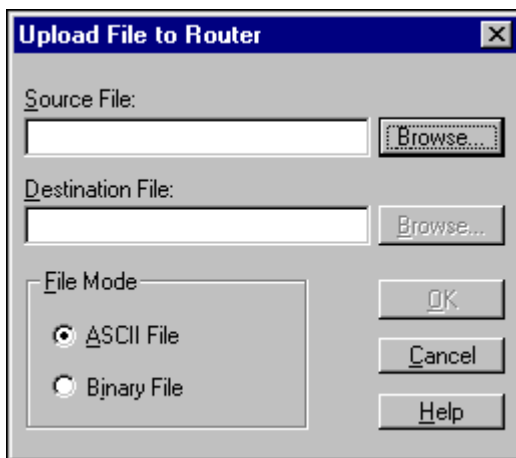
It is important to select the correct File Mode field. Transferring a Binary File with File Mode set to ASCII File will corrupt the contents of the file, and vice-versa.

**NOTE:** See "The TFTP Server" on page 197 for details on configuring the file transfer process and gathering file transfer statistics.

### To upload a file:

Any file on the PC can be uploaded to the device's floppy disk.

1. Click the [Upload File] button on the File Manager applet toolbar.

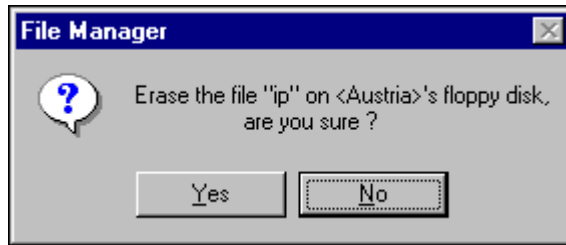


2. Select the Source file on the PC to transfer.
3. Select the Destination File name.
4. Select the proper File Mode.
5. Click on the [OK] button to start the TFTP operation. Or, click on the [Cancel] button to abort the operation.

### To erase a file:

Any file on the device's floppy disk can be deleted.

1. Select the desired file from the list displayed at the bottom of the File Manager applet.
2. Click the [Erase File] button on the toolbar. A message is displayed asking for confirmation to delete the file.



3. Click the [Yes] button to delete the file on the device's file system, or click the [No] button to cancel the operation.

### Rescanning a directory:

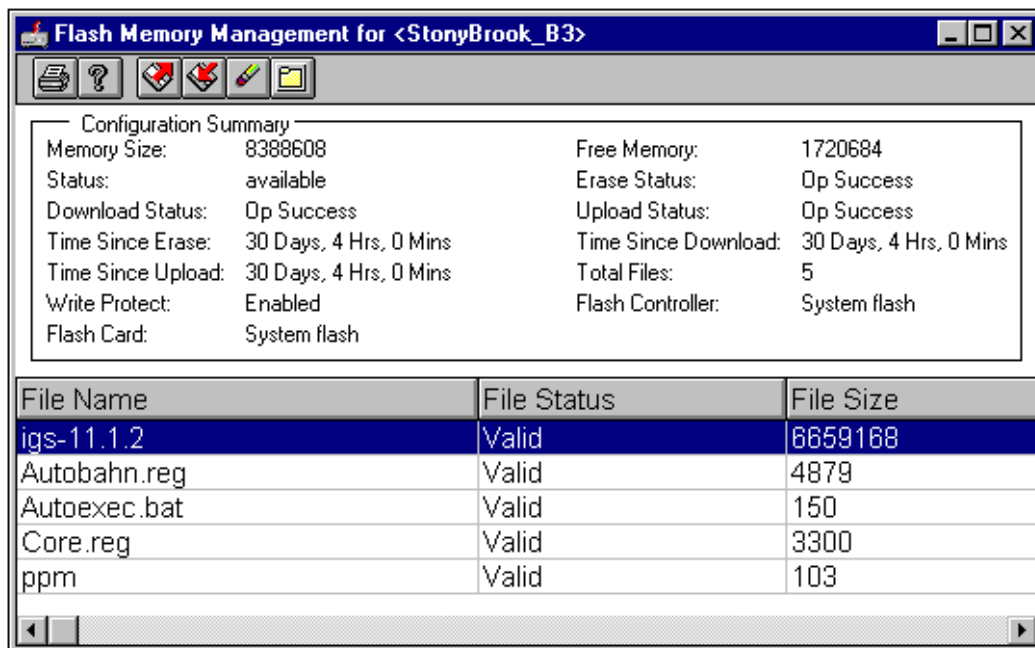
At times the device's file directory may need to be rescanned.

1. Click on the [Directory] button. The contents of the directory window will be refreshed.

## The Flash Manager applet: Cisco specific

The **Flash Manager** applet displays a list of files in the device's flash file system. This applet is only available for devices which have flash memory installed. Files can be uploaded and downloaded using this applet. The top pane contains a directory (summary) displaying information about the entire file system. The bottom pane contains a table with all the files in the Device's file system.

## Device Management



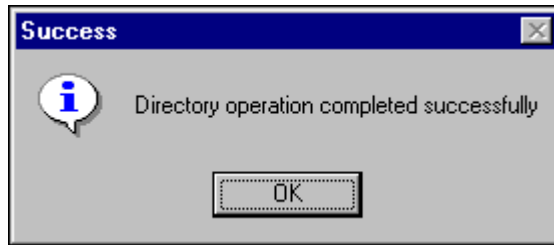
### Using the Flash Manager applet: Cisco specific

The Flash Manager for Cisco can be used to download or upload a file, and to erase the flash memory system.

#### To start the Flash Manager applet:

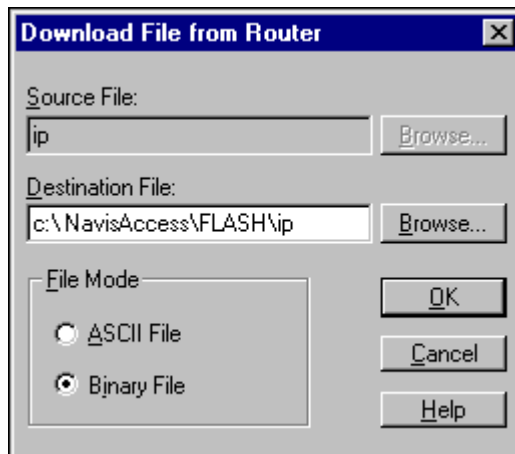
1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Flash Manager > Flash Manager**. From the application view, right-click the Flash Manager icon and select **Flash Manager**. The Flash Memory Management window opens.

Initially, the contents (name and type) are being updated, and are not in view. As the update is completed, the following message appears:



**To download a file:**

1. Select the desired file to download from the list displayed in the bottom pane of the Flash Manager applet.
2. Click on the [Download] button on the toolbar. The Download File from Router dialog box displays:



The following fields are displayed:

**Source File**

Contains the file name to transfer from the device's file system to the PC. The Source File edit space is automatically filled in with the file name (the full path information is stripped off). The [Browse] button is not available for the Source File edit space.

**Destination File**

Contains the name and location of the file to be written to the PC. Pressing the [Browse] button displays the standard file Browse dialog box,

which allows for easy selection of the destination directory. This field can be accessed and renamed.

### File Mode

Selects the file type to transfer. If the file being transferred is binary, select the Binary File radio button. Otherwise select the ASCII File radio button.

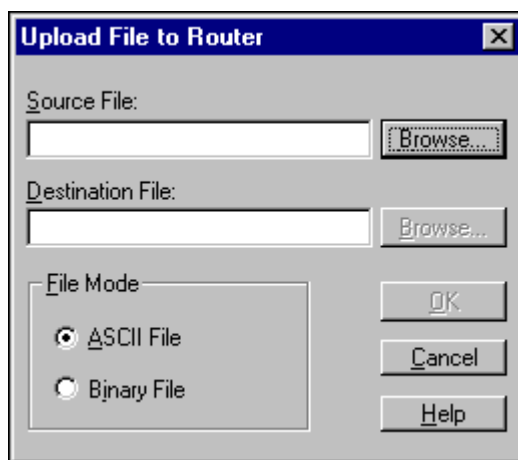
It is important to select the correct File Mode field. Transferring a Binary File with File Mode set to ASCII File will corrupt the contents of the file, and vice-versa.

**NOTE:** See "The TFTP Server" on page 197 for details on configuring the file transfer process and gathering file transfer statistics.

### To upload a file:

Any file on the PC can be uploaded to the device's flash file system.

1. Click the [Upload File] button on the Cisco Flash Memory Management applet toolbar.



2. Select the Source file on the PC to transfer.
3. Select the Destination File name.
4. Select the proper File Mode.
5. Click on the [OK] button to start the TFTP operation. Or, click on the [Cancel] button to abort the operation.

### To erase flash memory:

The entire Flash File System on the device can be erased. This operation clears out any entries currently stored in the Device's Flash File memory.

**This operation should only be performed if a new program image is going to be uploaded immediately, because if the device reboots, it will have no bootable image.**

1. Click the [Erase Flash Memory] button on the Cisco Flash Memory Management applet toolbar. A message is displayed asking for confirmation to delete the device's flash file system:



2. Click the [Yes] button to erase the flash file system, or click [No] to cancel the operation.

### Rescanning a directory:

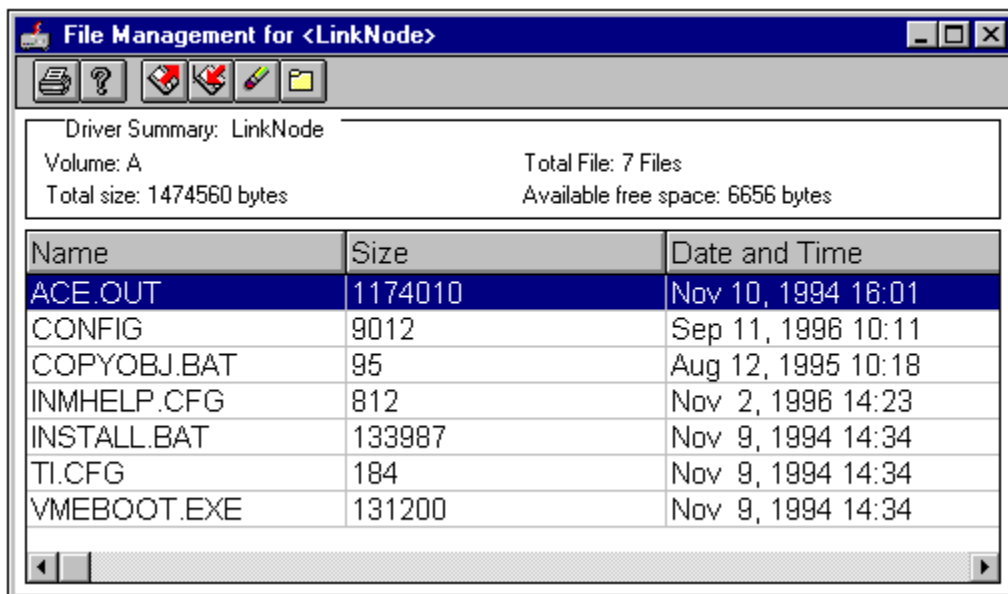
At times the device's file directory may need to be rescanned.

1. Click on the [Get Directory] button. The contents of the directory window will be refreshed.

### The File Manager applet: Bay/Wellfleet specific

The **File Management** applet displays a list of files in the device's file system. Files can be uploaded, downloaded and deleted using this applet. In addition, flash memory can be formatted. Downloads are performed using the TFTP Server.

The top pane contains a directory summary displaying information about the entire file system. The bottom pane contains a table with all the files in the device's file system.



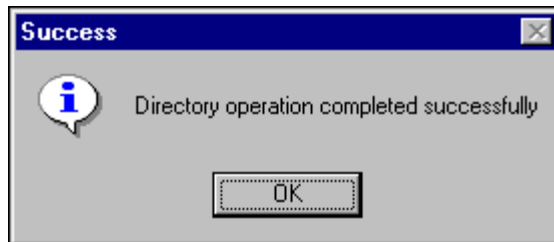
**NOTE:** Specialized toolbar buttons will vary with type of Wellfleet/Bay router and software installed on the router.

## Using the File Manager applet: Bay/Wellfleet specific

### To start the File Manager applet:

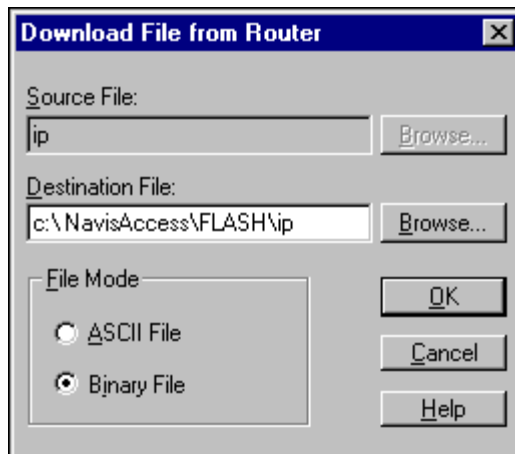
1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click the File Manager icon and select **File Manager**. The File Management window opens.

Initially, the contents (name and type) are being updated, and are not in view. As the update is completed, the following message appears:



### To download a file:

1. Select the desired file to download from the list displayed in the bottom pane of the File Manager applet.
2. Click on the [Download] button on the toolbar. The Download File from Router dialog box displays:



The following fields are displayed:

### **Source File**

Contains the file name to transfer from the device's file system to the PC. The Source File edit space is automatically filled in with the file name (the full path information is stripped off). The [Browse] button is not available for the Source File edit space.

### **Destination File**

Contains the name and location of the file to be written to the PC. Pressing the [Browse] button displays the standard file Browse dialog box, which allows for easy selection of the destination directory. This field can be accessed and renamed.

### **File Mode**

Selects the file type to transfer. If the file being transferred is binary, select the Binary File radio button. Otherwise select the ASCII File radio button.

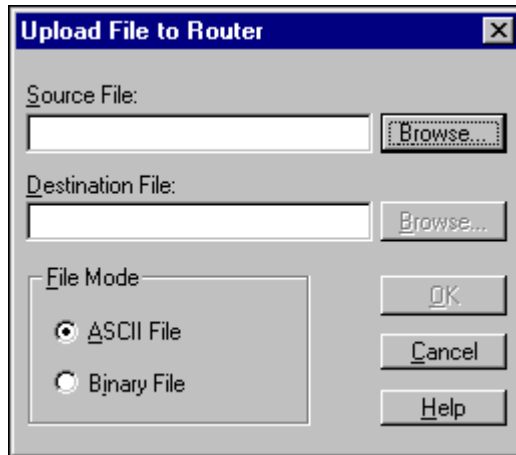
It is important to select the correct File Mode field. Transferring a Binary File with File Mode set to ASCII File will corrupt the contents of the file, and vice-versa.

**NOTE:** See "The TFTP Server" on page 197 for details on configuring the file transfer process and gathering file transfer statistics.

### **To upload a file:**

Any file on the PC can be uploaded to the device's file system.

1. Click the [Upload File] button on the File Manager applet toolbar.



2. Select the Source file on the PC to transfer.
3. Select the Destination File name.
4. Select the proper File Mode.
5. Click on the [OK] button to start the TFTP operation. Or, click on the [Cancel] button to abort the operation.

**To erase a file:**

Any file on the device's file system can be deleted.

1. Select the desired file from the list displayed at the bottom File Manager applet.
2. Click the [Erase File] button on the toolbar. A message is displayed asking for confirmation to delete the file.
3. Click the [Yes] button to delete the file on the device's file system, or click the [No] button to cancel the operation.

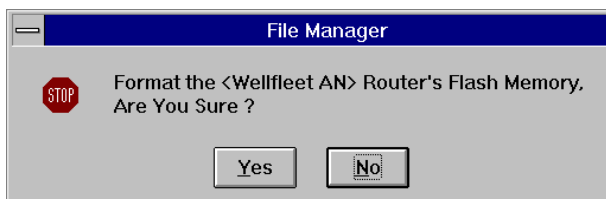
### Rescanning a directory:

At times the device's file directory may need to be rescanned.

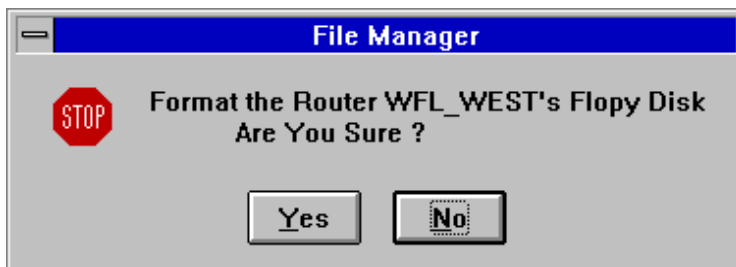
1. Click on the [Directory] button. The contents of the directory window will be refreshed.

### To format flash memory:

The [Format Device] button may include the following message which indicates that the entire Flash Memory on the device will be formatted. **This operation should only be performed if a new program image is going to be uploaded immediately, because if the device reboots, it will have no bootable image.**



On VME routers, it might be necessary to create a new distribution disk. First, format a floppy disk by clicking on the [Format Router] button. (This option is only available to VME systems. All other systems will reject the format command.) When the [Format Router] button is pressed a message is displayed asking for confirmation of the format operation:



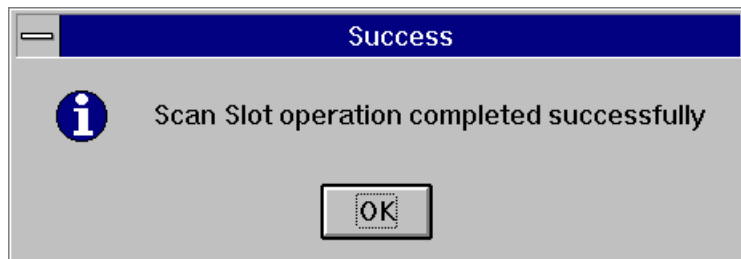
Press [Yes] to complete the format or [No] to abort.

**To compact the file system:**

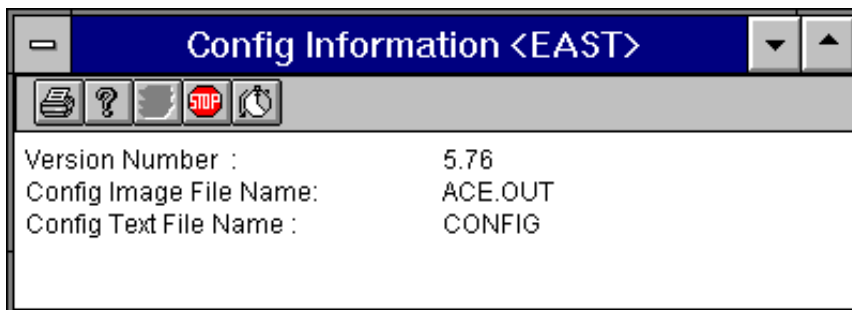
This feature is used to defragment the files in Wellfleet/Bay Flash Memory to maximize the amount of contiguous file space. This feature is used when a directory of the Flash Memory indicates that there is enough room to write a file to Flash, but writing the file is unsuccessful. Compacting the Router's Flash Memory may free the necessary space to write the file to Flash.

**Rescanning the Slot**

This feature is used to allow the user to move between slots on Wellfleet/Bay routers with multiple slots. When the user moves to a new slot, that slot is scanned and displays the file contents of the slot.

**Configuration Information for Wellfleet/Bay 5.XX**

Only with Wellfleet/Bay 5.XX software, on the boxmap toolbar is a [Get Configuration Information] button. Pressing on this button presents the Configuration Information screen:



Configuration information includes the software version number, config image file name, and config text file name.

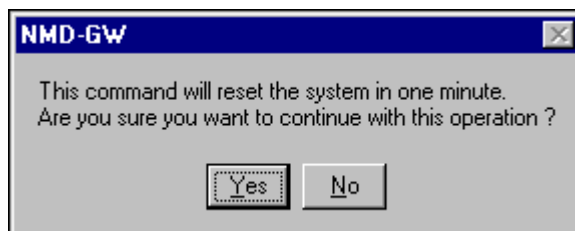
### System reset - Ascend devices

The **System Reset** applet lets you reset an Ascend MAX, MAX TNT or Pipeline device.

#### To reset a device:

1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click the Configuration icon and select **System Reset**. From the Physical View, right-click a blank area of the screen and select **Configuration > System Reset**.

A warning message similar to the following will appear:



The system reset will take place one minute after selecting [Yes].

### Radius Server applet - Ascend devices

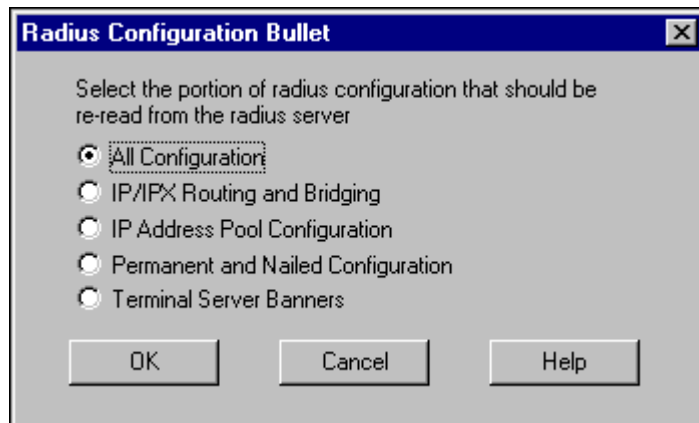
The **Radius Server** applet retrieves the remote configuration from the RADIUS

server and updates the selected parameters. This allows you to update the device whenever changes are made to the RADIUS server files.

### To update the RADIUS configuration:

1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click the Configuration icon and select **Radius Server**. From the Physical View, right-click a blank area of the screen and select **Configuration > Radius Server**.

The Radius Configuration screen appears:



Available options are:

#### **All Configuration**

Update all of the Radius configuration files.

#### **IP/IPX Routing and Bridging**

Updates only bridges, IP and IPX routing.

#### **IP Address Pool Configuration**

Updates only the IP address pool.

#### **Permanent and Nailed Configuration**

Updates only permanent and nailed configuration.

#### **Terminal Server Banners**

Updates the terminal server banner, which is the text a user sees when logging in to the unit's terminal server.

## The TFTP Server

The TFTP Server applet allows you to monitor the status of TFTP downloads and uploads, to view historical data about them, and to set parameters such as maximum retry and timeout.

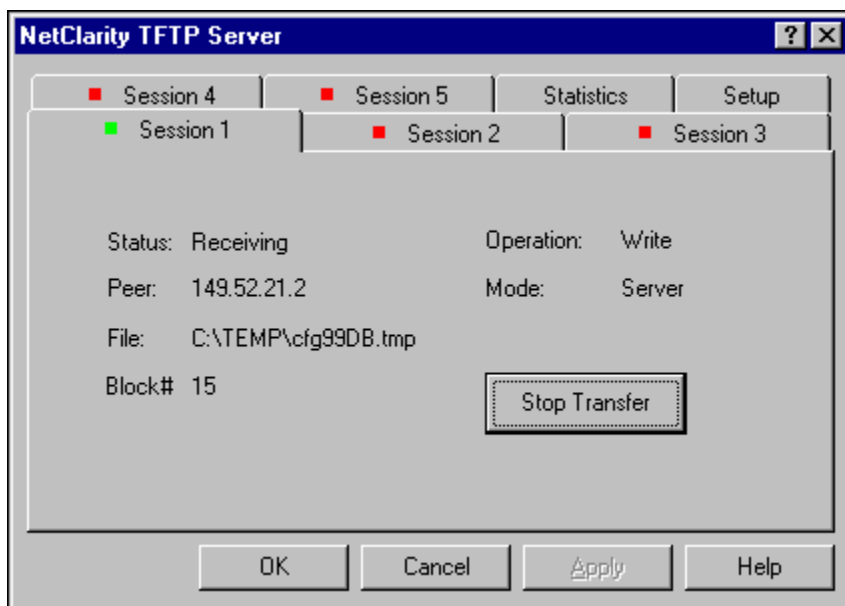
The TFTP Server applet is started automatically when NavisAccess starts and appears as a separate icon.

### **Opening the TFTP Server**

To open the TFTP Server applet, right-click on the TFTP Server icon and choose **Configure and Monitor TFTP**.

### **TFTP Server Session tabs**

The TFTP Server Session tabs display session information for ongoing TFTP downloads/uploads. When a session is in progress, the session tab will show a green highlight, as seen on the Session 1 tab below.



---

### Stopping a TFTP Transfer

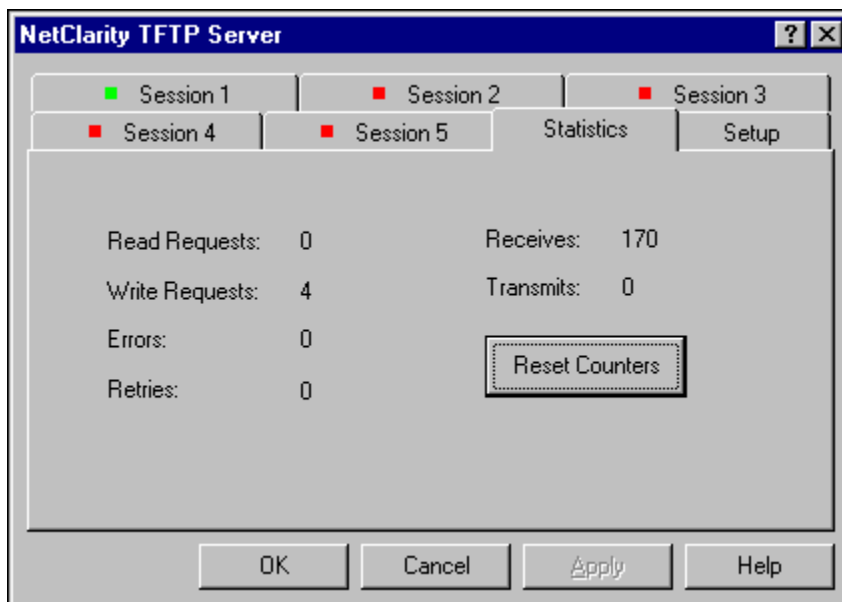
A TFTP session can be aborted by clicking the [Stop Transfer] button. When the TFTP server is idle, the [Stop Transfer] button becomes the [Clear Data] button, and can be used to reset the values on the TFTP Server Session tab.

Information displayed in the TFTP Server Session tab includes:

Field	Description
Status	Indicates status of the TFTP session. Status indicators are:  <b>Idle:</b> The TFTP server is not transmitting data.  <b>Receiving:</b> The TFTP server is receiving data from a device.  <b>Sending:</b> The TFTP server is sending data to a device.
Peer	The IP address of the peer application/device the server is contacting. This field is blank when status is Idle.
File	The name of the file being transferred.
Block#	The block number of the current transfer.
Operation	The type of activity currently taking place. Values are:  <b>Read:</b> the file is being read from the source.  <b>Write:</b> the file is being written to the destination.
Mode	The mode of the TFTP server. Values are:  <b>Server:</b> The TFTP server is acting as a server (sending data).  <b>Client:</b> The TFTP server is acting as a client (receiving data).

## TFTP Server Statistics tab

The TFTP Server Statistics tab displays global historical statistics for the TFTP server.



Information displayed in the TFTP Server Statistics tab includes:

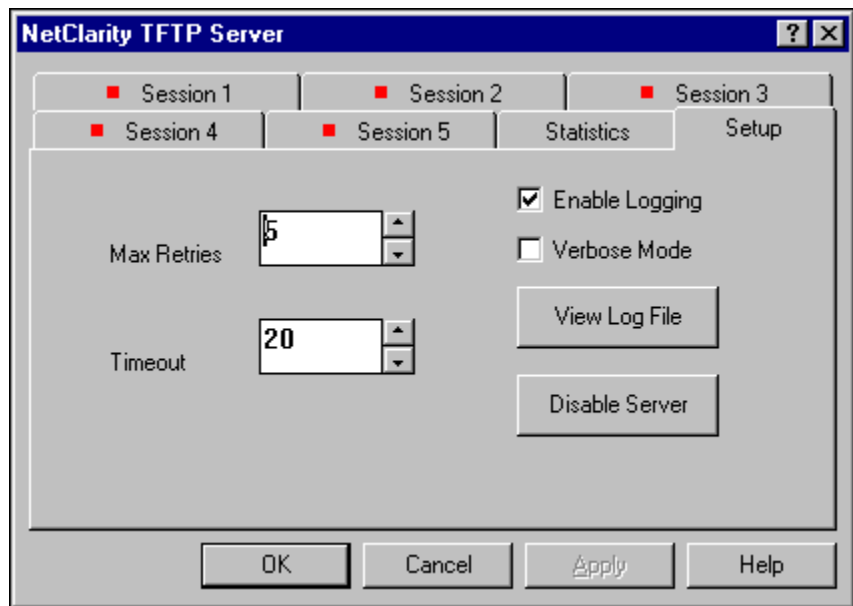
Field	Description
<b>Read Requests</b>	The total number of Read requests that have been received.
<b>Write Requests</b>	The total number of Write requests that have been received.
<b>Errors</b>	The total number of errors that have occurred during file transfers.
<b>Retries</b>	The total number of retry attempts.
<b>Receives</b>	The total number of blocks received during all file

Field	Description
	transfers.
<b>Transmits</b>	The total number of blocks transmitted during all file transfers.

To return all counters to zero, click the [Reset Counters] button.

## TFTP Server Setup tab

The TFTP Server Setup tab allows you to configure the TFTP server.



Fields that can be set from the Setup tab include:

Field	Description
<b>Max Retries</b>	Sets the number of times the TFTP server will retry a transfer before failing.
<b>Timeout</b>	Sets the amount of time, in seconds, that a transfer will be attempted before failing and retrying.

Field	Description
<b>Enable Logging</b>	Select this option to enable logging of TFTP events to the log file. To view the log file, click the [View Log File] button.
<b>Verbose Mode</b>	<p>Select this option to enable verbose mode logging. Verbose mode logging returns a block-by-block record of the file transfer. Without verbose mode, the log file will record the following:</p> <p><b>Start Date and time.</b> <b>Stop Date and time.</b> <b>File name.</b> <b>Source IP address.</b> <b>Destination IP address.</b></p> <p>Following is a sample, non-verbose log file entry:</p> <p><b>Thu Mar 20 14:21:26 1997 150.50.23.203</b> <b>FSTART Transfer of Cfgup.log to Cfgup.log</b></p> <p><b>Thu Mar 20 14:21:26 1997 192.168.30.180</b> <b>FEND Transfer of Cfgup.log to Cfgup.log.</b></p> <p><b>FSTART = start of file transfer. FEND = end of file transfer.</b></p>

To view the log file, click the [View Log File] button. The log file is saved as LOGFILE.TXT and stored in the NavisAccess home directory (c:\NavisAccess by default). You may delete the log file if it grows very large. A new one will be automatically created.

### Disabling the TFTP Server

To disable the TFTP Server, click on the TFTP Server Setup tab and click the [Disable Server] button. Doing so will terminate any ongoing sessions and prevent any new sessions from starting.

If you attempt a file transfer while the TFTP server is disabled, you will receive a “TFTP Operation Failed” error message.

If the TFTP Server is disabled, this is visually indicated by a change in the appearance of the TFTP Server icon.

## **The Telnet applet**

The Telnet applet uses the TCP/IP Telnet protocol to establish a terminal connection to the selected router. This allows access to all features available from the router such as: use of command interpreter, changing configurations, displaying router statistics and many other features. The features available through the telnet session are dependent on the manufacturer and the version of software running on the router

The Telnet applet requires the appropriate parameters (i.e. Password) be setup in the Telnet Configuration applet prior to launching the Telnet Applet.

### **Cisco-specific functions**

For Cisco routers, the show features of the router can be opened. Individual Cisco show commands will vary with the type of router and router software installed.

## **Starting the Telnet applet**

### **To start the Telnet applet from the Boxmap:**

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Telnet > Telnet**. From the application view, right-click the Telnet icon and select **Telnet**. The Telnet session window opens.

### **To start the Telnet applet from a device icon:**

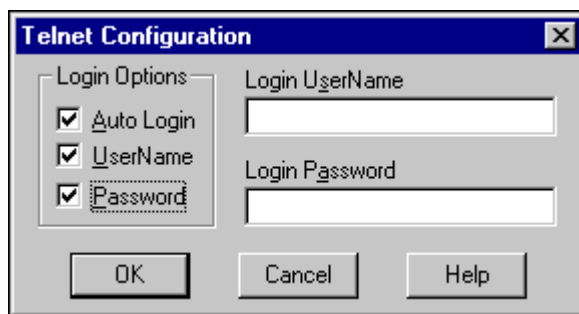
1. Right-click on a device icon and select **Telnet > Telnet**.

## **Configuring the Telnet applet**

### **To configure the Telnet applet:**

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Telnet > Configure**. From the application view, right-click the Telnet icon and select **Configure**. The Telnet Configuration window

opens.



Telnet Configuration options must be entered into the edit spaces and into the check boxes before a user attempts to establish a Telnet session. This is also necessary to initiate Show Commands (for Cisco routers only) from the **Telnet Icon**. The Network Administrator should set up these options.

### The Show Commands applet: Cisco specific

The **Show Commands** provides quick access to "show" commands on the router. Available commands vary to a great degree depending on the router software installed on the router.

The Show Commands applet issues specific show commands to the router and displays the results to the user. The show commands generally display statistics or status regarding various aspects of the router. The results of the commands are displayed in a video buffer. This allows the user to scroll back through and view the data received from the show command.

A sample Show Commands menu is shown below.



### **Additional Show Commands**

In addition to the Telnet applet, there are Show Commands available from the AppleTalk, Bridge and IPX icons.

### The Chassis Report applet: Overview

The **Chassis Report** displays the hardware configuration for the device, such as slot numbers, slot types and slot contents. The Chassis report is available for Ascend, Digital and Cisco devices. The contents of the Chassis report vary based on the kind of device.

Report types are:

- Ascend devices
- Digital devices (except the Gigaswitch)
- Cisco devices and the Digital Gigaswitch

Cisco routers must be using software version 9.2 and above.

### Using the Chassis Report

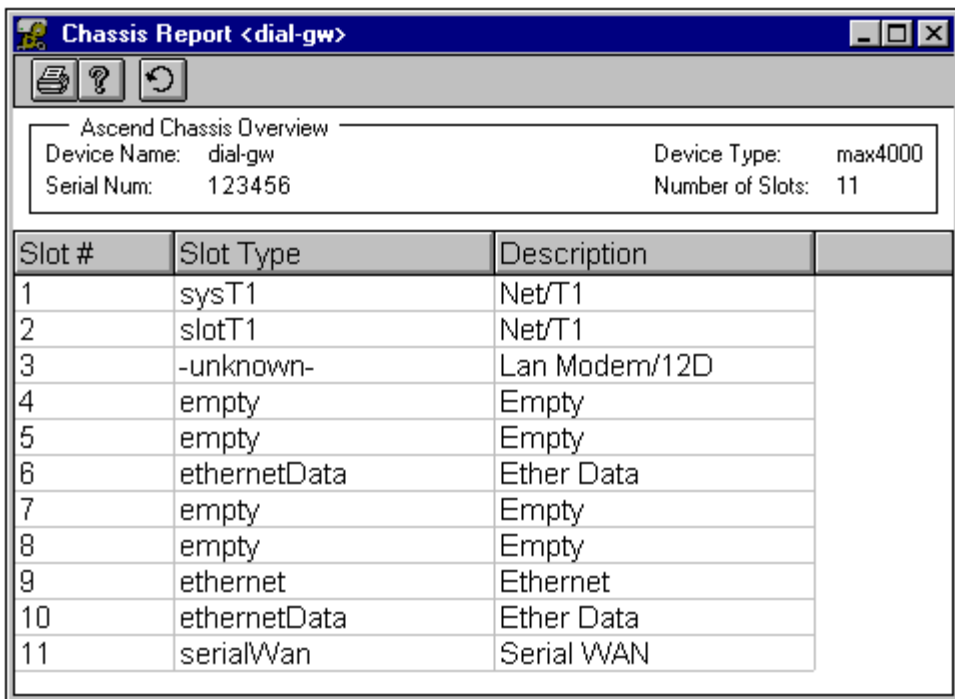
**To use the Chassis Report:**

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Chassis Report > Chassis Report**. From the application view, right-click the Chassis Report icon and select **Chassis Report**. The Chassis Report window opens.

**NOTE:** The Chassis Report is only available for Ascend, Cisco and Digital devices.

## The Chassis Report for Ascend devices

The Chassis Report consists of two panes. The upper section displays an overview of the device configuration and the lower section displays a table describing the cards installed in the device.



Slot #	Slot Type	Description	
1	sysT1	Net/T1	
2	slotT1	Net/T1	
3	-unknown-	Lan Modem/12D	
4	empty	Empty	
5	empty	Empty	
6	ethernetData	Ether Data	
7	empty	Empty	
8	empty	Empty	
9	ethernet	Ethernet	
10	ethernetData	Ether Data	
11	serialWan	Serial WAN	

## Device Management

---

The Chassis Overview section displays the following information:

Field Name	Description
Device Name	The name of the device.
Device Type	The type of device.
Serial Num	The serial number of the device.
Number of Slots	The number of slots found in the device.

The Chassis View table displays the following information:

Field Heading	Definition
Slot #	The slot number of the card.
Slot Type	The slot type.
Description	A brief description of the card. Empty slots will be listed as such.

## The Chassis Report for Digital devices

The Chassis Report consists of two panes. The upper section displays device information and the lower section displays a table describing the interfaces in the router.

**NOTE:** There is a separate Chassis Report for the Digital Gigaswitch.

DEC Device Overview				
Device Name: blu037		Device Type: <unknown>		
Wan Interfaces: 1		Lan Interfaces: 8		

IF Index	IF Name	IF Desc	IF Type	
1	eth0/net0 SCC E		ETHERNET CSI	
2	sl0/net1 SCC Se		PPP	
3	isdn0/net2 ISDN		BASICISDN	
4	isdn-d/isdn0 ISD		ISDN	
5	isdn-b1/isdn0 ISl		ISDN	
6	isdn-b2/isdn0 ISl		ISDN	
7	ppp/sl0 Point to l		PPP	
8	ppp/isdn0 Point t		PPP	
9	ppp/isdn0 Point t		PPP	

The Chassis Overview information includes:

Field Name	Description
Device Name	The name of the device.
Device Type	The type of device.
Wan Interfaces	The number of WAN interfaces on the device.
Lan Interfaces	The number of LAN interfaces on the device.

The Chassis View table includes the following information:

Field Heading	Definition
IF Index	The index number of the interface.
IF Name	The name of the interface.
IF Desc	A brief description of the interface as created using the interface Description applet.
IF Type	Indicates the type of interface.

## The Chassis Report for Cisco devices and the Digital Gigaswitch

The Chassis Report consists of two panes. The upper section displays device information and the lower displays a table describing the router interfaces.

Chassis Report <Patch>				
Chassis Overview				
Router Type:	multibus	Hardware Version:	Serial Number:	
Processor Ram:	16777216	nv Ram Size:	65536	nv Ram Used: 6031
Config Register:	0x2	Reload Register:	0x2	Number of Slots: -1
Rom Version:	System Bootstrap, Version 4.7(2), RELEASE SOFTWARE Copyright (c) 1986-1994 by cisco Systems			
Sys Version:	GS Software (GS3), Version 9.21(2), RELEASE SOFTWARE Copyright (c) 1986-1994 by cisco Systems, Inc. Compiled Wed 02-Mar-94 14			
Slot #	Card Type	Description	Hardware Ver	Software Ver
8	csc4	25MHz 68040		11.0
6	mci2e2t	MCI interface	1.1	1.11
7	csc-mcplus	pBus FLASH		
4	sci4s	SCI interface	2.0	1.4
1	sci4t	SCI interface	2.0	1.4
0	sci4t	SCI interface	2.0	1.4
2	sci4s	SCI interface	2.0	1.4
5	sci4s	SCI interface	2.0	1.4
3	sci4s	SCI interface	2.0	1.4

The Chassis Overview information includes:

Field Name	Description
<b>Router Type</b>	Model number.
<b>Processor Ram</b>	Total processor RAM installed in the router.
<b>Config Register</b>	The current configuration register setting on the router.
<b>Rom Version</b>	The version of microcode running on the router.
<b>Sys Version</b>	The version of IOS running on the router.
<b>Hardware</b>	The Hardware version of the chassis. This field is

---

Field Name	Description
Version	only supplied by certain Router Types.
nv Ram Size	Total nv RAM available. "nv RAM" is used to store the router config file.
Reload Register	The configuration register value for the next reload of the router.
Serial Number	The serial number of the chassis. This field is only supplied by certain Router Types.
nv Ram Used	Amount of RAM used by the current configuration.
Number of Slots	Total number of slots in the router chassis.

The Chassis View table includes the following information:

Field Heading	Definition
Slot #	The Slot number of the card.
Card Type	Indicates the model of the card.
Description	A brief description of the card.
Hardware Ver	Indicates the hardware version of the card.
Software Ver	Indicates the microcode version on the card.



# Automating Data Collection: The Schedule Wizard

## 9

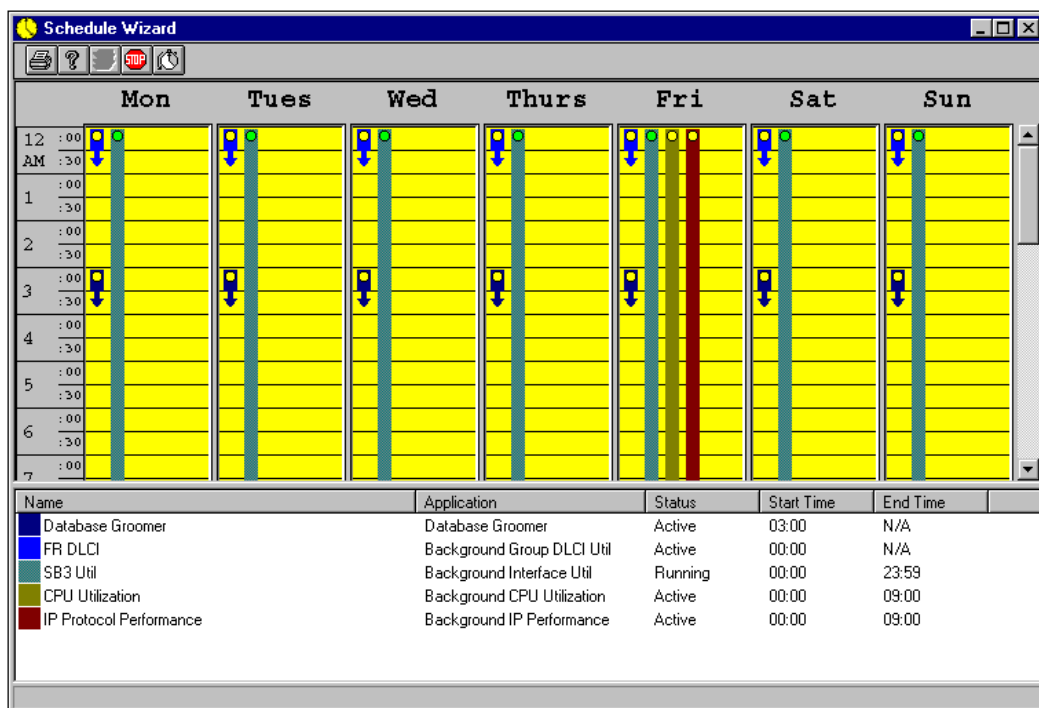
### **Menu Bar:** Config > Schedule

The Schedule Wizard is used to set up schedules to automatically perform repetitive background tasks in NavisAccess. Among the tasks that can be performed are:

- Gathering of performance data based on devices, device groups, interfaces, protocols (IP, IPX, AppleTalk, Frame Relay), CPU, etc.
- Autoscanning of network devices to update the NavisAccess database
- Gathering of device chassis information (i.e., the physical components of the device)
- Automated configuration file upload/download/diffing
- Automated device software upload/diffing
- Monitoring of interfaces for up/down status
- Monitoring of devices/interface for alarms
- Monitoring of utilization thresholds on devices/interfaces

Gathered data can be used to generate reports, either automatically based on Schedule Wizard configuration, or on an ad hoc basis using the Device DB program.

## The Schedule Wizard



**IMPORTANT:** In order for the Schedule Engine to work properly, the time and date settings of your system must be configured properly.

## More about schedule types

There are two different types of schedules in the Schedule Wizard.

- **Historical/Polled schedules** are of fixed duration, with a specified start and end point, and are used to gather data. A typical historical schedule would be the IP Performance schedule, which polls network devices to gather IP protocol performance data. Most historical schedules can be used to generate reports.

An Historical/Polled schedule is represented in the Schedule Wizard by a straight bar which displays in all of the time slots during which the schedule runs. There are two types of historical schedule: utilization schedules, which gather performance data, and alarm/threshold schedules, which monitor for error and threshold violations.

- **Configuration schedules** are designed to accomplish a specific task, as opposed to monitoring a device and collecting data over time. A configuration schedule begins at the pre-set time, and runs until it is finished. A typical configuration schedule is the Configuration Downloader schedule, which will download configuration files from all devices specified in the schedule setup.

A Configuration schedule is represented in the Schedule Wizard by a bar with an arrow which points down. This bar displays in the time slot in which you want the schedule to start.

A brief overview of available schedules follows. For details, see "Schedule Wizard Applications" on page 217.

The available historical/pollled schedules are:

### Utilization schedules:

- **Background AppleTalk Performance**  
Monitors performance of AppleTalk protocol.
- **Background CIR Trending**  
Monitors Frame Relay performance.
- **Background CPU Utilization**  
Monitors device CPU utilization.
- **Background IP Performance**  
Monitors performance of IP protocol.
- **Background IPX/SPX Performance**  
Monitors performance of IPX protocol.

### Alarm/Threshold Monitoring schedules:

- **Background Alarm Monitor**  
Monitors Alarm Monitor messages.
- **Background Interface Utilization**  
Monitors utilization levels of selected interfaces.
- **Interface Status Monitor**  
Monitors up/down status of interfaces in background.

The available configuration schedules are:

## The Schedule Wizard

---

- **AutoScan**  
Updates device information in the database.
- **Background Image Uploader**  
Uploads a software binary image to one or more devices at a scheduled time.
- **Device Change Control**  
Performs a differences operation on the device configuration file, physical chassis contents and software version number.
- **Configuration Uploader**  
Uploads a configuration file to one or more devices at a scheduled time.
- **Explorer**  
Runs the Explorer applet to discover devices on the network.
- **Database Groomer**  
Purges database information that is older than the specified purge date.

## Data collection and reporting: How it works

The Schedule Wizard is used to run applications which log data in an historical database. If you run an application, such as the IP Performance monitor, in real-time, the data collected will *not* be stored in an historical database, and therefore will not be available for analysis later. However, if you run the IP Performance Monitor application in the Schedule Wizard, data is logged to the database and graphical reports can be generated based on that data.

Note, however, that you can schedule data gathering to take place in the background, and still open and run the corresponding real-time application.

Calculated data can be exported to an ASCII file through the use of the Reporting Engine. This ASCII file can then be imported into any spreadsheet program.

### Generating Reports

The Schedule Wizard allows you to gather data about particular behaviors on particular devices. However, the Schedule Wizard only *collects* this data for the time periods you specify.

To view and understand the collected information, you need to create and run a report using the Device DB Reporting Engine. There are two ways to generate reports:

- Manually, using the Device DB program.
- Automatically, using the Report Automation option of the Schedule Wizard.

The Device DB Reporting Engine is aware of what the Schedule Wizard is doing. When you create a schedule using the wizard, you assign a task name to it. Then, when you are creating a report in Device DB, you can choose that schedule by name as the data source for your report. You can also select to have the report print automatically at a preset time.

This allows you to generate reports for specific time ranges and device lists. For example, using the two programs in conjunction, you can easily run a schedule to gather information about CPU utilization on three specific devices between the hours of 9:00 a.m. and 5:00 p.m. on Monday. Then you can generate a CPU Utilization report that graphically depicts the gathered information.

Similarly, you can scale up your information gathering and run reports covering a full week, 24 hours a day, on all your devices.

Because so many different reports are possible, almost all aspects of your network can be charted. Pinpointing bottlenecks and areas of performance degradation is no longer a guessing game, but a simple matter of gathering the needed information and viewing the analysis.

# **Schedule Wizard applications**

## **AutoScan**

The AutoScan application updates device information in the NavisAccess database without rediscovering each device. The user defines a schedule (usually run during off-peak hours) to AutoScan devices in the background. The application automatically scans each device included in the schedule. It discovers new interfaces and active protocols currently on the device. It also updates interfaces and protocols found on the device during a previous discovery session. Any changes found will be logged to the database.

## **Background Alarm Monitor**

The Background Alarm Monitor gathers Alarm Monitor messages without the need to have the Alarm Monitor application open and running. Devices can be monitored singly or in groups (including already defined groups).

Devices are monitored for the scheduled period and alarms issued when configured error thresholds set using the Threshold Manager are exceeded. Messages are sent to the Alarm Monitor (if running), the Event Viewer and to the historical database in the Event Report.

To create a Background Alarm Monitor schedule for the Threshold Manager, see "Creating a Threshold Manager Schedule" on page 331.

## **Background AppleTalk Performance**

The Background AppleTalk Performance application logs Apple Talk performance information into the historical database. AppleTalk Performance monitors Input, Forward, Local and Output packet statistics for the Apple Talk protocol, if it is active on the selected device(s). By default, data is reported at 15 minute intervals, unless specified otherwise under Application Parameters.

The Apple Performance application data is used to generate the AppleTalk Protocol Performance report in the Device DB program. The report can also be run using the Report Automation option in the Schedule Wizard.

To create an Apple Talk schedule, see "Creating a utilization schedule: protocols, CPU" on page 225.

### Background CIR Trending

The Background CIR Trending application logs CIR information into the historical database. CIR Trending monitors both sides of a Virtual Circuit for the selected device(s). By default, data is updated in 15 minute intervals, unless specified otherwise under Application Parameters.

The Background CIR Trending data is used to generate the Frame Relay VC Utilization, Frame Relay Network Capacity Leaders, Frame Relay Hourly Network Capacity Leaders and Frame Relay Daily Network Capacity reports in the Device DB program. The reports can also be run using the Report Automation option in the Schedule Wizard.

To create a Background CIR schedule, see "Creating a Frame Relay schedule: CIR trending" on page 230.

### Background CPU Utilization

The Background CPU Utilization application logs CPU Utilization information into the historical database. CPU Utilization monitors the current CPU utilization of the selected devices. By default, data is reported at 15 minute intervals, unless specified otherwise under Application Parameters.

The Background CPU Utilization application data is used to generate the CPU Utilization report in the Device DB program. The report can also be run using the Report Automation option in the Schedule Wizard.

To create a CPU schedule, see "Creating a utilization schedule: protocols, CPU" on page 225.

### Background Image Uploader

The Background Image Uploader uploads binary image files to one or more devices at a pre-set time. This allows for network-wide software updates without the use of error-prone and time consuming Telnet sessions.

Scheduled uploads to multiple devices are performed sequentially, not in parallel. This is done to limit damage in the event that a faulty software file is

## The Schedule Wizard

---

used.

Upon completing an upload, the device is reset and a validation check is performed. An event is generated to the Event Viewer indicating a successful upload. It is only after returning a successful update message that the upload operation for the next device in the schedule begins.

If the upload is *not* successful, a Critical event is sent to the Event Viewer and *the remainder of the upload schedule is terminated*, thereby protecting the rest of the network.

To create an Image Uploader schedule, see "Creating an Image Uploader schedule" on page 235.

## Background Interface Utilization

Create a Background Interface Utilization schedule to monitor interface utilization in real-time and to log utilization information into the historical database.

Devices are monitored for the scheduled period and events are issued when configured utilization thresholds set using the Interface Status Thresholds applet are exceeded. Messages are sent to the Event Viewer applet (if running), and to the historical database in the Event Report.

The Background Interface Utilization data is used to generate the Network Capacity Leaders, Daily Network Capacity, Hourly Network Capacity, Interface Utilization With Protocols and Interface Utilization Health Versus Time reports in the Device DB program. The reports can also be run using the Report Automation option in the Schedule Wizard.

To create a Background Interface Utilization schedule, see "Creating an Interface Utilization Thresholds schedule" on page 342.

## Background IP Performance

The Background IP Performance application logs IP performance information into the historical database. IP Performance monitors Input, Forward, Local and Output packet statistics for the IP protocol, if it is active on the selected device(s). By default, data is reported at 15 minute intervals, unless specified otherwise under Application Parameters.

The IP Performance application data is used to generate the IP Protocol Performance report in the Device DB program. The report can also be run using the Report Automation option in the Schedule Wizard.

To create an IP schedule, see "Creating a utilization schedule: protocols, CPU" on page 225.

## Background IPX/SPX Performance

The Background IPX/SPX Performance application logs IPX performance information into the historical database. IPX Performance monitors Input, Forward, Local and Output packet statistics for the IPX protocol, if it is active on the selected device(s). By default, data is reported at 15 minute intervals, unless specified otherwise under Application Parameters.

The IPX Performance application data is used to generate the IPX Protocol Performance report in the Device DB program. The report can also be run using the Report Automation option in the Schedule Wizard.

To create an IPX schedule, see "Creating a utilization schedule: protocols, CPU" on page 225.

## Configuration Uploader

The Configuration Uploader automatically uploads configuration files for specified devices at a designated time. This allows for network-wide configuration updates without the use of error-prone and time consuming Telnet sessions.

The Upload Text area can be edited with specific changes to the configuration file(s). The Options choices can yield a verbose response in the Event Viewer, saving of the new configuration file, and/or saving the new configuration file as the default. For Cisco routers, selecting **Save Config** writes the configuration file to non-volatile memory.

### Automating daily config changes

Because you can create multiple schedules for the same device, the Configuration Uploader allows you to upload different config files for different times of day. For example, you could send Config File A to Device 1 in the morning, and then send Config File B to Device 1 for the overnight period, using each config file to customize the device operation for that time period.

## The Schedule Wizard

---

To create a Configuration Uploader schedule, see "Creating a Configuration Uploader schedule" on page 238.

## Device Change Control

The Device Change Control application allows the user to perform a differences operation on the device configuration file, physical chassis contents and software version number. The differences operation compares the current device information with a previously saved version, and generates alerts if anything has changed.

The three change control options are:

- **Configuration File**

The configuration files for specified devices are retrieved beginning at the scheduled time. Once retrieved, the current configuration file running on the device is compared to that device's default configuration stored in the database. An alarm is automatically generated and sent to the Alarm Monitor and Event Viewer if differences between the default and current configuration are discovered.

- **Chassis Change Control**

Devices are scanned for chassis data beginning at the scheduled time. The current chassis information is compared to the information in the NavisAccess database. An alarm is generated if any changes are found. The kinds of changes that may be detected include: a new device has replaced the previous one at the same IP address; a change in serial number; a slot card has been moved or changed.

- **Binary Image Version**

The software version number for specified devices is retrieved and compared to the information in the NavisAccess database. An alarm is generated if a change is detected.

To create a Device Change Control schedule, see "Creating a Device Change Control schedule" on page 242.

## Database Groomer

The Database Groomer automatically purges data. Without the Database Groomer operating, databases could become extremely large.

The Database Groomer works with Schedule Wizard historical applications based on the purge period entered in the Set Number of Days field. For example, if you configure the Background IP Performance application with a 60 day purge period, all data older than 60 days will be deleted automatically. Each day going forward, the oldest day's data will be purged from the database.

By default, the purge period is set at 90 days. The Database Groomer is pre-configured to run every night at 3:00 a.m. *You do not need to schedule this application.* You cannot delete the Database Groomer, but you can change the time it begins, or you can deactivate it. Deactivation for long periods of time is not recommended.

## Explorer

The Explorer application discovers network devices beginning at the pre-set time. This allows network discovery, which can be a very time consuming process, to run at off-hours or be scheduled for periods of low network usage.

The Explorer can also be started manually. See "Introduction to device discovery" on page 48 for details on the discovery process.

To create an Explorer schedule, see "Creating an Explorer schedule" on page 246.

## Interface Status Monitor

Create an Interface Status Monitor schedule to monitor interfaces in real-time and to log Interface Status information into the historical database. Interface Status Monitor monitors the current state of the interfaces (either up or down) for the selected device(s) and logs the amount of time the interface spends in any state.

Devices are monitored for the scheduled period and alerts issued when configured status thresholds set using the Interface Status Thresholds applet are exceeded. Messages are sent to the Alert applet (if running), and to the historical database in the Event Report.

To create an Interface Status Monitor schedule, see "Creating an Interface Status Thresholds schedule" on page 348.

**NOTE:** Before the schedule is run, device interfaces must be configured using the Interface Status Thresholds applet.

### Using the Schedule Wizard

Schedules are represented by bars, one type for historical/polled schedules, another for configuration schedules. Right-clicking a schedule bar displays the Schedule Wizard Pop-up Menu. In addition, there are several schedule editing options available when you place the cursor on the schedule bar. Use the cursor to:

- Move a schedule to run in a different time slot.
- Increase the number of days across which a schedule will run.
- Change the length of time an Historical/Polling schedule will run.

If you are rescheduling an application, keep in mind that a schedule can only be a single block of time, and must be the same size block anywhere it appears. For example, you can run schedule "ABC" for four hours on Monday and four hours on Wednesday, but you cannot also run it for two hours on Tuesday. To run a two hour schedule you must create a new one, or reduce "ABC" to two hours everywhere it runs.

#### **Changing a Schedule**

Changing a schedule is a simple drag-and-drop procedure.

If you place your cursor in the middle of a schedule bar and click your mouse, you can drag the schedule up or down to change the time period. For example, you can move a two hour schedule running from 1:00-3:00 p.m. down to 5:00-7:00 p.m. Only the time *slot* will change, not the two hour schedule length. If a schedule covers more than one day, all the associated schedule bars will move at the same time.

You can add new days to the schedule by clicking the bar and moving sideways. Drag the bar to a new day and release the mouse button.

To change the length of a schedule, click the top or bottom of the schedule bar. You can then drag the bar, making it shorter or longer as needed. Release the mouse button to set the new time.

To remove one day from a schedule, right-click on the bar and choose **Delete > Day**.

#### **Starting and stopping a schedule**

There are several options available from the right-click menu of the Schedule Wizard. Click on a schedule in either the schedule window (top pane) or the schedule list (bottom pane) to access the following:

Menu Item	Description
<b>New Schedule</b>	Begins the process of creating a new schedule.
<b>Delete</b>	Deletes either an entire schedule or a day from a schedule that runs over multiple days.
<b>Edit Schedule</b>	Edit any of the schedule's configuration options.
<b>Activate Schedule</b>	Prepares a schedule to be run. A schedule must be activated before it can be run.
<b>DeActivate Schedule</b>	Prevents a schedule from being run. A schedule that has been deactivated will not start the next time it is scheduled to run. Deactivating a schedule that is currently running stops the schedule as well as deactivating it.
<b>Stop Schedule</b>	Stops a schedule that is currently running. A schedule that is stopped remains active, so that it will start the next time it is scheduled to run.
<b>Resume Schedule</b>	Re-starts a schedule that has been stopped if it is still within the specified time frame for that schedule.

## Creating schedules

### Creating a utilization schedule: protocols, CPU

Utilization schedules gather utilization data for use in generating reports through the DeviceDB program. Available utilization schedules are:

- Background AppleTalk Performance
- Background IP Performance
- Background IPX/SPX Performance

## The Schedule Wizard

---

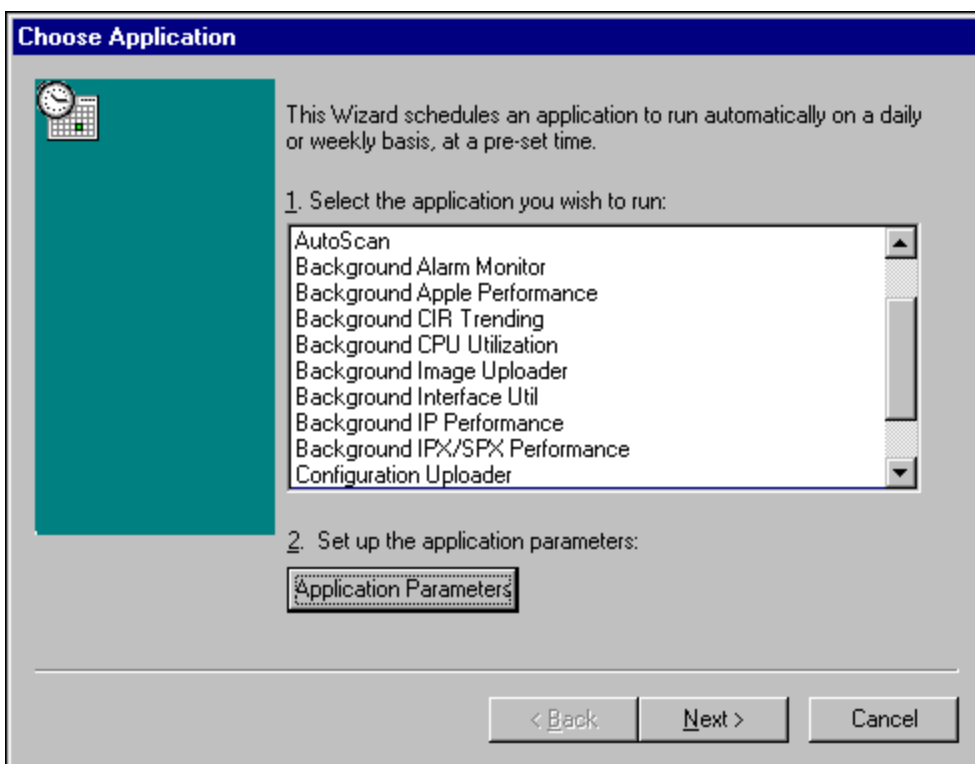
- Background CPU Utilization

**NOTE:** Frame Relay utilization and Interface utilization are covered separately.

**To create a utilization schedule:**

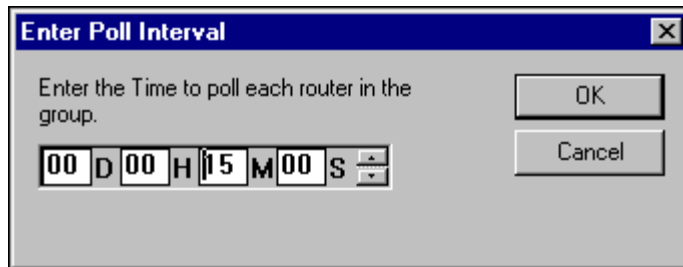
1. Highlight the time period during which the schedule will run.  
To do so, click and hold your left mouse button in the Schedule window, and drag the pointer up, down or sideways until the time period you wish to cover has been highlighted.
2. Right-click the highlighted area and select **New Schedule**.

The New Schedule Wizard appears:



3. Select one of the utilization monitoring applications. Each schedule can only have one application, or task, associated with it.

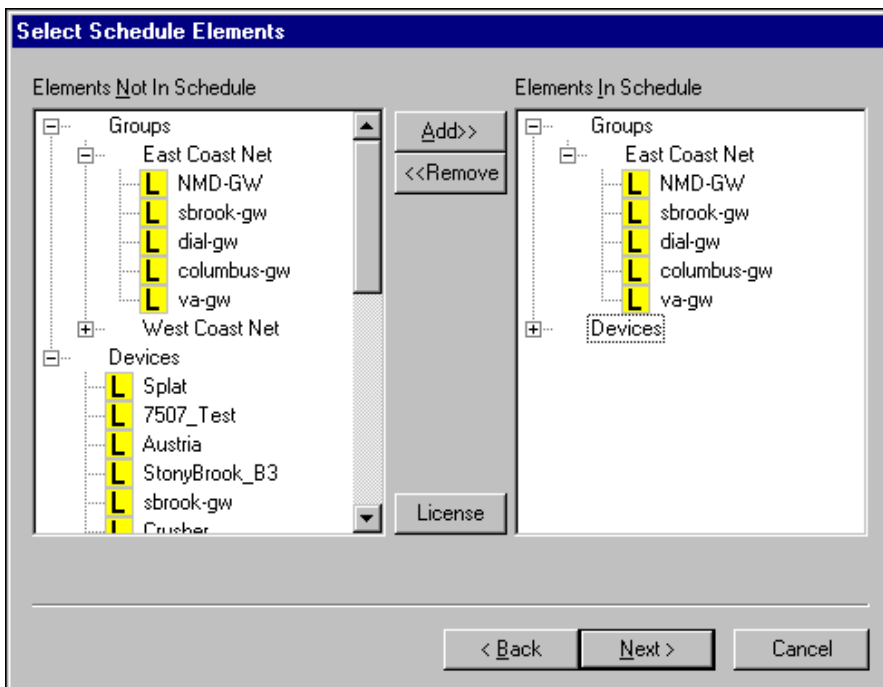
4. If necessary, change the application parameters.



For utilization schedules, the only parameter to set is the polling interval used during background performance monitoring. By default, devices are polled every 15 minutes.

5. Click [Next].

The Select Schedule Elements dialog box displays.



## The Schedule Wizard

---

6. Select the elements (Groups and Devices) you want included in the schedule.

To include an element in the schedule, first double-click on Groups or Devices to expand their respective trees (or click the plus sign "+"), then highlight the elements you want to select in the left pane. Click [Add] to add them to the Elements in Schedule field (right pane). Standard [Shift] and [Ctrl] key selection options apply.

Elements that appear in Groups have been previously configured as Device Groups in the Group Wizard. If you select at the Group level, all devices in the group will be added.

7. Click [Next]. The Select Logging Options dialog box displays:

**Select Logging Options**

1. Select how many days worth of data to keep in the database. Data older than the set number of days is purged.

Set Number of Days:

90

2. Select this check box to disable purging historical data:

☐ Do not purge Data

< Back   Next >   Cancel

8. Set the logging options:  
**Set Number of Days**

Specify the number of days, from the current day, for which you want the database to hold data. When the number of days is exceeded, the oldest data will begin to automatically be purged on a daily basis. For example, if you use the default 90 days, on the 91st day the data captured 90 days before (which is the day you created the schedule) will be purged.

### Do not purge Data

Select if you do not want the data to automatically be purged.

Click [Next] to continue.

9. The Select Automatic Reports dialog displays.

**Select Automatic Reports**

☒ Report Automation

1. All reports associated with the selected schedule are listed below. Reports can be run automatically at a pre-selected time, specified in the Time to Run Report field. To choose a frequency, highlight one or more reports, select Weekly and/or Daily, and click Apply.

Name	Weekly	Daily
IP Protocol Performance	No	Yes

2. Time to run report: 01:00

3. Frequency: ☐ Weekly ☒ Daily

< Back   Next >   Cancel

By default, the Schedule Wizard will automatically run reports. De-select the Report Automation check box if you do not want the reports to run automatically.

### Reports

## The Schedule Wizard

---

Lists the report(s) available.

### **Time to run report**

You can change the time the report will run using the "Time to run report" spin box. Reports run by default at 1:00 a.m. to avoid processor overhead during peak hours. The spin box uses a 24-hour clock (for example, 3:00 p.m. would be 15:00).

### **Frequency**

You can choose to run a given report daily and/or weekly. To change the settings, highlight the report(s), click the Weekly and/or Daily check box, and click [Apply].

Weekly reports run on Sunday, at the time selected in the Time to run report field.

When a report is run, the Schedule Wizard will print the report to your default printer. To view reports on screen, or to run additional reports, use the Device DB program.

10. Click [Next] to open the Create a New Task dialog.

Type in a name for the schedule. The name should help identify the type of task and the devices being used.

11. Click [Next] to open the Finish Creating the Task dialog box.

The schedule appears in the schedule list below the Schedule Wizard calendar.

By default, the new schedule will be automatically activated. If you do not want the schedule to be activated, click the Deactivate Schedule box. A deactivated schedule can be started at a later time by right-clicking on the schedule name in the Schedule Wizard and selecting Activate.

## Creating a Frame Relay schedule: CIR trending

The CIR Trending schedule gathers Frame Relay related utilization data by monitoring both sides of a virtual circuit as well as CIR.

### **To create a Frame Relay schedule:**

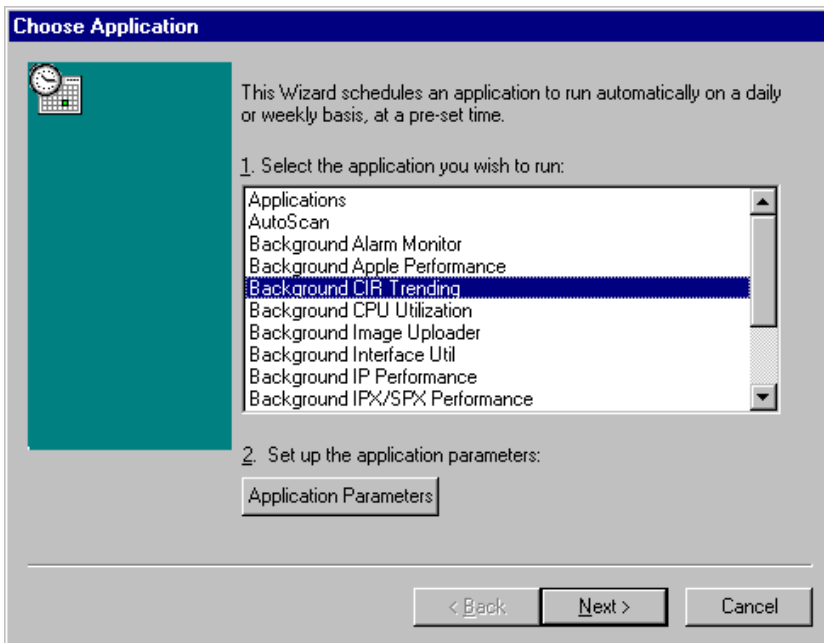
1. Highlight the time period during which the schedule will run.

To do so, click and hold your left mouse button in the Schedule window,

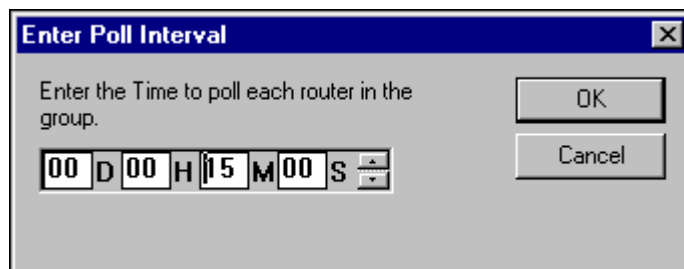
and drag the pointer up, down or sideways until the time period you wish to cover has been highlighted.

2. Right-click the highlighted area and select **New Schedule**.

The New Schedule Wizard appears:



3. Select **Background CIR Trending**. Each schedule can only have one application, or task, associated with it.
4. If necessary, change the application parameters.



For utilization schedules, the only parameter to set is the polling interval

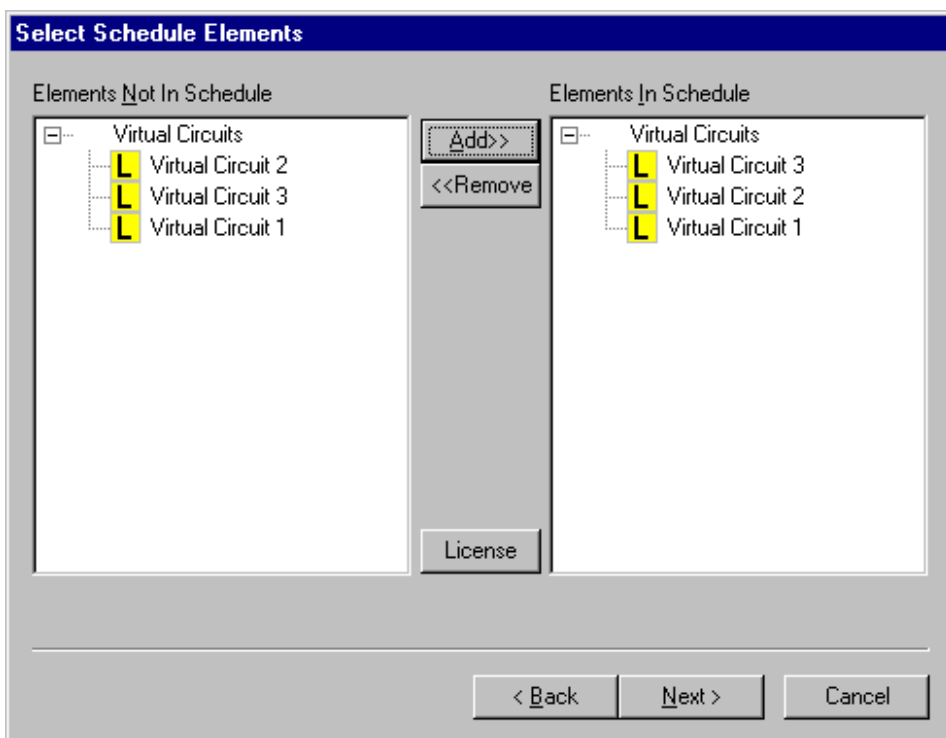
## The Schedule Wizard

---

used during background performance monitoring. By default, devices are polled every 15 minutes.

5. Click [Next].

The Select Schedule Elements dialog box displays.



6. The dialog will display only configured Virtual Circuits. If you have not configured any Virtual Circuits, this window will be empty, and you will not be able to create a schedule.

Select the Virtual Circuits you want included in the schedule.

To include a Virtual Circuit, highlight the VCs you want to select in the left pane. Click [Add] to add them to the Elements in Schedule field (right pane). Standard [Shift] and [Ctrl] key selection options apply.

7. Click [Next]. The Select Logging Options dialog box displays:

**Select Logging Options**

1. Select how many days worth of data to keep in the database. Data older than the set number of days is purged.

Set Number of Days:

90

2. Select this check box to disable purging historical data:

☐ Do not purge Data

< Back   Next >   Cancel

8. Set the logging options:

**Set Number of Days**

Specify the number of days, from the current day, for which you want the database to hold data. When the number of days is exceeded, the oldest data will begin to automatically be purged on a daily basis. For example, if you use the default 90 days, on the 91st day the data captured 90 days before (which is the day you created the schedule) will be purged.

**Do not purge Data**

Select if you do not want the data to automatically be purged.

Click [Next] to continue.

9. The Select Automatic Reports dialog displays.

By default, the Schedule Wizard will automatically run reports. De-select the Report Automation check box if you do not want the reports to run

## The Schedule Wizard

---

automatically.

### Reports

Lists the report(s) available. Available reports are:

- **Frame Relay VC Utilization**  
Shows the level of utilization for the selected virtual circuits as a percentage of the CIR.
- **Frame Relay Hourly Network Capacity**  
Shows the percentage of Frame Relay network capacity utilized over a selected time of day. Includes virtual circuit throughput, and FECN and BECN statistics.
- **Frame Relay Network Capacity Leaders**  
Shows the top N virtual circuits in terms of CIR utilization. N is the number of circuits reported on, determined by user selection when the report is run. The default value is top 10.
- **Frame Relay Daily Network Capacity**  
Shows the percentage of Frame Relay network capacity utilized over a selected number of days. Includes virtual circuit throughput, and FECN and BECN statistics.

### Time to run report

You can change the time the report will run using the "Time to run report" spin box. Reports run by default at 1:00 a.m., to avoid processor overhead during peak hours. The spin box uses a 24-hour clock (for example, 3:00 p.m. would be 15:00).

### Frequency

You can choose to run a given report daily and/or weekly. To change the settings, highlight the report(s), click the Weekly and/or Daily check box, and click [Apply].

Weekly reports run on Sunday, at the time selected in the Time to run report field.

When a report is run, the Schedule Wizard will print the report to your default printer. To view reports on screen, or to run additional reports, use the Device DB program.

10. Click [Next] to open the Create a New Task dialog.

Type in a name for the schedule. The name should help identify the type

of task and the devices being used.

11. Click [Next] to open the Finish Creating the Task dialog box.

The schedule appears in the schedule list below the Schedule Wizard calendar.

By default, the new schedule will be automatically activated. If you do not want the schedule to be activated, click the Deactivate Schedule box. A deactivated schedule can be started at a later time by right-clicking on the schedule name in the Schedule Wizard and selecting Activate.

### Creating an Image Uploader schedule

The Background Image Uploader schedule uploads a binary image to one or more devices at a pre-set time.

#### **To create an image upload schedule:**

1. Highlight the time period during which the schedule will run.

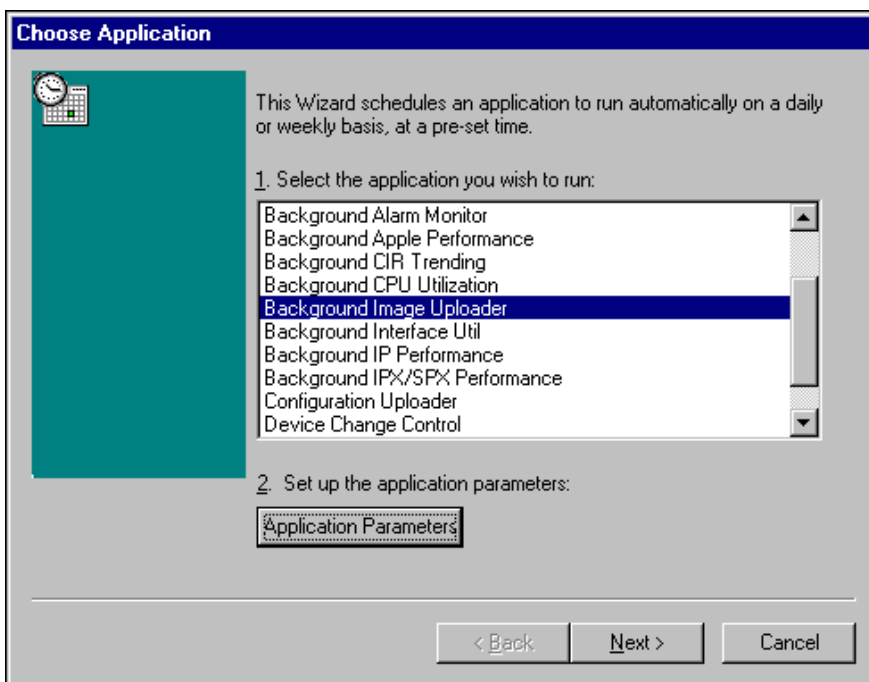
To do so, click and hold your left mouse button in the Schedule window, and drag the pointer up, down or sideways until the time period you wish to cover has been highlighted.

2. Right-click the highlighted area and select New Schedule.

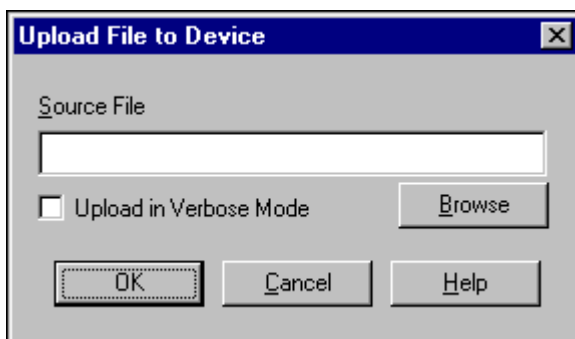
The New Schedule Wizard appears:

## The Schedule Wizard

---



3. Select the Background Image Uploader application.
4. Click the [Application Parameters] button.



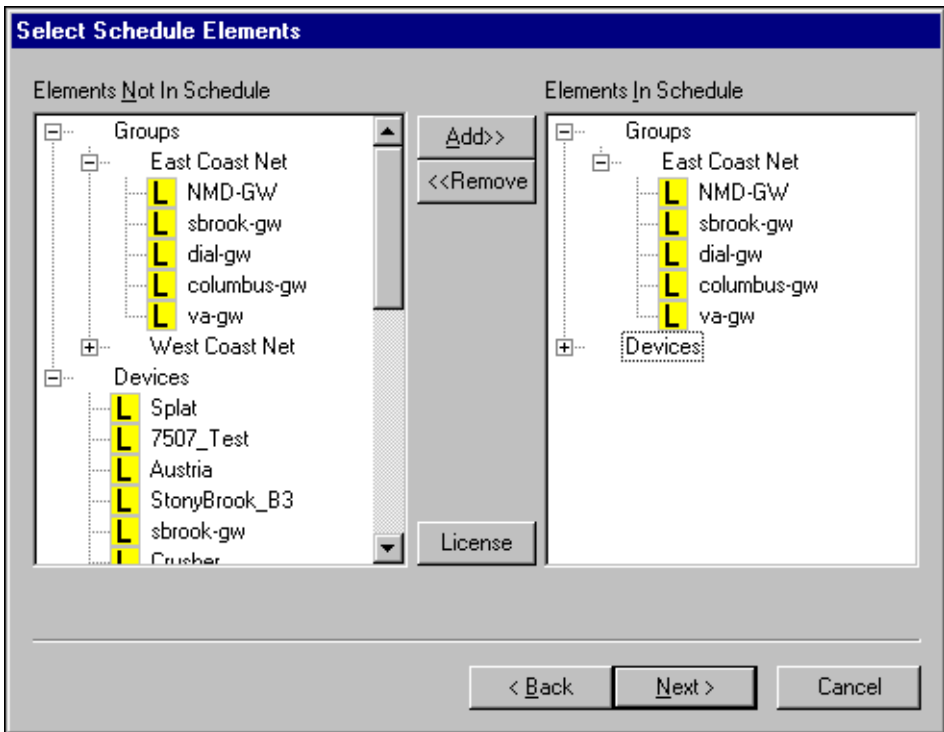
Enter the path and name of the file to upload, or use the [Browse] button to locate the file. By default, the [Browse] button opens in the NavisAccess directory. You may wish to create a sub-directory in which

to store image files.

Click [Ok] when done.

5. Click [Next].

The Select Schedule Elements dialog box displays.



6. Select the elements (Groups and Devices) you want included in the schedule.

To include an element in the schedule, first double-click on Groups or Devices to expand their respective trees (or click the plus sign "+"), then highlight the elements you want to select in the left pane. Click [Add] to add them to the Elements in Schedule field (right pane). Standard [Shift] and [Ctrl] key selection options apply.

Elements that appear in Groups have been previously configured as Device Groups. If you select at the Group level, all devices in the group

## The Schedule Wizard

---

will be added.

7. Click [Next] to open the Create a New Task dialog.

Type in a name for the schedule. The name should help identify the type of task and the devices being used.

8. Click [Next] to open the Finish Creating the Task dialog box.

The schedule appears in the schedule list below the Schedule Wizard calendar.

By default, the new schedule will be automatically activated. If you do not want the schedule to be activated, click the Deactivate Schedule box. A deactivated schedule can be started at a later time by right-clicking on the schedule name in the Schedule Wizard and selecting Activate.

## Creating a Configuration Uploader schedule

The Configuration Uploader schedule uploads a configuration file to one or more devices at a pre-set time.

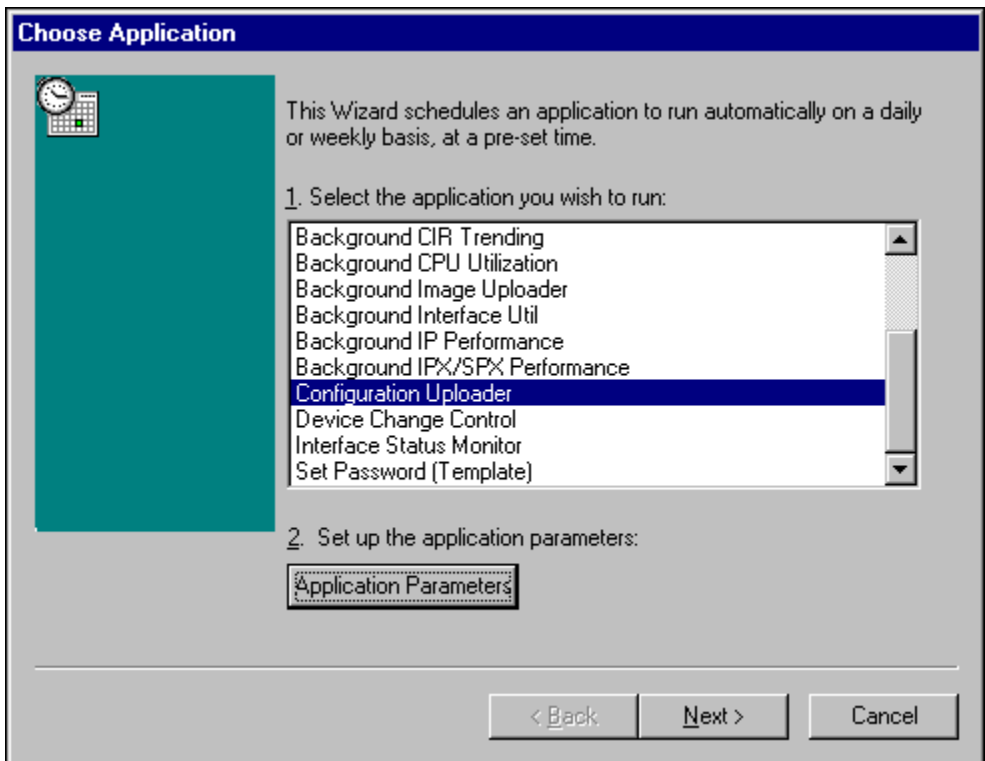
### To create a configuration upload schedule:

1. Highlight the time period during which the schedule will run.

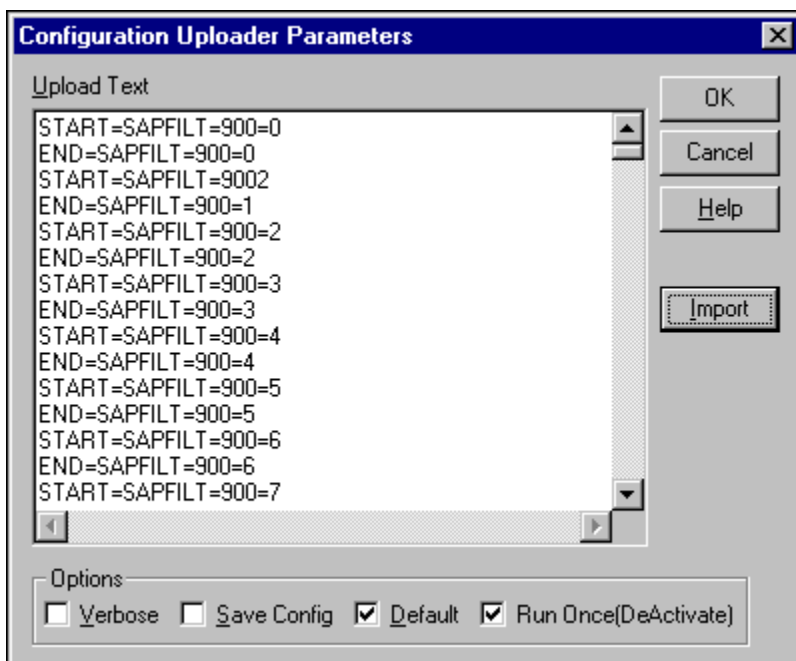
To do so, click and hold your left mouse button in the Schedule window, and drag the pointer up, down or sideways until the time period you wish to cover has been highlighted.

2. Right-click the highlighted area and select **New Schedule**.

The New Schedule Wizard appears:



3. Select the Configuration Uploader application.
4. Click the [Application Parameters] button.



Enter the configuration file into the Upload Text area. This can be done by cutting and pasting a configuration file, or by clicking the [Import] button and selecting a config file through the directory structure.

The configuration file can be edited in the Upload Text area. This allows you to make modifications to a saved file.

Options choices are:

**Verbose**

Generates a more detailed Event Viewer message.

**Save Config**

Saves the configuration file you are uploading.

**Default**

When used in conjunction with the Save Config option, saves the configuration file as the default configuration file for the device or devices.

**Run Once (DeActivate)**

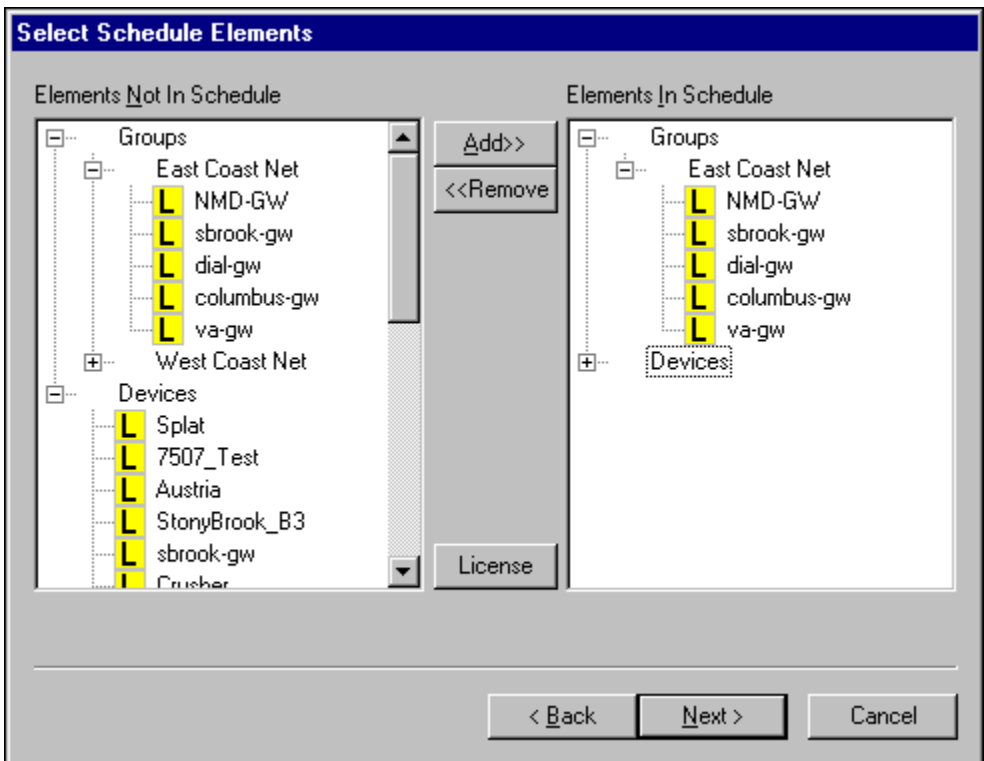
Select this option if you want the upload to take place only one time. If

you do not select this option, the configuration file will be uploaded again on each day that it is scheduled to run.

Click [Ok] when done.

5. Click [Next].

The Select Schedule Elements dialog box displays.



6. Select the elements (Groups and Devices) you want included in the schedule.

To include an element in the schedule, first double-click on Groups or Devices to expand their respective trees (or click the plus sign "+"), then highlight the elements you want to select in the left pane. Click [Add] to add them to the Elements in Schedule field (right pane). Standard [Shift] and [Ctrl] key selection options apply.

## The Schedule Wizard

---

Elements that appear in Groups have been previously configured as Device Groups. If you select at the Group level, all devices in the group will be added.

7. Click [Next] to open the Create a New Task dialog.

Type in a name for the schedule. The name should help identify the type of task and the devices being used.

8. Click [Next] to open the Finish Creating the Task dialog box.

The schedule appears in the schedule list below the Schedule Wizard calendar.

By default, the new schedule will be automatically activated. If you do not want the schedule to be activated, click the Deactivate Schedule box. A deactivated schedule can be started at a later time by right-clicking on the schedule name in the Schedule Wizard and selecting Activate.

## Creating a Device Change Control schedule

The Device Change Control schedule compares current device information (configuration file, physical chassis contents, software version) with previously stored information in the database.

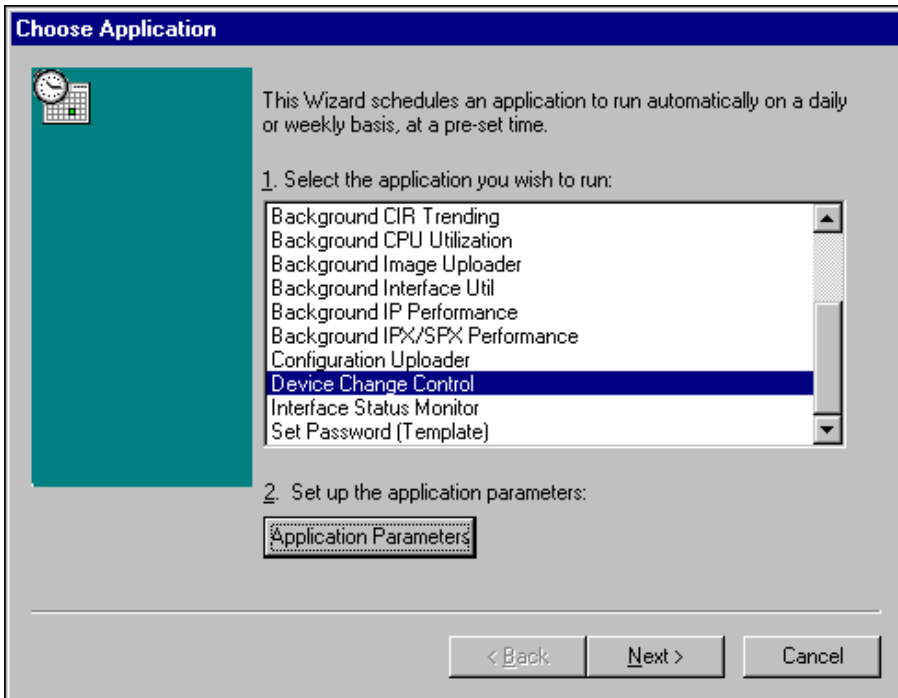
### To create a device change control schedule:

1. Highlight the time period during which the schedule will run.

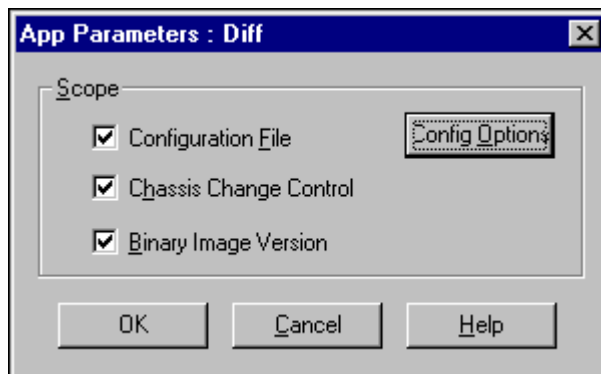
To do so, click and hold your left mouse button in the Schedule window, and drag the pointer up, down or sideways until the time period you wish to cover has been highlighted.

2. Right-click the highlighted area and select **New Schedule**.

The New Schedule Wizard appears:



3. Select the Device Change Control application.
4. Click the [Application Parameters] button.



Select the operations you wish to perform:

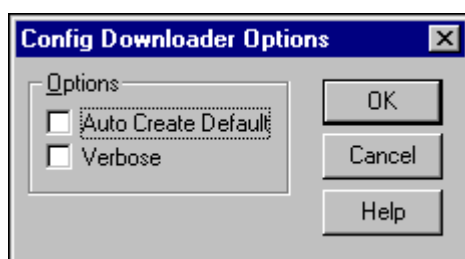
### Configuration File

## The Schedule Wizard

---

Retrieves the configuration files for specified devices. Once retrieved, the current configuration file running on the device is compared to that device's default configuration stored in the database. An alarm is automatically generated and sent to the Alarm Monitor and Event Viewer if differences between the default and current configuration are discovered.

There are additional options available by clicking the [Config Options] button:



### **Auto Create Default**

Saves the downloaded configuration file as the default file in the database. This can be used to establish a default the first time a configuration file is downloaded.

### **Verbose**

Provides a descriptive report for each download comparison available in the Event Viewer.

### **Chassis Change Control**

Scans devices for chassis data. The current chassis information is compared to the information in the NavisAccess database. An alarm is generated if any changes are found.

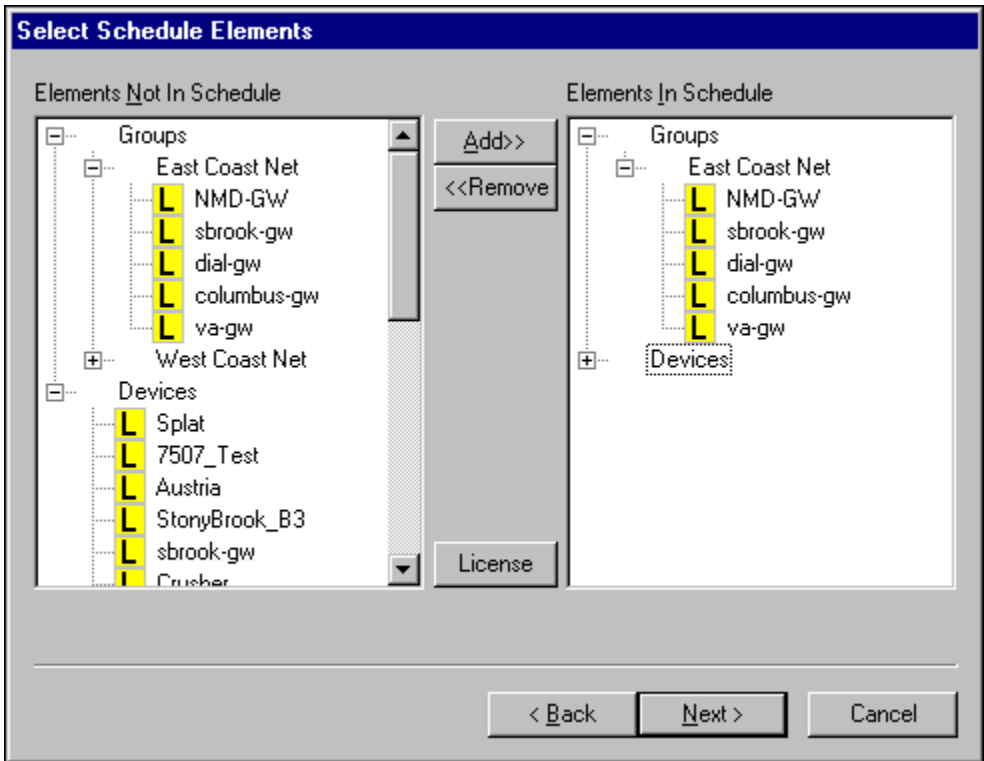
### **Binary Image Version**

Retrieves the software version number for specified devices and compares it to the information in the NavisAccess database. An alarm is generated if a change is detected.

Click [Ok] when done.

5. Click [Next].

The Select Schedule Elements dialog box displays.



6. Select the elements (Groups and Devices) you want included in the schedule.

To include an element in the schedule, first double-click on Groups or Devices to expand their respective trees (or click the plus sign "+"), then highlight the elements you want to select in the left pane. Click [Add] to add them to the Elements in Schedule field (right pane). Standard [Shift] and [Ctrl] key selection options apply.

Elements that appear in Groups have been previously configured as Device Groups. If you select at the Group level, all devices in the group will be added.

7. Click [Next] to open the Create a New Task dialog.

Type in a name for the schedule. The name should help identify the type of task and the devices being used.

## The Schedule Wizard

---

8. Click [Next] to open the Finish Creating the Task dialog box.

The schedule appears in the schedule list below the Schedule Wizard calendar.

By default, the new schedule will be automatically activated. If you do not want the schedule to be activated, click the Deactivate Schedule box. A deactivated schedule can be started at a later time by right-clicking on the schedule name in the Schedule Wizard and selecting Activate.

## Creating an Explorer schedule

The Explorer schedule runs the Explorer application to discover network devices.

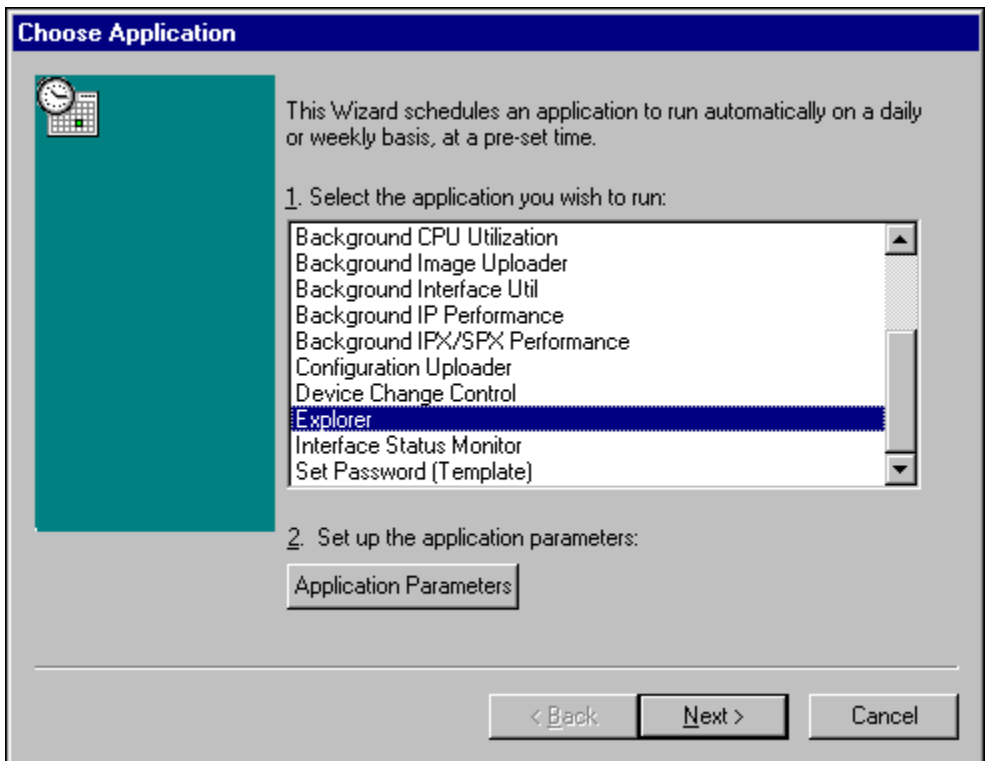
### To create an explorer schedule:

1. Highlight the time period during which the schedule will run.

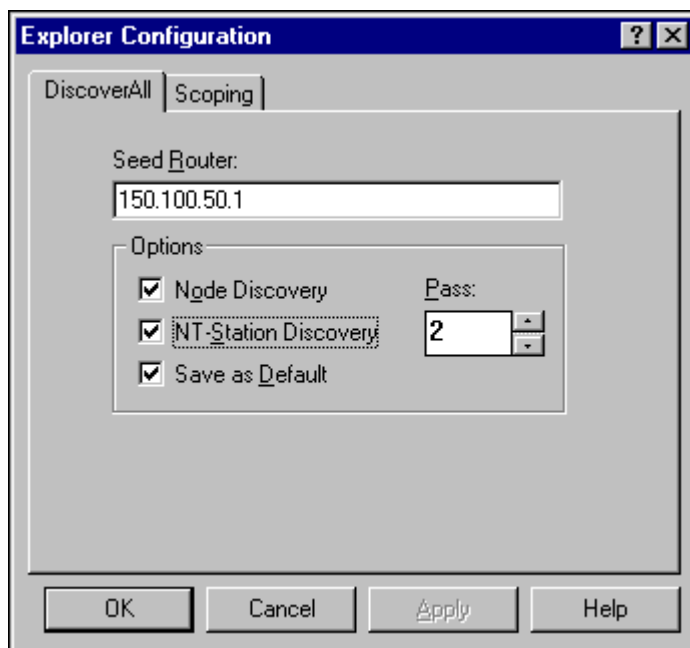
To do so, click and hold your left mouse button in the Schedule window, and drag the pointer up, down or sideways until the time period you wish to cover has been highlighted.

2. Right-click the highlighted area and select **New Schedule**.

The New Schedule Wizard appears:



3. Select the Explorer application.
4. Click the [Application Parameters] button.



5. Configure the settings on the **Discover All** tab.

### Seed Router

Provide the IP Address for your “Seed Router.” This router is defined as the starting point for discovery of your network.0

### Node Discovery

Select to have NavisAccess find all system nodes. This option is not recommended for most networks.

### NT-Station Discovery

Select to have NavisAccess discover all NT workstations and servers. This option is not recommended for most networks.

**NOTE:** To be successfully discovered, the NT machine must have SNMP Service enabled.

### Save as Default

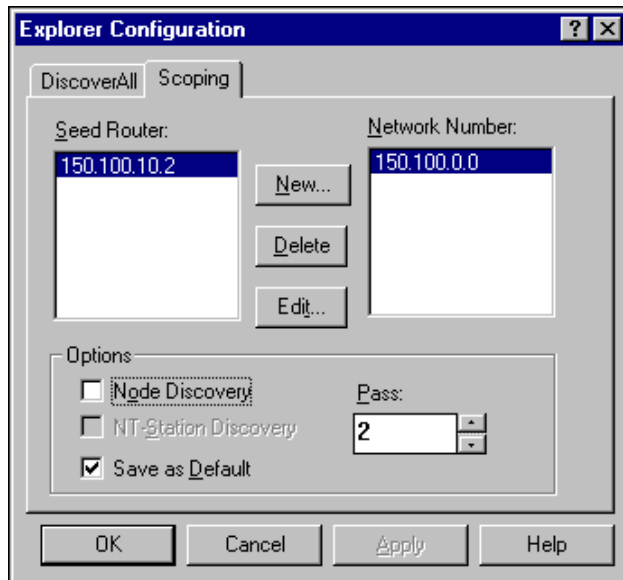
With this option enabled, when Explorer is run for a second time, it will begin from the point at which it left off. That is, it will not rediscover devices already discovered. This option is selected by default, and is recommended, particularly for large networks.

### Pass

Establish the number of passes for the auto discovery to make.

The range for the number of passes is from 1 to 10. Since many devices go down and up, and at times are too busy to respond to SNMP requests, there is the distinct possibility that some may be missed by the Explorer if only one pass is selected. It is therefore recommended that you select at least 2 passes.

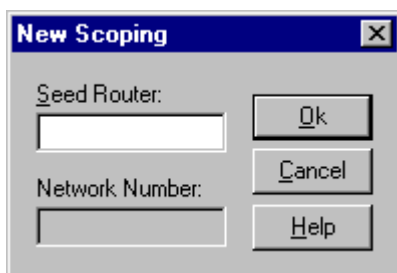
6. If you want to limit the networks which can be discovered, click the **Scoping** tab. In large networks, this can provide a more precise picture of a section of the network. If you are not using Scoping, skip to Step 6.



7. Each network you want to discover requires a seed router. Enter an IP address for each router you wish to use during network discovery. To do this, click the [New] button to open the New Scoping dialog box:

## The Schedule Wizard

---



The Network Number field is automatically filled in.

8. Click [Next] to open the Create a New Task dialog.

Type in a name for the schedule. The name should help identify the type of task and the devices being used.

9. Click [Next] to open the Finish Creating the Task dialog box.

The schedule appears in the schedule list below the Schedule Wizard calendar.

By default, the new schedule will be automatically activated. If you do not want the schedule to be activated, click the Deactivate Schedule box. A deactivated schedule can be started at a later time by right-clicking on the schedule name in the Schedule Wizard and selecting Activate.

## **Device Database: Overview**

The Device Database Program (DeviceDB) is a separate application that is used by NavisAccess for database maintenance and reporting. There are several components to DeviceDB.

### **Database maintenance**

A database is maintained for each device discovered by NavisAccess. The DeviceDB program allows you to delete selected devices from the database, or to delete specific interfaces and/or protocols on a device. In addition, you can view and delete configuration files for each device which are maintained in the database. (**NOTE:** configuration files must first be downloaded and stored in the database.) You can also view and delete chassis information for each device.

### **Database tools**

The DBMaint application provides database tools for operations such as database backup, restore and repair, and for generating a fresh database.

### **Reporting**

While NavisAccess is running, it is constantly collecting and logging performance data to the database. Specific types of data can be collected by setting up monitoring schedules for devices, protocols, performance, etc. The DeviceDB program generates historical reports using this stored information.

Remote access devices (Ascend MAX, MAX TNT and Pipeline) generate data when Call Logging is properly configured on the device.

Because DeviceDB collects performance data over extended time periods, reports can be used to better understand historical usage, performance trends, capacity needs, and so on. In addition, for some types of reports data can be generated both on a per-device basis, or averaged across a group. This is particularly useful for remote access devices, where group-wide, aggregate data is often more significant than data specific to one device.

In addition to historical reporting, DeviceDB generates configuration reports (device information) and ad hoc query reports (for chassis information,

## Database and Reporting

---

software versions, etc.).

See "Reporting: Overview" (page 265) for a listing of all available reports.

### **Data collection**

For details on how to schedule data collection, see "The Schedule Wizard" on page 213. To understand the important relationship between Device DB and the Schedule Wizard, please see "Data Collection and Reporting: How it works" on page 216.

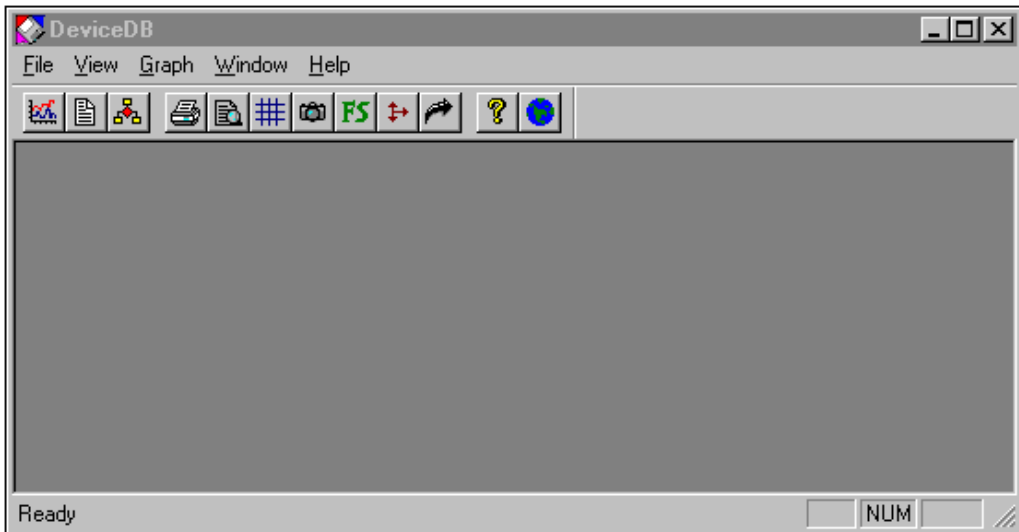
## Starting The Device Database program

### **To start the Database Program:**

1. It is advisable to close NavisAccess if you are going to perform database maintenance. If your intention is to run reports only (perform no maintenance), then NavisAccess may remain open.
2. From the Windows NT Start menu, select **Programs > NavisAccess > DeviceDB**.

You may also open Device DB through the NavisAccess main window by selecting **Tools > DeviceDB** from the main menu. (After starting DeviceDB, you may exit NavisAccess.)

The DeviceDB main window displays:



3. To perform database maintenance, click the [Device Maintenance] button. To create or run performance reports, click the [Open the Profile Selection] button or select **File > Graph Profiles** from the main menu. To create or run text-based reports, select **File > Text Profiles** from the main menu.

## **Database Maintenance: DeviceDB**

### **Database Maintenance: overview**

Database maintenance is performed through the Maintenance View screen. Several functions are available:

- Deleting a device, device interface or device protocol address from the database.
- Viewing device chassis information.
- Deleting device chassis information from the database, either for an entire device or a specific card.
- Viewing and deleting a stored configuration file for a device.

#### **Why do I need database maintenance?**

If a device is removed from your network, or a card is removed from a device,

## Database and Reporting

---

NavisAccess will still maintain its database entries. These devices or cards can be deleted from the database to insure they will no longer appear in the Group Wizard or Internet Map, and to remove unneeded data from the database.

Also, NavisAccess may locate many devices during its discovery process which it cannot identify, typically because of incorrect community string entries. This may populate the Group Wizard with many question mark icons indicating unknown devices. These icons can only be removed through the Device Maintenance screen.

**Please note:** if you delete an interface or address inadvertently, NavisAccess will rediscover it the next time the device is scanned (such as opening the Boxmap) and return it to the database. However, if an interface is removed permanently from a device, it is advisable to delete it through the Device Maintenance screen.

Similarly, chassis information can be deleted from the database when a card is removed from a device. Configuration files can be deleted from the database as well. This is quicker than deleting them through the Configure Router applet.

### To open the Maintenance View screen:

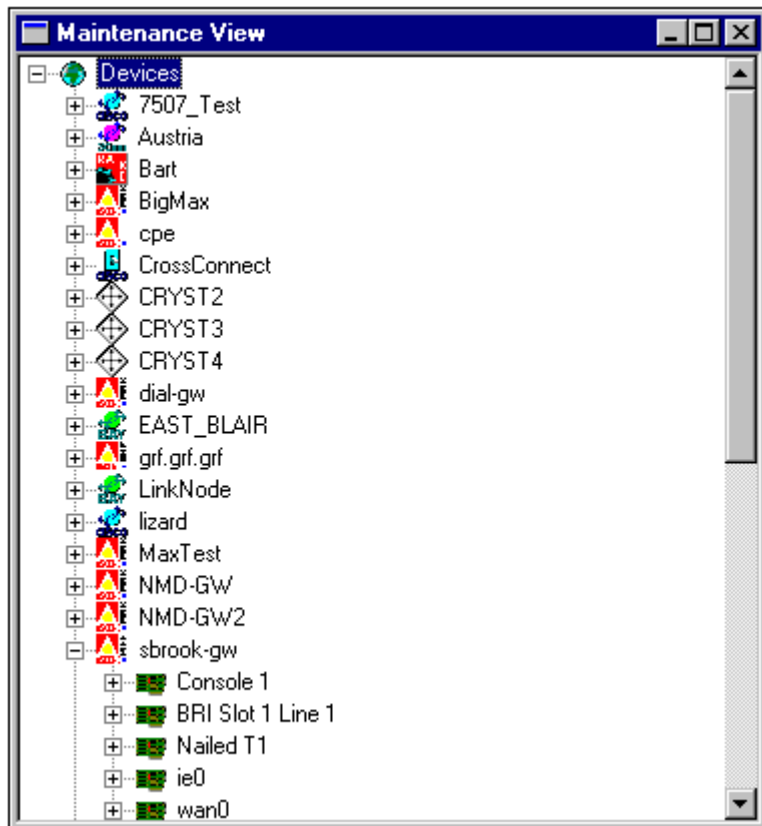
1. From the main menu in DeviceDB, select **File > Maintenance**. Alternately, click the [Device Maintenance] button.

## Deleting devices, interfaces and protocols

Devices, interfaces and protocols are deleted through the Device Maintenance screen.

### To delete a device:

1. Open the Device Maintenance window:



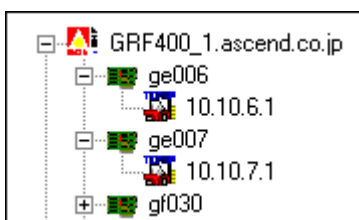
Devices are organized alphabetically in a standard tree view, with three levels.

### 1. Device

### 2. Interface

### 3. Protocol

For example, the section shown below shows an Ascend GRF at Level 1, three interfaces at Level 2, and two TCP/IP icons at Level 3, indicated by their IP address.



2. To delete a device, interface or protocol address, right-click on it and make the appropriate selection, either **Delete Device**, **Delete Interface**, or **Delete Address** respectively.

Depending on the volume of data accumulated for the deleted object, the deletion process may take a few moments.

**NOTE:** Deleting an object deletes it *only* in the NavisAccess database. No action is taken on the physical device.

## Chassis information: viewing and deleting

Device chassis information can be viewed and deleted from the database through the Maintenance View. Chassis information includes device type, available cards, number of slots, etc.

**NOTE:** Availability of chassis information will depend on device type and software version. Some devices will have no chassis information available, others will have limited information.

### To view and delete chassis information:

1. Right-click on a device in the Maintenance View window and select **Chassis Maintenance**. The Chassis Maintenance window opens:

Chassis Maintenance

Chassis Information:

Router Type:

multibus

Processor Ram:

16777216

Config Register:

Rom Version:

System Bootstrap, V

Sys Version:

GS Software (GS3).

Hardware Version:

nv Ram Size:

65536

Reload Register:

Serial number:

nv Ram Used:

6980

Number of Slots:

-1

Card Information:

Available Cards:

sci4s

Card Type:

sci4s

Description:

SCI interface

Hardware Version:

2.0

Software Version:

1.4

OK

Delete All Chassis Info

Delete This Card

2. The Chassis Maintenance screen is divided into two sections: Chassis Information and Card Information.

The Chassis Information section includes the following:

Title:	Definition:
Router Type	The type of router or model number.
Processor Ram	Total processor RAM installed in the device.
Config Register	The current configuration register setting on the device.
Rom Version	The version of microcode running on the device.
Sys Version	The version of IOS running on the device.

## Database and Reporting

---

Title:	Definition:
<b>Hardware Version</b>	The hardware version of the chassis. This field is only supported by certain Device Types.
<b>Nv Ram Size</b>	Total nv RAM available. NvRAM is used to store the device config file.
<b>Reload Register</b>	The configuration register value for the next reload of the device.
<b>Serial Number</b>	The device serial number.
<b>Nv Ram Used</b>	Amount of RAM used by the current configuration.
<b>Number of Slots</b>	Slots contained in the chassis.

In the Card Information section, details are available for each card on the device. A different card can be viewed by making a selection in the Available Cards drop-down box. The Card Information section includes the following:

Title:	Definition:
<b>Available Cards</b>	Card(s) available in the slot
<b>Card Type</b>	Indicates the model of the card
<b>Description</b>	A brief description of the card.
<b>Hardware Version</b>	Indicates the H/W version of the card.
<b>Software Version</b>	Indicates the microcode version on the card.

3. To delete all chassis information for a device, click the [Delete All Chassis Info] button. To delete information only for a specific card, choose the card in the Available Cards drop-down box and click the [Delete This Card] button.

## Configuration File Database: viewing and deleting

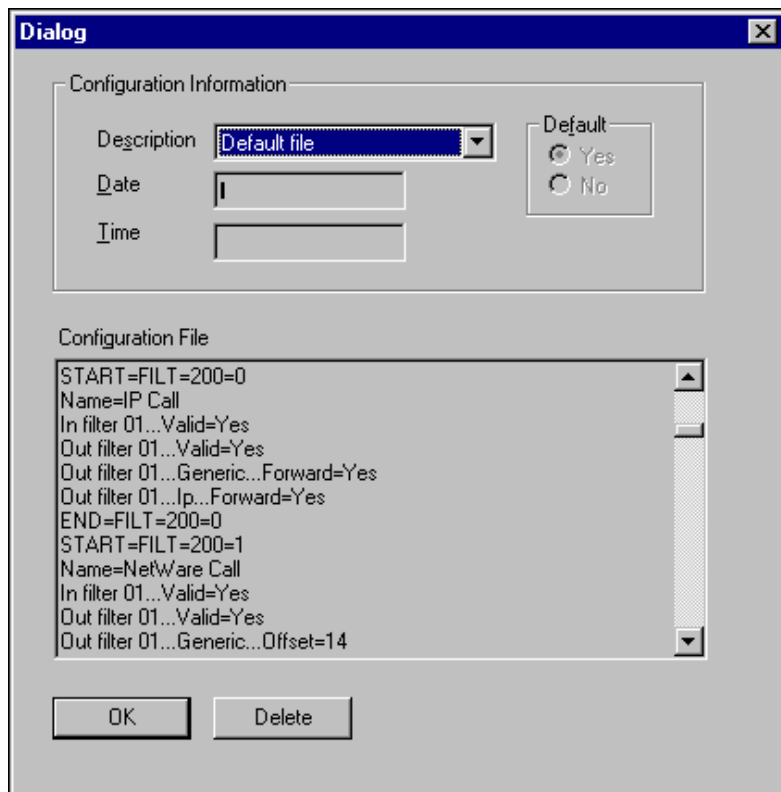
NavisAccess can download and store device configuration files using the Configure Router applet. Each device has its own set of configuration files. The Device Database program can view and delete the files in the database.

### To view or delete a configuration file:

1. Right-click on a device and select **Config Maintenance**.

**NOTE:** If you have not downloaded and stored at least one configuration file for the device, this option will not be available.

2. The configuration information is displayed:



The screenshot shows a 'Dialog' window with a title bar containing a close button. The window is divided into two main sections. The top section, titled 'Configuration Information', contains a 'Description' dropdown menu with 'Default file' selected, a 'Date' text input field, a 'Time' text input field, and a 'Default' group box with 'Yes' and 'No' radio buttons. The bottom section, titled 'Configuration File', contains a list box with the following text: START=FILT=200=0, Name=IP Call, In filter 01...Valid=Yes, Out filter 01...Valid=Yes, Out filter 01...Generic...Forward=Yes, Out filter 01...Ip...Forward=Yes, END=FILT=200=0, START=FILT=200=1, Name=NetWare Call, In filter 01...Valid=Yes, Out filter 01...Valid=Yes, Out filter 01...Generic...Offset=14. At the bottom of the window are 'OK' and 'Delete' buttons.

The following fields are displayed:

**Description**

The name given to the configuration file when it was saved. Select a file by using the drop-down box.

**Date/Time**

The date and time the file was last saved in NavisAccess.

**Default**

Indicates if the selected file is the default configuration file.

**Configuration File**

Displays the configuration file text. This field is for viewing only. To edit a configuration file, use the Configure Router applet.

3. To delete a configuration file, select the file in the Description drop-down box and click the [Delete] button.

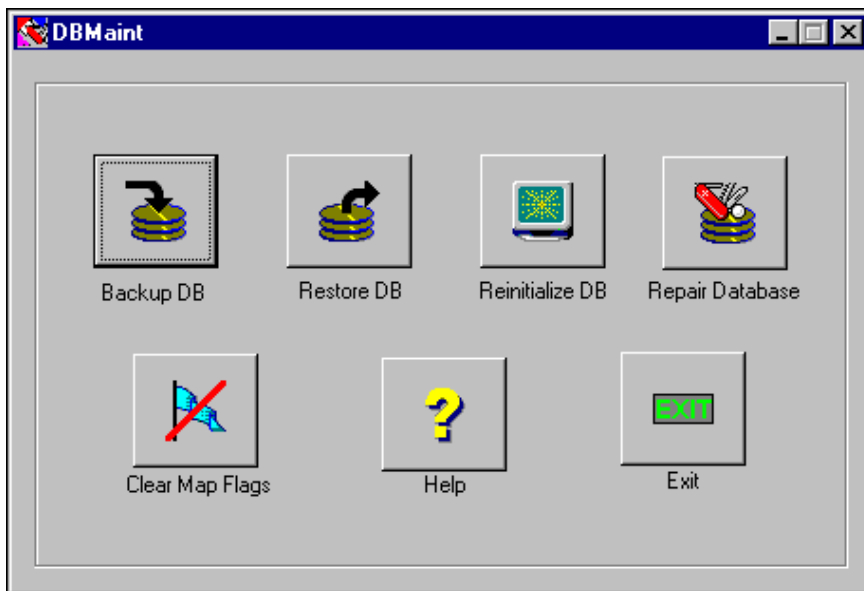
**NOTE:** Deleting a configuration file will delete it only from the NavisAccess database. The configuration file on the physical device is not touched in any way.

## **Database Tools: overview**

NavisAccess provides database tools that can be used for the following:

- **Database backup**  
Saves up to three copies of the NavisAccess database.
- **Database restore**  
Returns the database to a previous state using a backup file.
- **Database reinitializing**  
Deletes current database and replaces it with the original, empty database.
- **Database repair**  
Repairs database tables.

Database tools are run from the DBMaint application.



### **The Clear Flags button**

The Clear Flags button is provided as an additional support tool. This application will be needed only in very rare and specific instances.

**This tool should be used only when requested by Ascend Communications technical support.**

### Database backup and restore

NavisAccess allows you to backup and save up to three copies of the NavisAccess database. Any of these copies can be used to restore the database to a previous state. You may also want to include the backup files in your server backup plans to store them on tape or other backup media.

#### To back up the database:

1. Start the DBMaint applet from the NavisAccess program group or Windows NT Start button. Choose **Start > NavisAccess > DBMaint**.
2. A login screen appears. Enter a NavisAccess user name and password.

**NOTE:** Only users with Administrator rights will be able to access the DBMaint application.

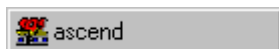
The DBMaint screen appears.

3. Click the Backup DB button. A verification message box appears. Click [OK] to continue.
4. The Backup Status screen shows the progress of the backup. A message box indicates when the backup is complete.

The backup file is stored in the **NavisAccess/database** directory under the file name **Ascend.000**. Up to three backups can be stored (Ascend.000, Ascend.001, Ascend.002).

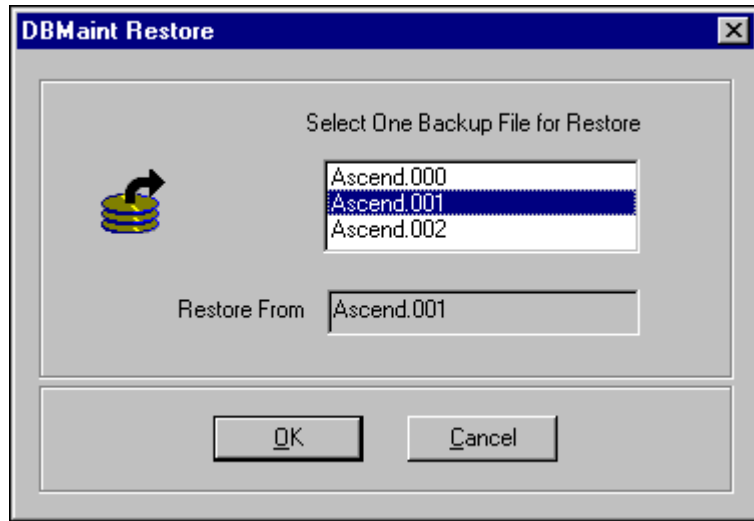
#### To restore the database:

1. Start the DBMaint application as described above.
2. Click the Restore DB button.
3. If your database is running, you will receive a message asking you to shut down the database. To shut the database, right-click the Ascend database icon found on the task bar or the desktop and select Close.



After closing, click the Restore DB button again.

4. The DBMaint Restore screen appears:



The window will display up to three files (if you have done three backups or more). These are always the last three backups, with **Ascend.000** being the most recent and **Ascend.002** the oldest.

Select a backup file from those listed in the window and click [OK]. The Restore Status screen will display while the database is being restored.

## Generating a fresh database

NavisAccess allows you to create a fresh, empty database through the Reinitialize Database application

**NOTE:** Reinitializing the database will destroy all data in the current database. It is advisable to backup a copy of your current database before starting the reinitialize application.

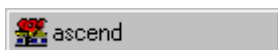
### To reinitialize the database:

1. Start the DBMaint applet from the NavisAccess program group or Windows NT Start button. Choose **Start > NavisAccess > DBMaint**.
2. A login screen appears. Enter a NavisAccess user name and password.

**NOTE:** Only users with Administrator rights will be able to access the DBMaint application.

The DBMaint screen appears.

3. Click the Reinitialize DB button. A warning message appears. Click [OK] to proceed.
4. If your database is running, you will receive a message asking you to shut down the database. To shut the database, right-click the Ascend database icon found on the task bar or the desktop and select **Close**.



After closing, click the Reinitialize DB button again.

5. A status screen shows the progress of the re-initialization.

## Repairing a database

NavisAccess allows you to repair your database in the rare and specific instance that a "Corrupt database" message is received.

**NOTE: The Repair Database application should only be used if a "corrupt database" message has been received.** It is advisable to contact Ascend technical support before proceeding with this operation.

### To repair the database:

1. Start the DBMaint applet from the NavisAccess program group or Windows NT Start button. Choose **Start > NavisAccess > DBMaint**.
2. A login screen appears. Enter a NavisAccess user name and password.

**NOTE:** Only users with Administrator rights will be able to access the DBMaint application.

The DBMaint screen appears.

3. Click the Repair Database button. A warning message appears. Click [OK] to proceed.
4. Upon completion, a "Tables Restored" message will be received.

## **Reporting**

### **Reporting: overview**

The Device Database program uses database information to generate both graphical and text-based reports. Following are brief report descriptions. For details on reports, see "Report Details and Samples" (page 292).

There are several categories of reports.

**Remote access performance reports:** Graphical reports that depict performance at the access layer. Data for these reports is generated by the Access Watch application.

Available reports are:

- **Hourly Average Connect Rate**  
Graphs the average connect rate (in Kbps) for individual devices or aggregate data for groups of devices on an hourly basis.
- **Daily Average Connect Rate**  
Graphs the average connect rate (in Kbps) for individual devices or aggregate data for groups of devices on a daily basis.
- **Hourly Network Channel Availability/Utilization**  
Graphs the percentage of channel availability and utilization for individual devices or aggregate data for groups of devices on an hourly basis.
- **Daily Network Channel Availability/Utilization**  
Graphs the percentage of channel availability and utilization for individual devices or aggregate data for groups of devices on a daily basis.
- **Hourly Average Network Connect Time**  
Graphs the average user connect time for individual devices or aggregate data for groups of devices on an hourly basis.
- **Daily Average Network Connect Time**  
Graphs the average user connect time for individual devices or aggregate data for groups of devices on a daily basis.
- **Hourly Modem Availability/Utilization**  
Graphs the percentage of modem availability and utilization for individual

devices or aggregate data for groups of devices on an hourly basis.

- **Daily Modem Availability/Utilization**  
Graphs the percentage of modem availability and utilization for individual devices or aggregate data for groups of devices on a daily basis.
- **Hourly Number of Logins**  
Graphs the number of user logins for individual devices or aggregate data for groups of devices on an hourly basis.
- **Daily Number of Logins**  
Graphs the number of user logins for individual devices or aggregate data for groups of devices on a daily basis.
- **Hourly Active Sessions**  
Graphs the number of active sessions for individual devices or aggregate data for groups of devices on an hourly basis.
- **Daily Active Sessions**  
Graphs the number of active sessions for individual devices or aggregate data for groups of devices on a daily basis.

**Network performance reports:** Graphical reports that depict various aspects of network performance. Available reports are:

- **Network Capacity Leaders**  
Graphs the ten interfaces with the highest percentage of used capacity for a selected time and date range.
- **Daily Network Capacity**  
Graphs the percentage of utilized network capacity over a number of days.
- **Hourly Network Capacity**  
Graphs the utilized network capacity over a selected time of day.
- **Interface Utilization With Protocols**  
Graphs the interface utilization and the individual protocol utilization (IP, IPX, AppleTalk) for the specified hours of a day.
- **Interface Utilization Versus Time**  
Graphs the interface utilization for the specified hours of a day.
- **Interface Utilization as a Percentage Of Time**  
Graphs the percentage of a selected time period that an interface was within a specified utilization range.

- **CPU Utilization**

Graphs the percentage of CPU utilization versus a specified time of day

## Database and Reporting

---

- **Apple Talk Protocol Performance**  
Graphs AppleTalk packet statistics over a given time period.
- **IPX Protocol Performance**  
Graphs IPX packet statistics over a given time period.
- **IP Protocol Performance**  
Graphs IP packet statistics over a given time period.
- **Frame Relay VC Utilization**  
Graphs the level of utilization for the selected virtual circuits as a percentage of the CIR.
- **Frame Relay Network Capacity Leaders**  
Graphs the top N virtual circuits in terms of CIR utilization. N is the number of circuits reported on, determined by user selection when the report is run. The default value is top 10.
- **Frame Relay Hourly Network Capacity**  
Graphs the utilization of Frame Relay network capacity over a selected time of day.
- **Frame Relay Daily Network Capacity**  
Graphs the utilization of Frame Relay network capacity over a selected number of days.

**Configuration reports:** Text-based reports that provide device-specific information. Available reports are:

- **Device report**  
Displays an informational summary for each device selected. Information includes: Device Name, manufacturer, Software Version, etc.
- **Address report**  
The Address Report displays the network addresses for each interface on a device, including a breakdown by protocol..

**Query reports:** Text-based reports that are generated based on user-defined queries. Available reports are:

- **Configuration report**  
Performs ad hoc queries against the configuration file database, allowing you to specify phrases or parts of phrases that may be in the device configuration file.

- **Chassis report**  
Performs ad hoc queries against the device database to locate devices containing specific chassis information. Predetermined database fields, such as router type and hardware version, are used as search criteria.
- **Versions report**  
Performs ad hoc queries against the device database to search for devices running a specific software version.
- **Account Disconnect report**  
Returns a list of all call disconnect reasons and progress types for a specified time period.

## Creating a Performance Report

Both Remote Access performance and network performance reports are created in the same fashion. Before generating a report, please note the following:

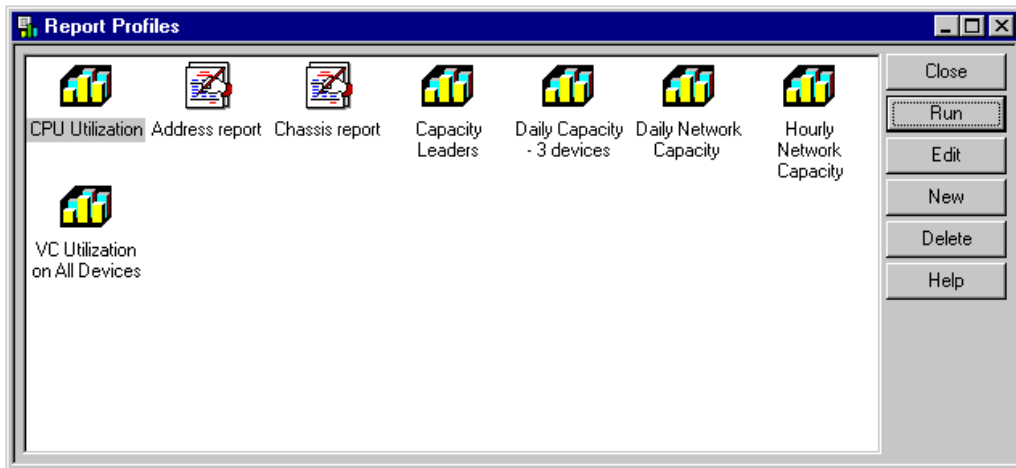
- Data must have been gathered for the report. Remote Access data is gathered automatically for all Ascend devices that have call logging configured. Network performance data is gathered by running data gathering applications using the Schedule Wizard.

### To generate reports:

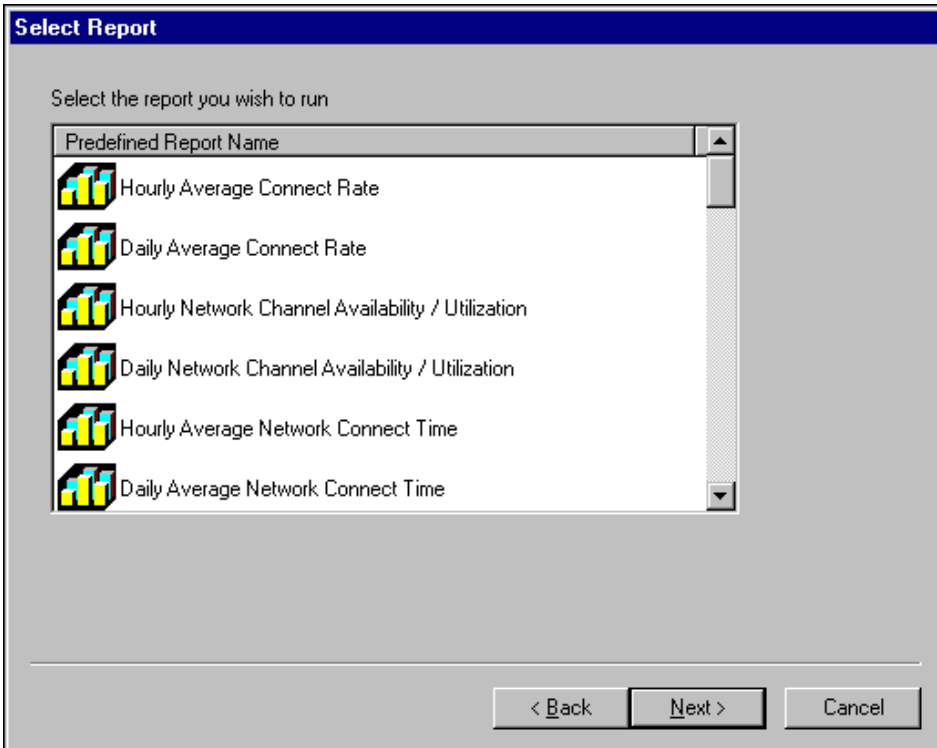
1. Open the Device Database program.
2. Click the [Open the Profile Selection] button to open the Report Profiles window.

## Database and Reporting

---

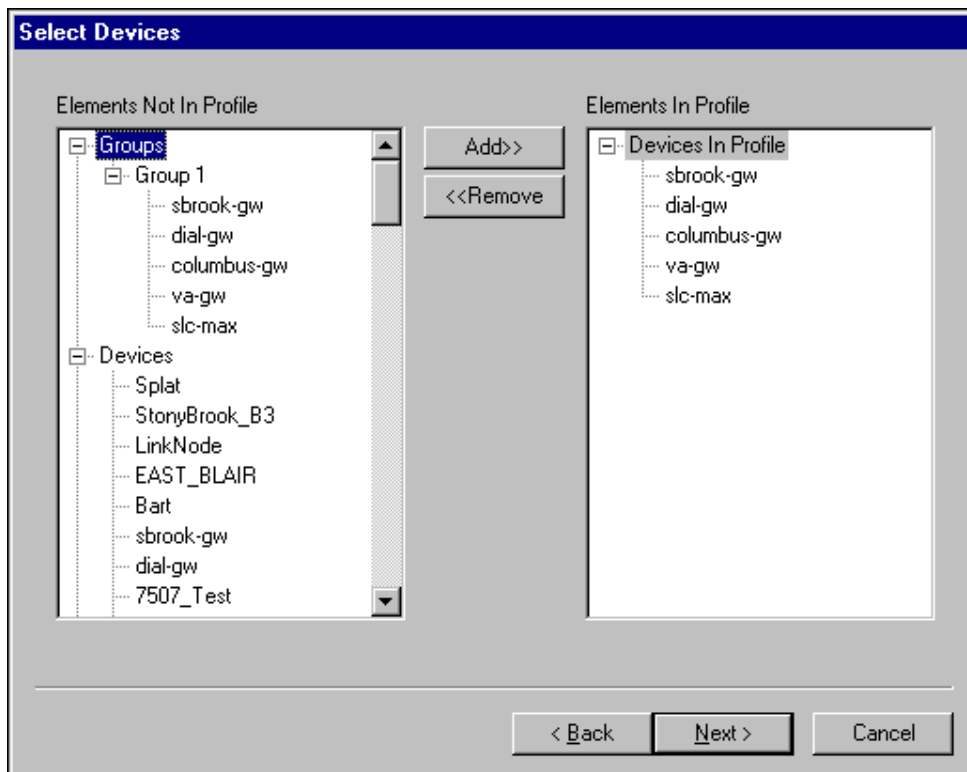


3. Click [New]. The Enter Profile Name screen displays.
4. Specify the name for the profile in the Select Profile Name field.
5. Click [Next]. The Select Report screen displays:



6. Select the report you want associated with this profile. See "Report Details and Samples" (page 292) for details on specific performance reports.
7. Click [Next].

The Select Devices screen displays:



Select the elements you want included in this report. Elements include groups of devices, individual devices, and interfaces on devices (for interface-specific reports). Select the elements from:

### Groups

All groups created in NavisAccess are listed. Groups are configured through the Group Wizard. They are also automatically formed when you group devices while creating a schedule.

### Devices

All devices discovered by NavisAccess and entered into its database are listed.

### Schedules

All devices included in a schedule are listed. This is a convenient way to generate a report on the information that has been gathered by a particular schedule.

8. Click [Next]. The screen that appears will vary, based on the type of report selected.

### Remote Access Reports

For Remote Access reports the following screen appears:

Select Time Range / Display Format

Begin Time: 00:00

End Time: 23:59

Display Format

☒ Display Data Averaged For The Group

☐ Display Data Specific To Each Device

< Back   Next >   Cancel

Make selections for the following fields:

#### Begin Time/End Time

Enter the time period you wish the report to cover. The default values of 00:00 (12:00 AM) and 23:59 (11:59 PM) cover a full day.

## Database and Reporting

---

### Display Data Averaged For The Group

This option will generate a single graph that displays aggregate data for all devices selected. For example, the Daily Logins report would show the total number of logins for all devices combined.

### Display Data Specific to Each Device

This option will generate separate graph lines for each device selected.

### Network Performance Reports

For network performance reports, the following screen appears (some fields may not appear, depending on the type of report selected):

**Select Time Range / Num Interfaces / Sort By**

Begin Time: 00:00

End Time: 23:59

Top N Leaders: 10

Sort By:  
☒ Received  
☐ Sent

Top N field found only in "Network Capacity Leaders" and "Frame Relay Network Capacity Leaders" reports.

Sort By field found only in "Frame Relay Network Capacity Leaders" report.

< Back   Next >   Cancel

Make selections for the following fields:

**Begin Time/End Time**

Enter the time period you wish the report to cover. The default values of 00:00 (12:00 AM) and 23:59 (11:59 PM) cover a full day.

### Top N Leaders

Generates report data for the top N interfaces (or top N virtual circuits for Frame Relay) from the total number of devices specified in the Select Devices window. **Capacity Leaders** reports only.

### Sort By Received/Sent

Sorts Top N virtual circuits in descending order based on amount of data **received by** or **sent by** the devices connected to the virtual circuit. For example, with **Top N** set to 20 and **Sort By** set to Received, the report would show the 20 virtual circuits that have the highest percentage of CIR utilization in terms of data received. Please note, that due to variations in sending and receiving rates, changing the **Sort By** parameter might change which devices appear in a report.

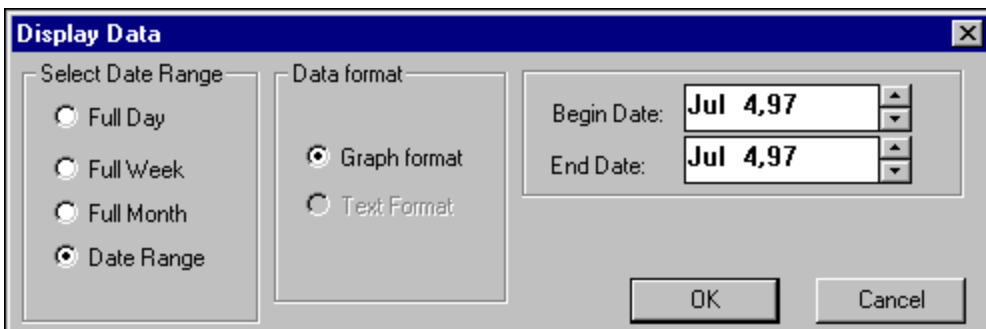
10. Click [Next]. The Profile Creation Finished screen displays.
11. Click [Finish]. This completes the report profile creation process. An icon that represents the profile you created is added to the profile screen.

## Running, editing and deleting performance reports

After creating a report in the Report Profiles window, the report must be generated.

### To run a report:

1. Select the report profile you want to run from those available in the profiles field.
2. Click the [Run] button, or right-click on the report and select **Run**.  
For performance-based reports, the Display Data window displays:



Make selections from the following fields:

### Select Date Range

Specify the range of dates you want included in the report.

**Full Day:** the last full day (not the current day).

**Full Week:** the last full Sunday to Saturday period.

**Full Month:** the last full month (not the current month).

**Date Range:** allows selection of a specific date range. See Begin Date/End Date below.

### Data Format

Specify the format in which you want the data displayed, either Graph or Text (not available for all reports).

### Begin Date/End Date

Specify an exact date range. The Date Range option must be selected in the Select Date Range field to activate this feature.

3. When you are finished specifying your options, click [OK]. The report will be generated and will appear on screen.

### Editing a report

Use the [Edit] button to edit a report profile that you have created,. When you edit a profile, you can change any configuration information you originally specified, such as devices selected. Note that you cannot change the *type* of report, only the parameters.

**To edit a report profile:**

1. Select the report profile to edit from those available in the profiles field.
2. Click the [Edit] button, or right-click on a report and select **Edit**

The configuration screens will appear containing your original profile selections. Change the specifications according to your needs.

### Deleting a report

Use the [Delete] button to delete a profile from the Reports Profiles screen. To delete a report profile:

1. Select the report profile you want to delete from those available in the profiles field.
2. Click [Delete].

## Creating Configuration and Query Reports

Configuration and Query reports are used to search through the NavisAccess device database and return information based on devices selected and/or ad hoc queries. Before generating a report, please note the following:

- Reports can only be generated for devices that have been discovered by NavisAccess.
- A configuration report can only be generated for devices which have had configuration files downloaded into the NavisAccess configuration file database.

The following sections explain how to create configuration and query reports.

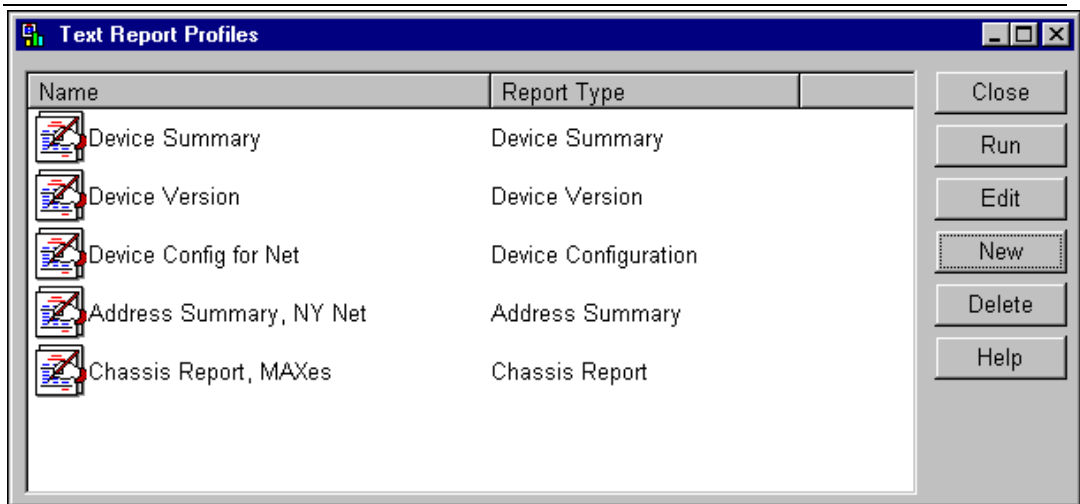
## Creating an Address Summary report

The Address Summary report displays the network addresses for each interface on a device.

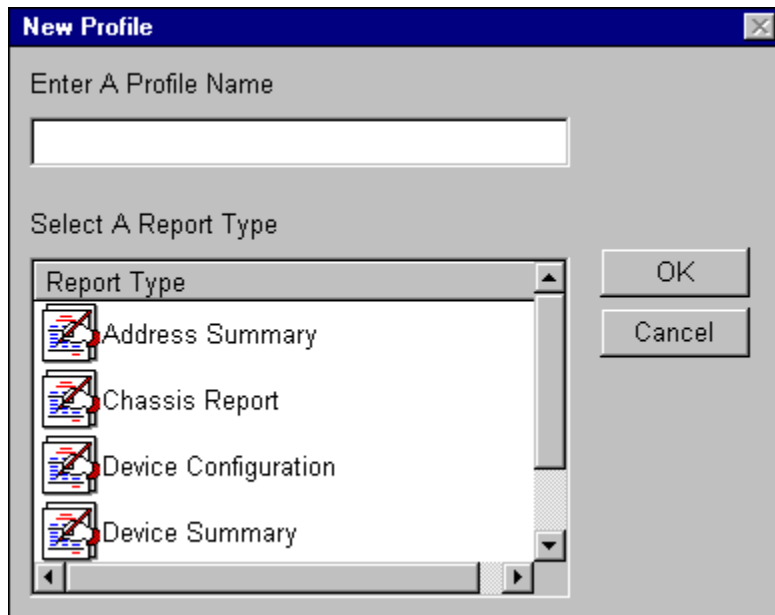
### To create the report:

1. Open the Device Database program.
2. From the main menu, select **File > Text Profiles** to open the Text Report Profiles window.

## Database and Reporting

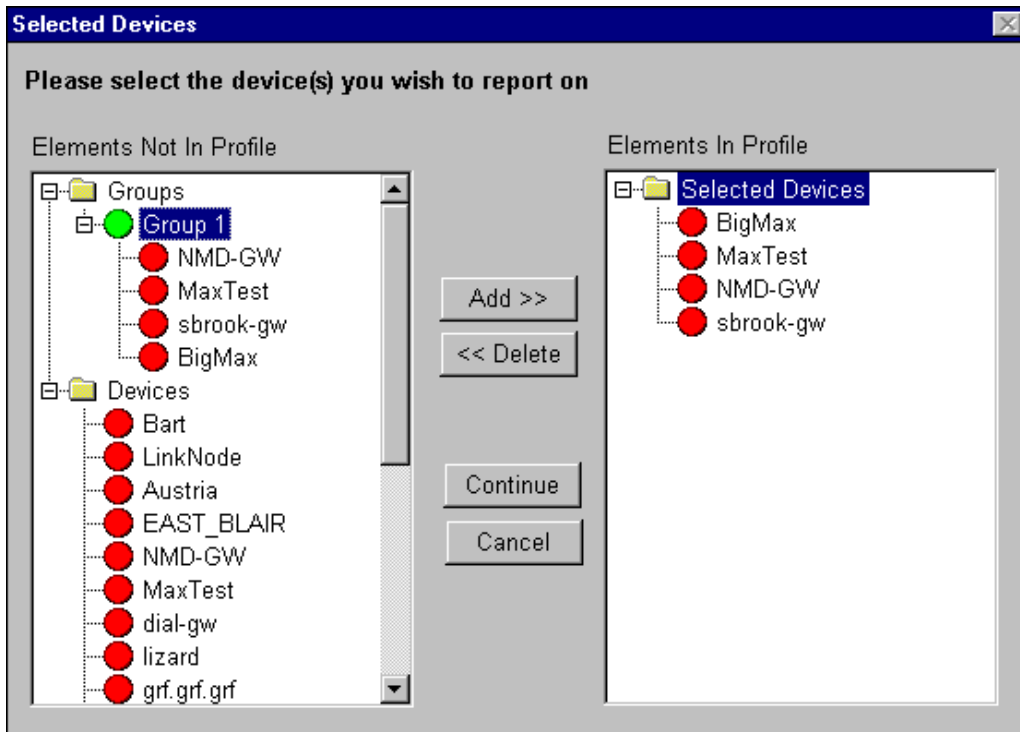


3. Click [New]. The New Profile screen displays:



4. Specify the name for the profile in the Enter a Profile Name field.
5. Select **Address Summary** from the Report Type list.

6. Click [OK] to open the Selected Devices screen:



Select the elements you want included in this report. Elements include groups of devices and individual devices. Select the elements from:

### Groups

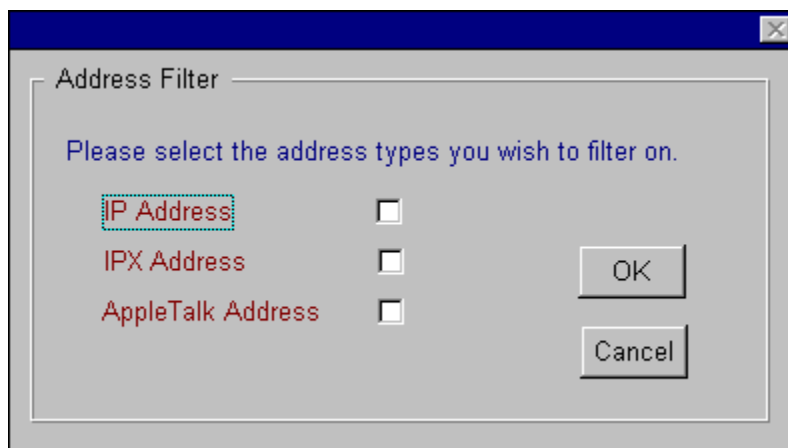
All groups created in NavisAccess are listed. Groups are configured through the Group Wizard.

### Devices

All devices discovered by NavisAccess and entered into its database are listed.

To add a group of device, highlight it and click the [Add] button. Or, you can just double-click on the name.

7. Click [Continue] to open the Address Filter screen.



Select the type of addresses you wish to search for and click [OK].

8. The Address Summary report will automatically be displayed. You can save both the report and the report profile, allowing you to rerun the report at a later time with updated data.

## Creating a Chassis Report

The Chassis Report searches for specific chassis information on a device, or for full chassis information.

### To create the report:

1. Open the Device Database program.
2. From the main menu, select **File > Text Profiles** to open the Text Report Profiles window.
3. Click [New]. The New Profile screen displays:
4. Specify the name for the profile in the Enter a Profile Name field.
5. Select **Chassis Report** from the Report Type list.
6. Click [OK] to open the Selected Devices screen:

Select the elements you want included in this report. Elements include groups of devices and individual devices. Select the elements from:

### Groups

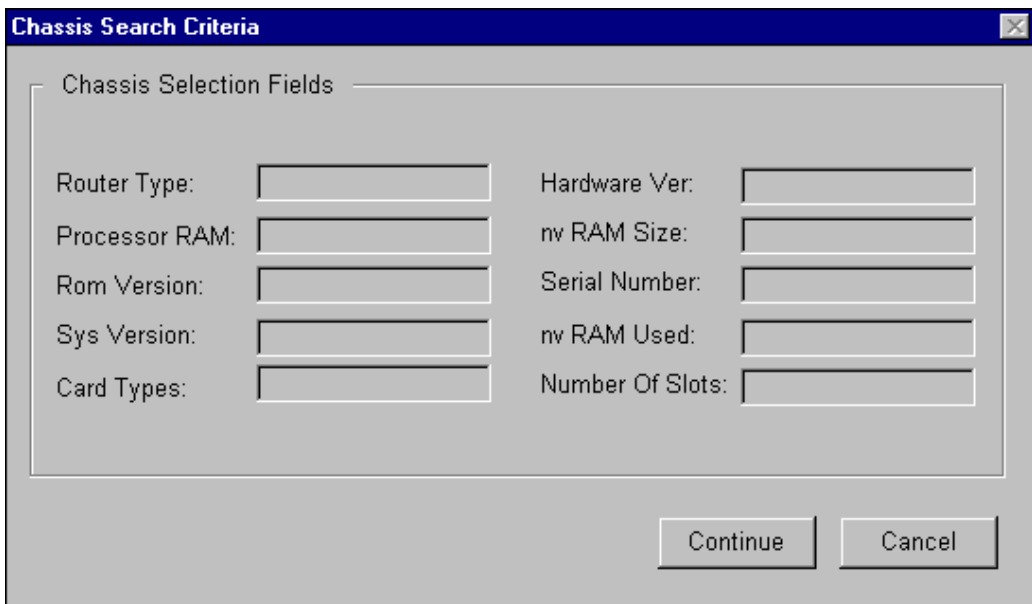
All groups created in NavisAccess are listed. Groups are configured through the Group Wizard.

### Devices

All devices discovered by NavisAccess and entered into its database are listed.

To add a group of device, highlight it and click the [Add] button. Or, you can just double-click on the name.

7. Click [Continue] to open the Chassis Search Criteria screen.



The image shows a Windows-style dialog box titled "Chassis Search Criteria". It has a blue title bar with a close button in the top right corner. The main area is a light gray rectangle with a thin border. Inside this area, the text "Chassis Selection Fields" is followed by a horizontal line. Below this line, there are ten text input fields arranged in two columns. The left column contains: "Router Type:", "Processor RAM:", "Rom Version:", "Sys Version:", and "Card Types:". The right column contains: "Hardware Ver:", "nv RAM Size:", "Serial Number:", "nv RAM Used:", and "Number Of Slots:". Each label is followed by an empty rectangular text box. At the bottom right of the dialog box, outside the main gray area, are two buttons: "Continue" and "Cancel".

There are two options at this point. You can leave the screen blank, in which case it will return chassis reports for all selected devices. Or, you can enter strings into selected fields to search for only those devices that include that information.

For example, you could enter "lanModemP12" in the Card Types field to search the selected devices for those that contain this card. If you are not sure of what to enter, run a blank chassis report for a device you know contains the item you are looking for. The report will then contain the value in proper format.

8. Click [Continue] to display the Chassis Report. You can save both the

report and the report profile, allowing you to rerun the report at a later time with updated data.

### Creating a Device Configuration report

The Device Configuration report searches through saved configuration files for specific text strings.

**NOTE:** A configuration report can only be generated for devices which have had configuration files downloaded into the NavisAccess configuration file database.

#### To create the report:

1. Open the Device Database program.
2. From the main menu, select **File > Text Profiles** to open the Text Report Profiles window.
3. Click [New]. The New Profile screen displays:
4. Specify the name for the profile in the Enter a Profile Name field.
5. Select **Device Configuration** from the Report Type list.
6. Click [OK] to open the Selected Devices screen:

Select the elements you want included in this report. Elements include groups of devices and individual devices. Select the elements from:

#### Groups

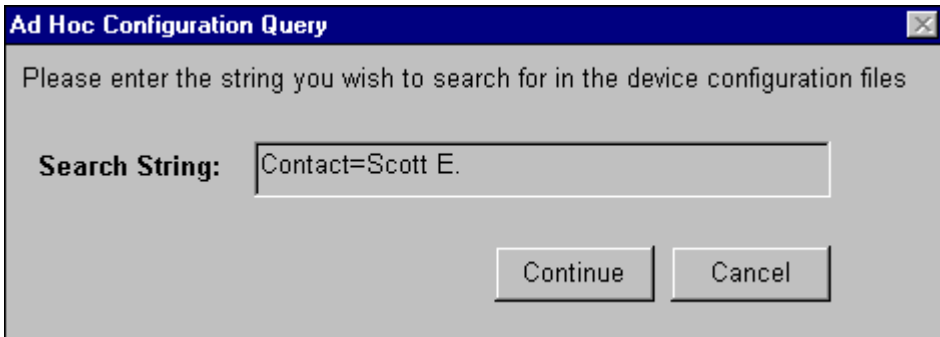
All groups created in NavisAccess are listed. Groups are configured through the Group Wizard.

#### Devices

All devices discovered by NavisAccess and entered into its database are listed.

To add a group of device, highlight it and click the [Add] button. Or, you can just double-click on the name.

7. Click [Continue] to open the Ad Hoc Configuration Query screen.

A screenshot of a Windows-style dialog box titled "Ad Hoc Configuration Query". The dialog has a blue title bar with a close button in the top right corner. The main area is light gray and contains the text "Please enter the string you wish to search for in the device configuration files". Below this text is a label "Search String:" followed by a text input field containing the text "Contact=Scott E.". At the bottom right of the dialog are two buttons: "Continue" and "Cancel".

**Ad Hoc Configuration Query**

Please enter the string you wish to search for in the device configuration files

**Search String:**

Enter the text string you wish to search for in the configuration files of the selected devices.

For example, you may wish to locate all the devices that have a particular person as a device contact. In this case, you would enter "Contact=*contact\_name*".

If you are not sure of the syntax used, you can retrieve a stored configuration file using the Configure Router applet and read through it to locate the proper syntax.

8. Click [Continue] to display the Device Configuration Report. You can save both the report and the report profile, allowing you to rerun the report at a later time with updated data.

### Creating a Device Summary report

The Device Summary report returns a list containing device name, manufacturer, software version, and managed IP address.

#### To create the report:

1. Open the Device Database program.
2. From the main menu, select **File > Text Profiles** to open the Text Report Profiles window.
3. Click [New]. The New Profile screen displays:
4. Specify the name for the profile in the Enter a Profile Name field.
5. Select **Device Summary** from the Report Type list.
6. Click [OK] to open the Selected Devices screen:

Select the elements you want included in this report. Elements include groups of devices and individual devices. Select the elements from:

#### Groups

All groups created in NavisAccess are listed. Groups are configured through the Group Wizard.

#### Devices

All devices discovered by NavisAccess and entered into its database are listed.

To add a group of device, highlight it and click the [Add] button. Or, you can just double-click on the name.

7. Click [Continue] to display the Device Configuration Report. You can save both the report and the report profile, allowing you to rerun the report at a later time with updated data.

## Creating a Device Version report

The Device Version report searches through the database to locate devices running a particular level of software.

### To create the report:

1. Open the Device Database program.
2. From the main menu, select **File > Text Profiles** to open the Text Report Profiles window.
3. Click [New]. The New Profile screen displays:
4. Specify the name for the profile in the Enter a Profile Name field.
5. Select **Device Version** from the Report Type list.
6. Click [OK] to open the Selected Devices screen:

Select the elements you want included in this report. Elements include groups of devices and individual devices. Select the elements from:

### Groups

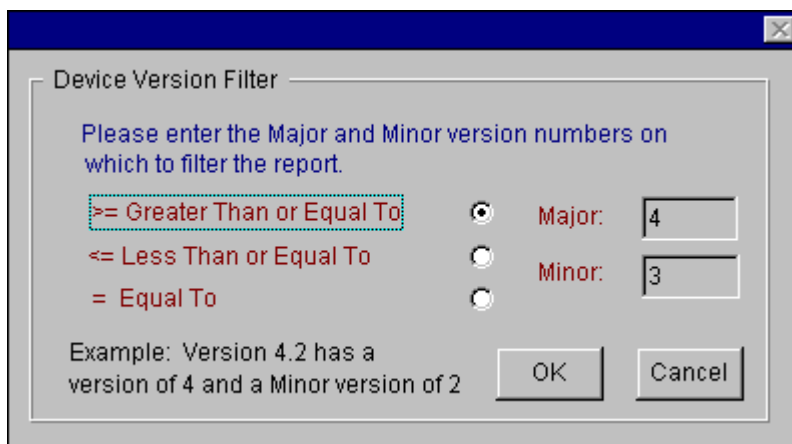
All groups created in NavisAccess are listed. Groups are configured through the Group Wizard.

### Devices

All devices discovered by NavisAccess and entered into its database are listed.

To add a group of device, highlight it and click the [Add] button. Or, you can just double-click on the name.

8. Click [Continue] to open the Device Version Filter screen.



The screen allows you to enter a major and minor version number to search for. For example, if you were looking for software version 4.3, you would enter 4 as the Major number and 3 as the Minor.

You can further define your search by looking for any version number greater than, less than or equal to this number.

9. Click [Continue] to display the Device Version Report. You can save both the report and the report profile, allowing you to rerun the report at a later time with updated data.

## Creating an Account Disconnect report

The Account Disconnect report returns a list of all call disconnect reasons and progress types for a specified time period. The report also provides the number of times each disconnect reasons was reported, and the percentage in terms of all calls.

### To create the report:

1. Open the Device Database program.
2. From the main menu, select **File > Text Profiles** to open the Text Report Profiles window.
3. Click [New]. The New Profile screen displays:
4. Specify the name for the profile in the Enter a Profile Name field.

5. Select **Account Disconnect** from the Report Type list.

6. Click [OK] to open the Selected Devices screen:

Select the elements you want included in this report. Elements include groups of devices and individual devices. Select the elements from:

#### Groups

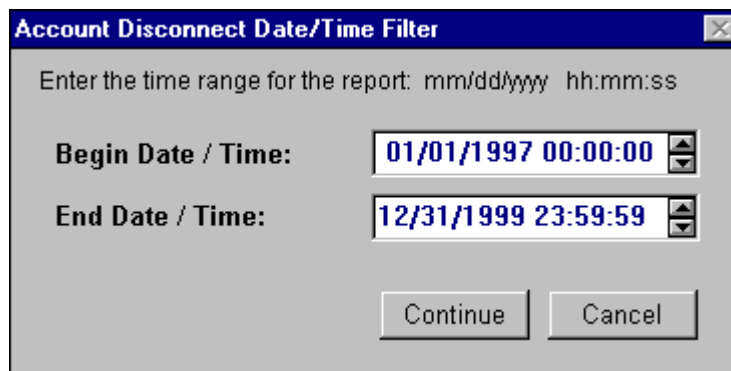
All groups created in NavisAccess are listed. Groups are configured through the Group Wizard.

#### Devices

All devices discovered by NavisAccess and entered into its database are listed.

To add a group of device, highlight it and click the [Add] button. Or, you can just double-click on the name.

7. Click [Continue] to open the Date/Time Filter screen.



Enter a Begin Date and End Date for the period you wish to report on.

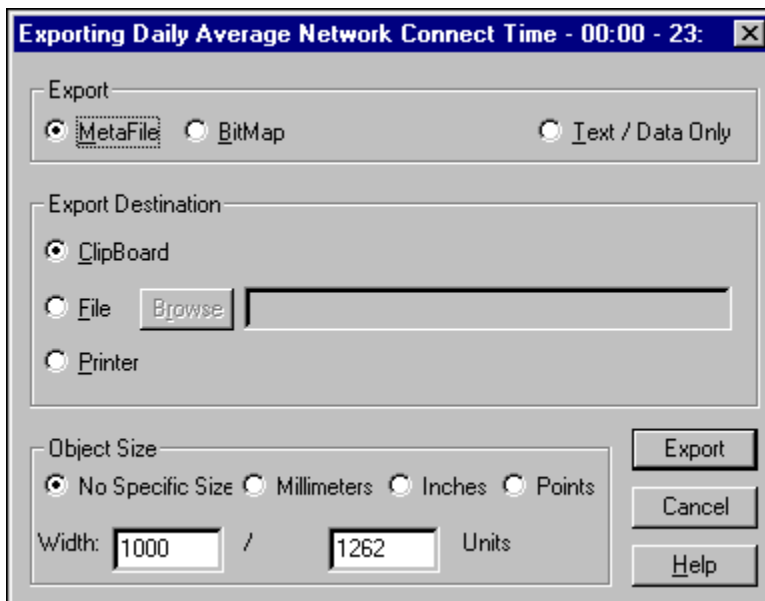
8. Click [Continue] to display the Account Disconnect Report. You can save both the report and the report profile, allowing you to rerun the report at a later time with updated data.

## Exporting graph data

Graph data can be exported as a MetaFile, Bitmap or as text/data.

#### To export data:

1. Select an open graph and click the [Export Graph Points] button.



Fields on the screen will change based on selections in the Export field. Choose from the following:

### **Export**

Select either a MetaFile, a BitMap, or Text/Data only.

### **Export Destination**

Select the ClipBoard, a File, or a Printer. If you select to export to a file, use the [Browse] button to select a directory to which to export.

### **Object Size**

Select a specific size for the graph.

2. When you are finished selecting your options, click the [Export] button.

## **Publishing Web reports**

DeviceDB allows you to convert reports into HTML format for publication on a Web server. A daily and weekly report directory is automatically created, allowing simple access to the reports. If reports are configured to run daily and weekly, the most recent reports for the given day or week are always included.

**To publish Web reports:**

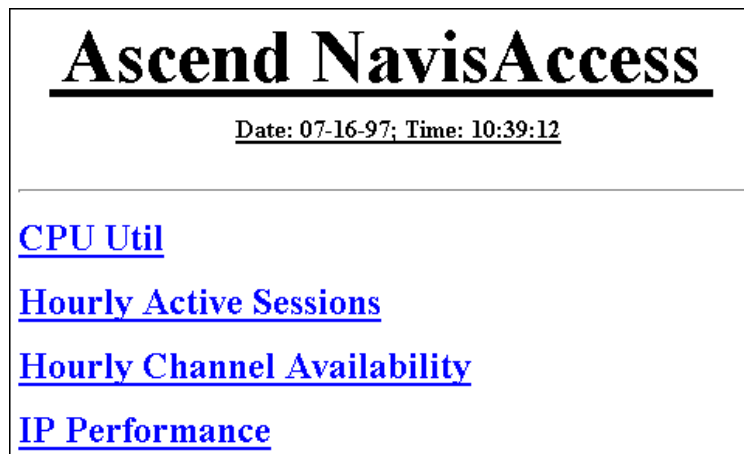
1. Run a report in DeviceDB.
2. With the report on screen, click the [Publish to Web] button.

The report will automatically be converted into HTML format, and a directory structure will be generated. The directory will be created in the location specified in the NavisAccess Configuration options under the WebReport tab.

### Accessing the reports

By default, reports are placed in a directory called **rootreportdir**. Each report generates its own sub-directory, named after the report name. For example, if you name a report "Hourly Active Sessions" when you create it, there will be an **Hourly Active Sessions** sub-directory under rootreportdir.

Within rootreportdir is an index file called MASTER.HTML. Clicking on this file opens a master index which lists all the HTML reports. For example:



The blue links connect to each of the reports that have been run. Clicking on a blue link opens the report index. For example:

# **Ascend NavisAccess**

Date: 07-16-97; Time: 10:34:19

---

[Monday Report](#)

[Tuesday Report](#)

[Wednesday Report](#)

[Thursday Report](#)

[Friday Report](#)

[Saturday Report](#)

[Sunday Report](#)

---

[Week One Report](#)

[Week Two Report](#)

[Week Three Report](#)

[Week Four Report](#)

This index provides access to the most recent daily reports for the past week, and the most recent weekly reports for the past month. Clicking on a report link opens the page index for the specific report. For example:

# **Ascend NavisAccess**

**Date: 07-16-97; Time: 10:34:19**

**Schedule Name: IP Performance**

**Report Name: IP Protocol Performance**

**This is a daily report for Wednesday**

**[Page1 of the report.](#)**

**[Page2 of the report.](#)**

**[Page3 of the report.](#)**

**[Page4 of the report.](#)**

**[Page5 of the report.](#)**

This screen lists the Schedule Name (user defined name) and the Report Name (the system name). Individual report page links are provided. Clicking on a link will open the corresponding report

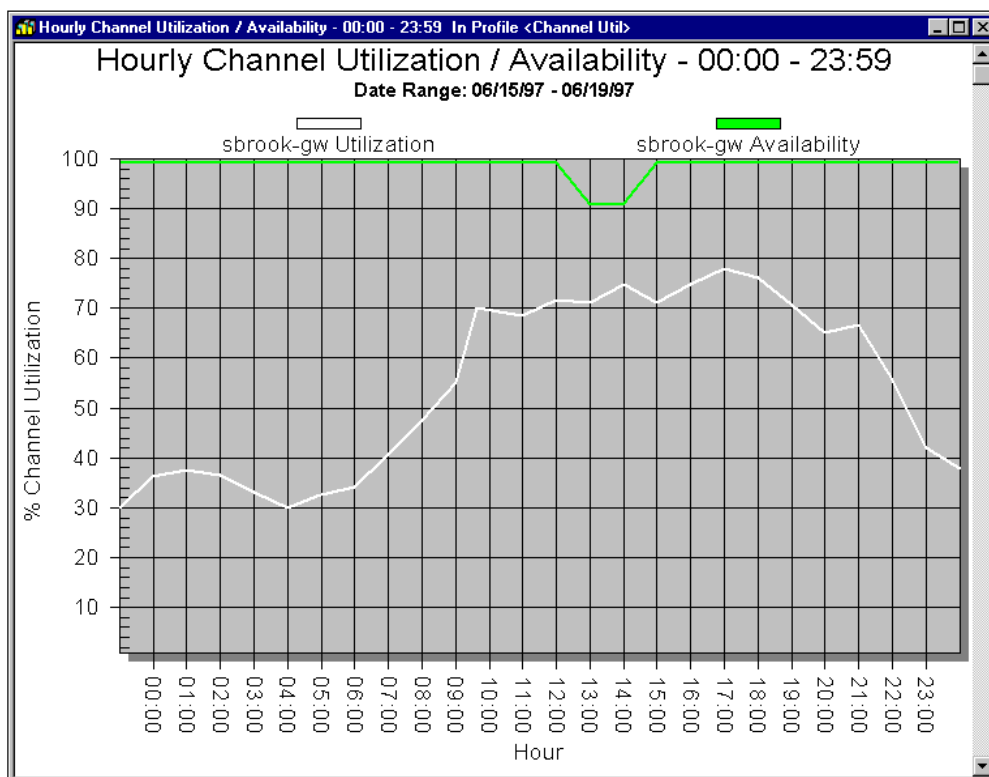
## Report details and samples

### Remote Access Reports

#### Hourly/Daily Network Channel Availability/Utilization

The Network Channel Availability/Utilization reports generate graphs which plot the percentage of channel availability and utilization for individual devices or aggregate data for groups of devices on an hourly or daily basis.

Below is a sample of an Hourly chart for an individual device. To see other devices, click on the down scroll bar.



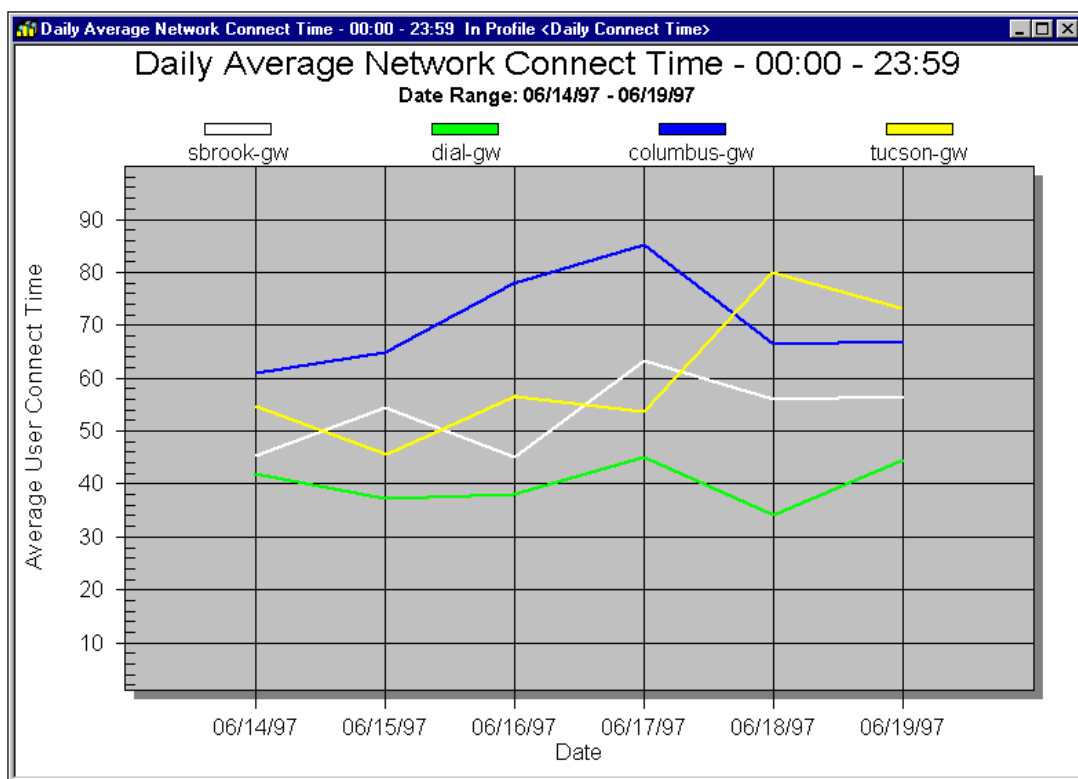
This report graphs one line showing the Channel Utilization over time, and another line showing the Channel Availability. In the graph above, Availability is almost always 100% for the day, while Utilization rises and falls

over the course of the day. Peak utilization reaches 80%. This information is vital for capacity planning.

### Hourly/Daily Average Network Connect Time

The Average Network Connect Time reports generate graphs which plot the average user connect time for individual devices or aggregate data for groups of devices on an hourly or daily basis.

Below is a sample of a Daily chart for an individual devices. Up to four devices will be displayed in one graph. To see more devices, click on the down scroll bar.

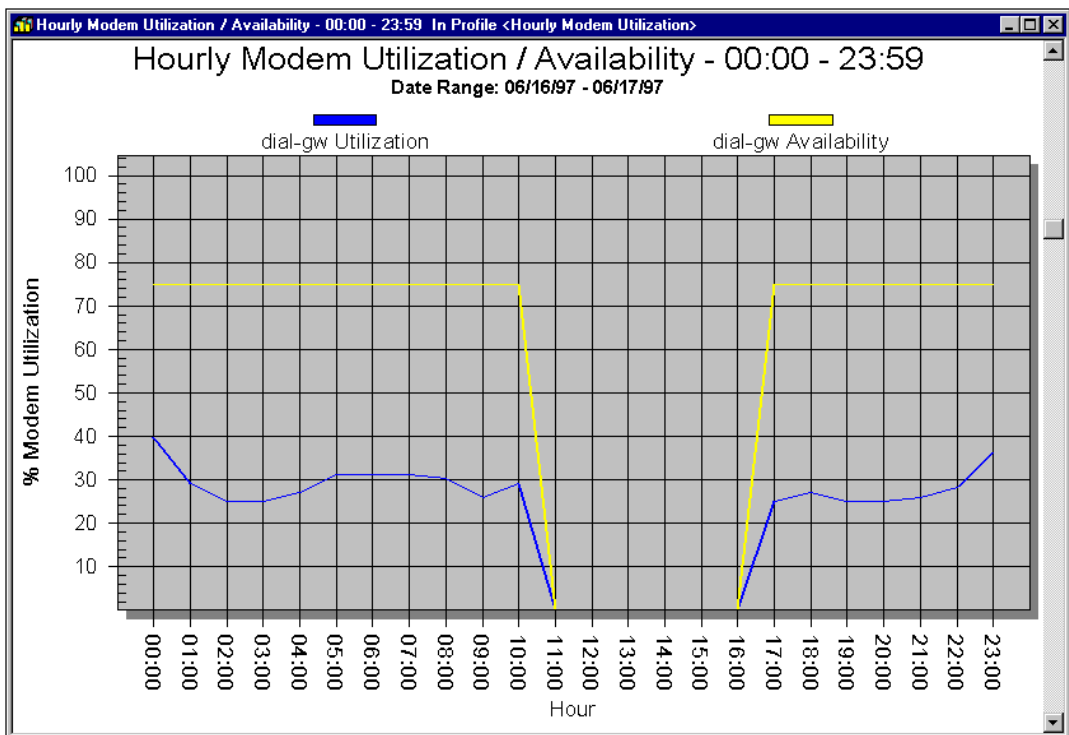


This graph displays average user connect time for four devices over the course of six days. Each device is graphed individually. You could also generate graphs showing aggregate connect time for the group.

## Hourly/Daily Modem Availability/Utilization

The Modem Availability/Utilization reports generate graphs which plot the percentage of modem availability and utilization for individual devices or aggregate data for groups of devices on an hourly or daily basis.

Below is a sample of an Hourly chart for an individual device. If more than one device is included in the report, click on the down scroll bar to see other devices.

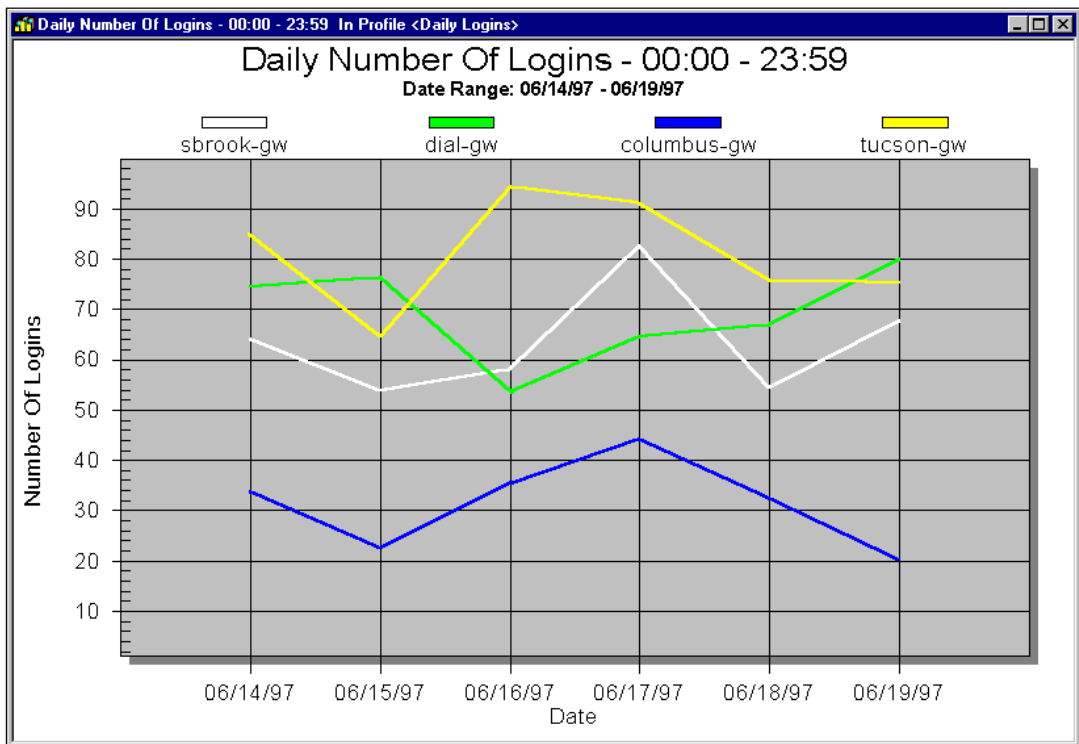


The chart above shows a consistent level of modem utilization until 11:00 a.m., when availability drops to zero. Clearly, this indicates the device was taken off-line or failed some time between 10 and 11 a.m. The device was restored between 4 and 5 p.m. (16:00 - 17:00) and service resumed close to the previous level.

### Hourly/Daily Number of Logins

The Number of Logins reports generate graphs which plot the number of logins for individual devices or aggregate data for groups of devices on an hourly or daily basis.

Below is a sample of a Daily chart for individual devices. Up to four devices will be displayed in one graph. To see more devices, click on the down scroll bar.

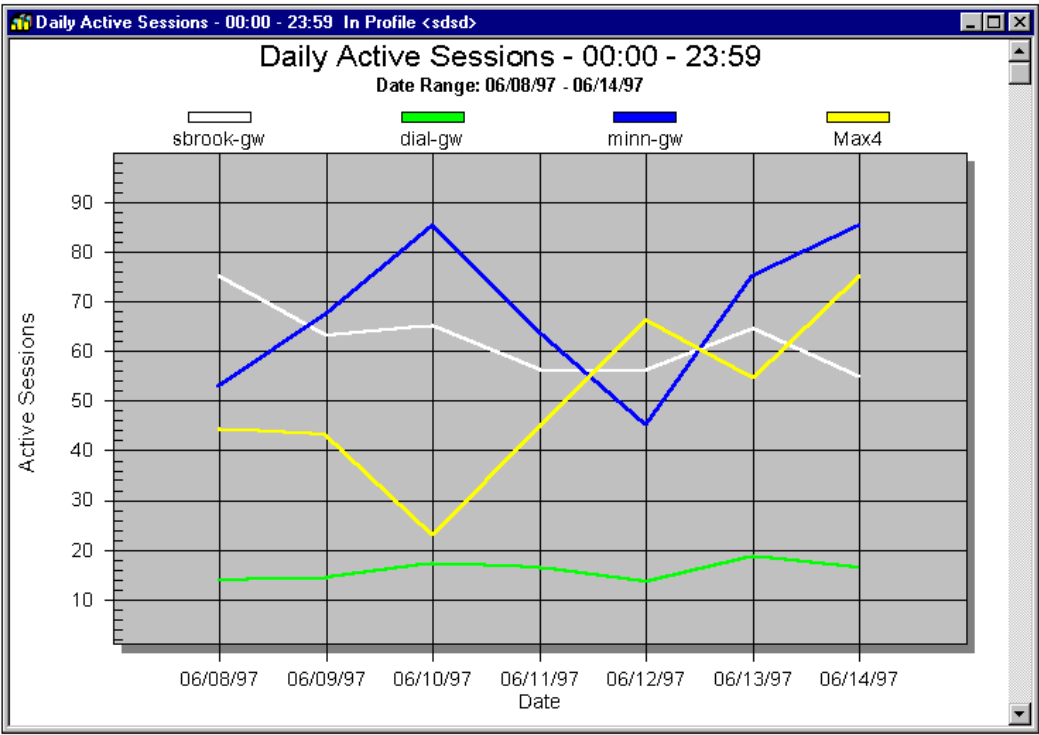


This graph displays the daily number of logins for four devices over the course of six days. Each device is graphed individually. You could also generate graphs showing aggregate number of logins for the group.

### Hourly/Daily Active Sessions

The Active Sessions reports generate graphs which plot the number of active sessions recorded for individual devices or aggregate data for groups of devices on an hourly or daily basis.

Below is a sample of a Daily chart for individual devices. Up to four devices will be displayed in one graph. To see more devices, click on the down scroll bar.



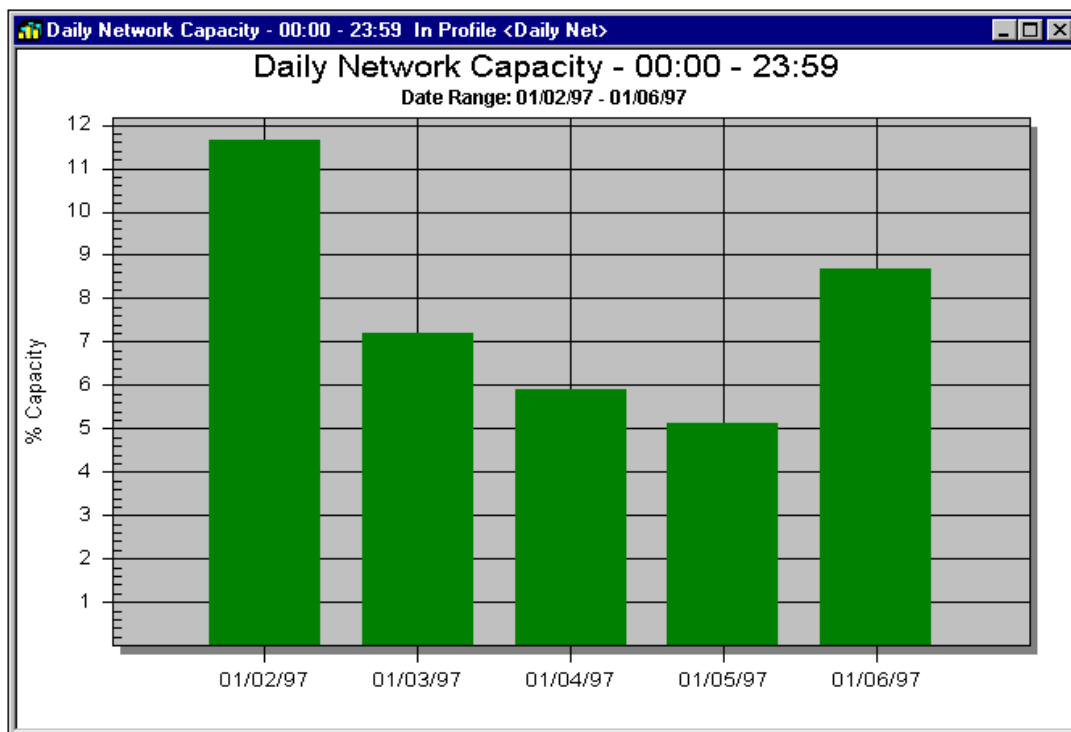
This graph displays the daily number of active sessions for four devices over the course of six days. Each device is graphed individually. You could also generate graphs showing aggregate number of sessions for the group.

## Network Performance Reports

### Daily Network Capacity

This report generates a bar graph that plots the percentage of utilized network capacity over a number of days. Each bar represents one network utilization number for that day. A representative utilization number is generated by averaging the utilization from the different interfaces on the included devices over the complete set of hours selected.

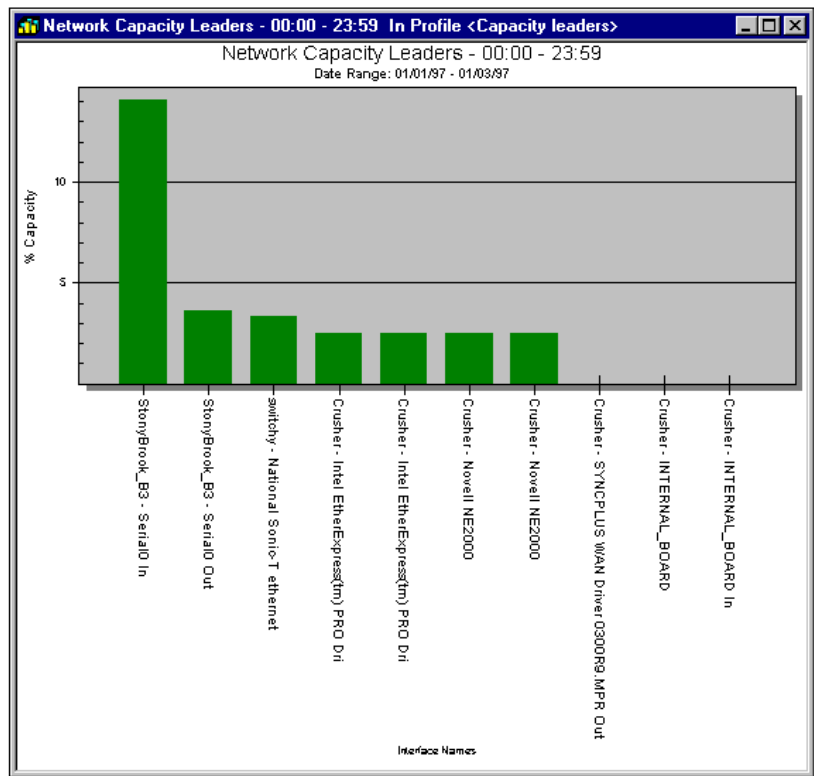
A sample report is shown below:



Data for this report is collected using the Background Interface Utilization schedule in the Schedule Wizard.

### Network Capacity Leaders

This report generates a graph that plots the ten interfaces with the highest percentage of used capacity for a selected time and date range. Each bar represents one device. A representative utilization number is generated by averaging the utilization from each interface on every included device over the selected time and date range. Each half (input and output) of a full duplex serial interface is treated as a separate interface.



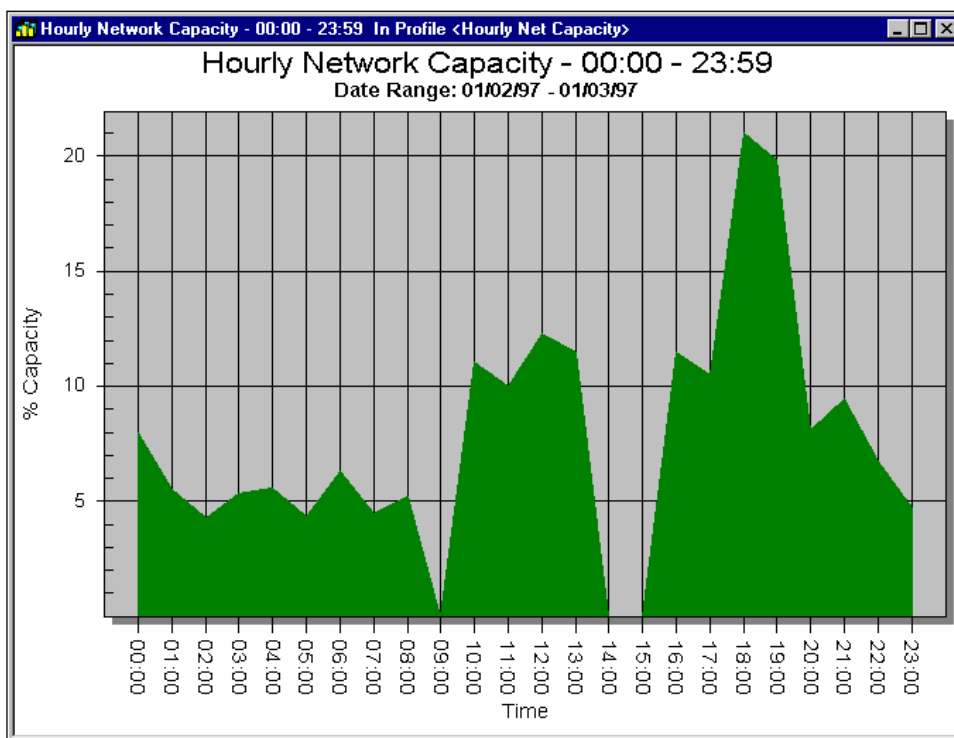
The report above shows the top ten interfaces in terms of network capacity. Looking at the first two bars, you can see that the device StonyBrook\_B3 is shown with input and output separately.

Data for this report is collected using the Background Interface Utilization schedule in the Schedule Wizard.

### Hourly Network Capacity

This report generates a mountain graph that plots the utilized network capacity over a selected time of day. A representative utilization number is generated by averaging the utilization from the different interfaces on the included devices.

This graph provides a clear overview of network usage over the given period.

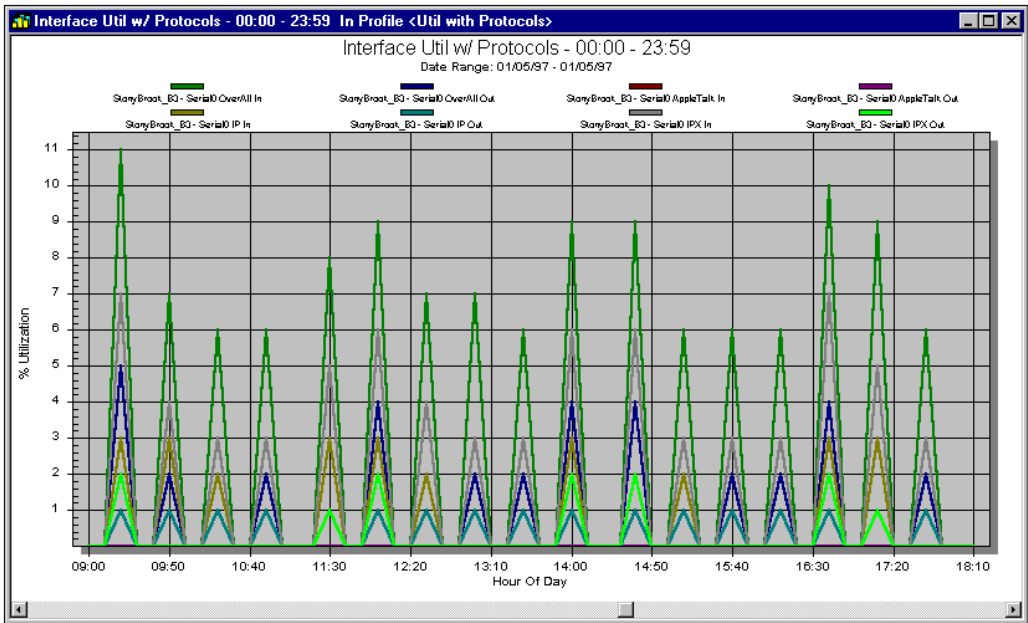


The graph above shows network usage over a 24-hour period. The network capacity only once rises above 20%, showing a network that has a lot of extra bandwidth available. Usage drops to zero right before 9:00 a.m. and then rises significantly, perhaps showing that the network went down and was restarted. Also, between the hours of 2:00 and 3:00 p.m. the network again seems to have dropped to zero, showing that it may have been inaccessible during that time.

Data for this report is collected using the Background Interface Utilization schedule in the Schedule Wizard.

## Interface Utilization With Protocols

This report generates a line graph that plots the interface utilization and the individual protocol utilization for the specified hours of a day. There is a maximum of four series per interface (IP, IPX, AppleTalk, and Overall), except for full duplex serial interfaces which may have eight, corresponding to one for input and one for output. The calculation for each data point on a series is the average overall percentage utilization over the previous ten minutes. A sample report is shown below.



The graph above shows interface utilization on one device (StonyBrook\_B3) on January 5, between the hours of 9:00 a.m. and 6:00 p.m.

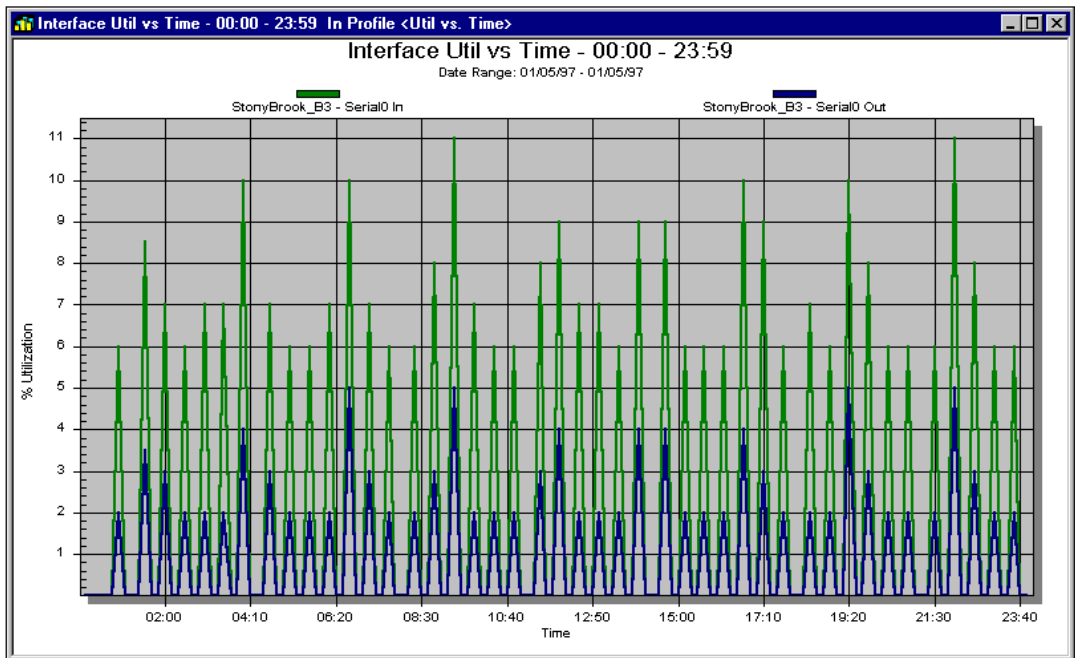
The highest peaks on the graph, in green, are the overall utilization rate. This rate is broken down into individual protocols in the graph. For example, the busiest individual protocol was incoming IPX (shown in gray). The least used is AppleTalk, which does not appear on the graph at all.

Data for this report is collected using the Background Interface Utilization schedule in the Schedule Wizard.

### Interface Utilization Versus Time

This report generates a line graph that plots the interface utilization for the specified hours of a day. There is one series per interface, except for full duplex serial interfaces which have two: one for input and one for output. The calculation for each data point on a series is the average overall percentage utilization over the previous ten minutes.

A sample report is shown below.

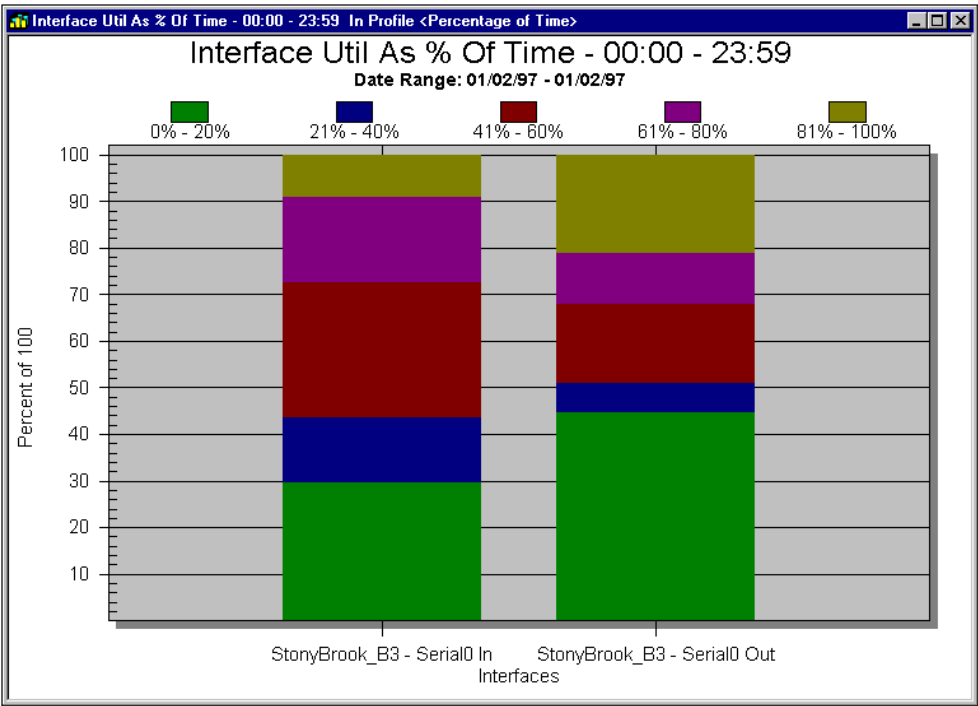


In the above report, both input and output for the device StonyBrook\_B3 are shown over a 24-hour period. It is clear that input is consistently higher than output, while neither one is particularly high, reaching a maximum level of 11 percent.

Data for this report is collected using the Background Interface Utilization schedule in the Schedule Wizard.

### Interface Utilization As A Percentage Of Time

This report generates a stacked bar graph that plots the percentage of a selected time period that an interface was within a specified utilization range. Each interface has its own single bar, except for full duplex interfaces, which have two bars: one for input and one for output. Each interface type has an associated set of utilization ranges against which data is compared to determine the percentage of total data that fell into each specified range.

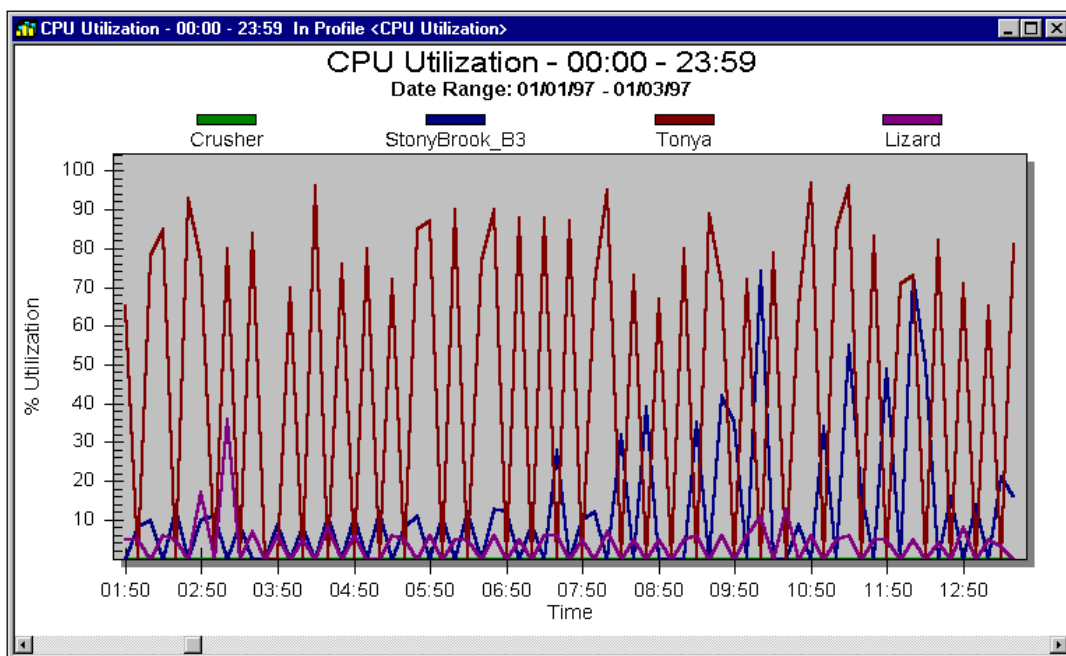


From the chart above, we can learn that on January 2, the **Serial0 In** interface of device **StonyBrook\_B3** ran between 0 and 20% of capacity for 30% of the day. It ran at 21-40% of capacity for 14% of the day, at 41%-60% of capacity for 28% of the day, at 61%-80% of capacity for 18% of the day, and at 81%-100% of capacity for 8% of the day. Similar readings can be seen for the Out interface. Data for this report is collected using the Background Interface Utilization schedule in the Schedule Wizard.

### CPU Utilization

This report generates a line graph that plots the percentage utilization of the CPUs of selected devices versus a specified time of day.

**NOTE:** The CPU Utilization report is not currently available for Ascend devices.



The graph above shows CPU utilization for four devices over a three day period, approximately between the hours of 1:00 a.m. and 1:00 p.m. It is clear that the CPU utilization of device **Tonya** consistently spikes to very high levels, often over 90%. Device **StonyBrook\_B3** had low utilization until about 7:00 a.m. when CPU utilization began to rise significantly, until dropping off around 12 noon. Device **Lizard** maintained a consistent level through most of the period. And device **Crusher**, barely visible along the very bottom of the graph, shows a utilization level too low to register.

Data for this report is collected using the Background CPU Utilization schedule in the Schedule Wizard.

## AppleTalk Protocol Performance

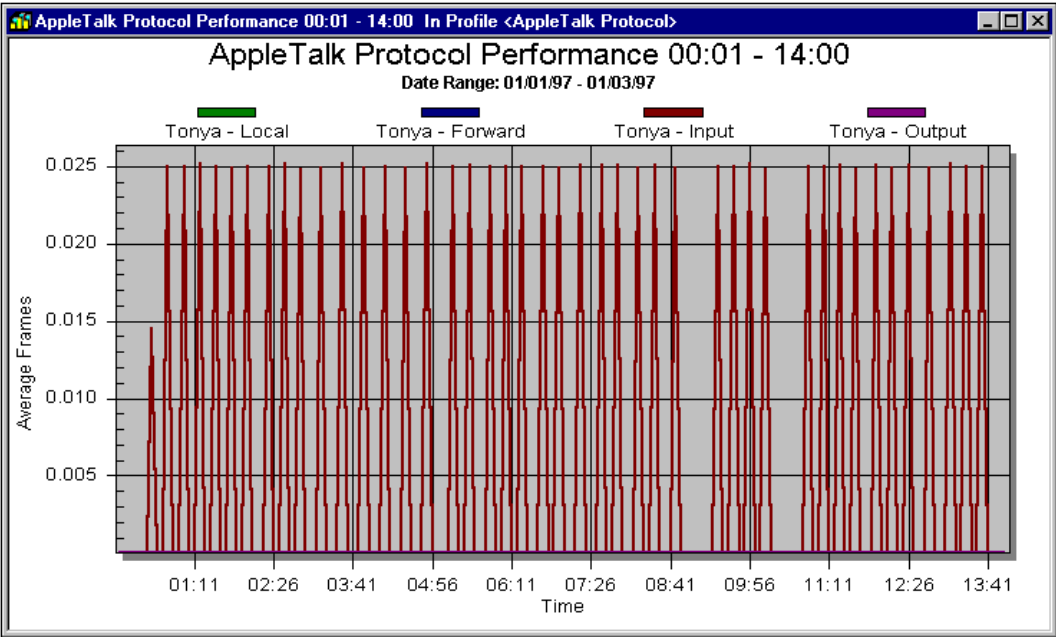
This report generates a line graph showing AppleTalk packet statistics over a given time period. Four separate variables are graphed for each device:

**Input** - The number of datagrams received by the device.

**Output** - The number of datagrams sent by the device.

**Local** - The number of incoming datagrams for which forwarding was not required.

**Forward** - The number of datagrams forwarded by the device.



Data for this report is collected using the Background AppleTalk Performance schedule in the Schedule Wizard.

### IP Protocol Performance

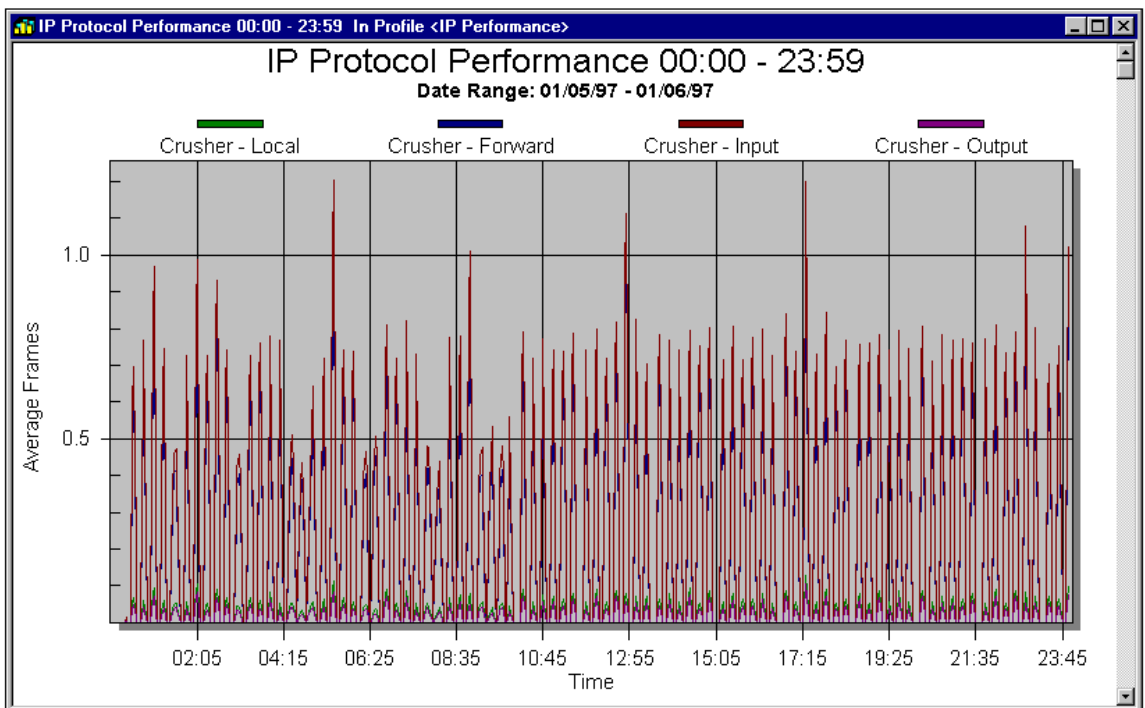
This report generates a line graph showing IP packet statistics over a given time period. Four separate variables are graphed for each device:

**Input** - The number of datagrams received by the device.

**Output** - The number of datagrams sent by the device.

**Local** - The number of incoming datagrams for which forwarding was not required.

**Forward** - The number of datagrams forwarded by the device.

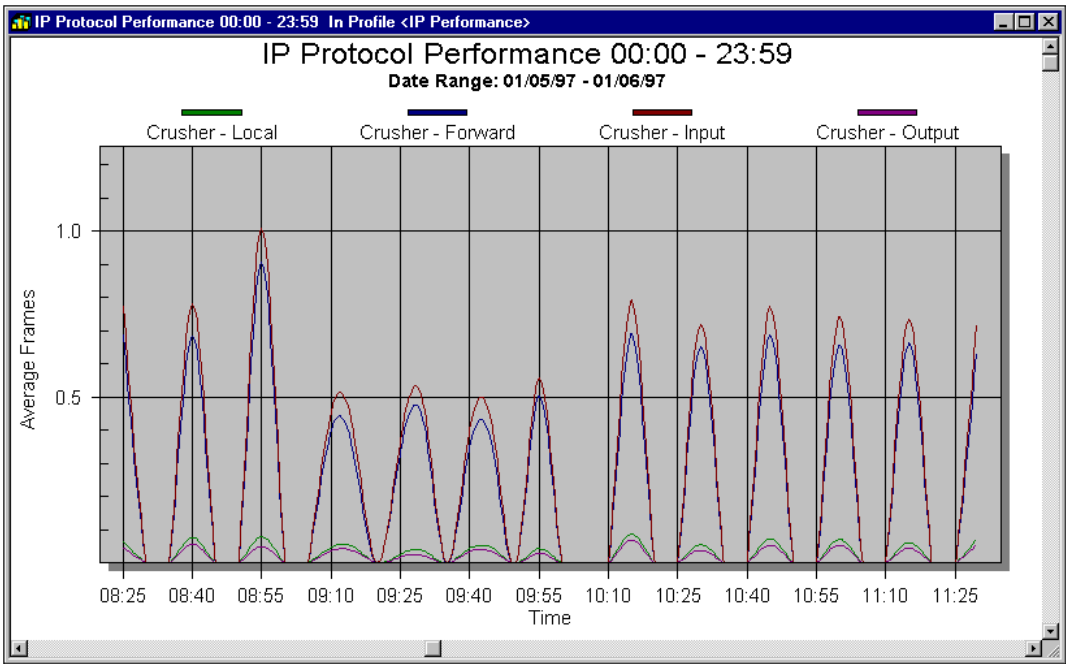


The graph above shows IP Protocol performance for device Crusher. Four different values are charted for this device.

There are a few things to note about this graph. First, devices other than Crusher were selected for this report. To view the next device, click the down

scrollbar. Each selected device has a separate graph.

Also, due to the closeness of the "input" (**dark red**) and "forward" (**dark blue**) readings, it is hard to distinguish them on the graph. However, by zooming in on a selection of data, the graph lines will widen and the lines will distinguish themselves. Below is the same graph as above, zoomed in between the hours of 8:30 a.m. and 11:30 a.m. Note how the input and forward readings now are separately readable, with forward consistently just a hair below input.



### IPX Protocol Performance

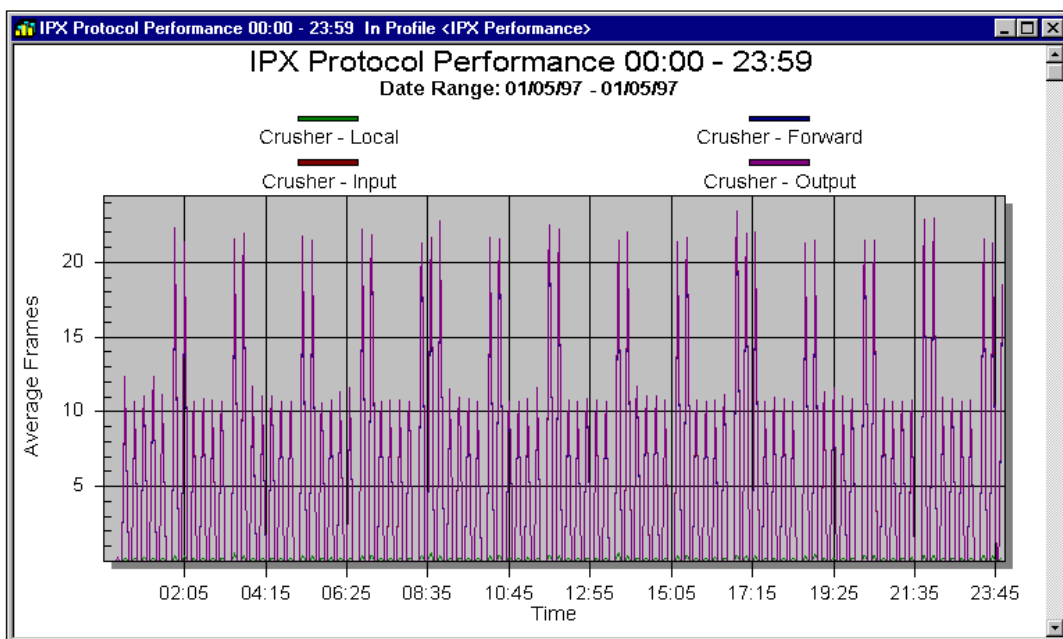
This report generates a line graph showing IPX packet statistics over a given time period. Four separate variables are graphed for each device:

**Input** - The number of datagrams received by the device.

**Output** - The number of datagrams sent by the device.

**Local** - The number of incoming datagrams for which forwarding was not required.

**Forward** - The number of datagrams forwarded by the device.



Data for this report is collected using the Background IPX/SPX Performance schedule in the Schedule Wizard.

### Frame Relay VC Utilization

This report shows the level of utilization for the selected virtual circuits as a

percentage of the CIR. Each channel on the virtual circuit is shown on a separate page, with Sent and Received information shown as bar graphs, and Virtual Circuit Throughput shown as a line graph overlay. To understand the complete **A-to-B** and **B-to-A** circuit, you will need to view two separate graphs.

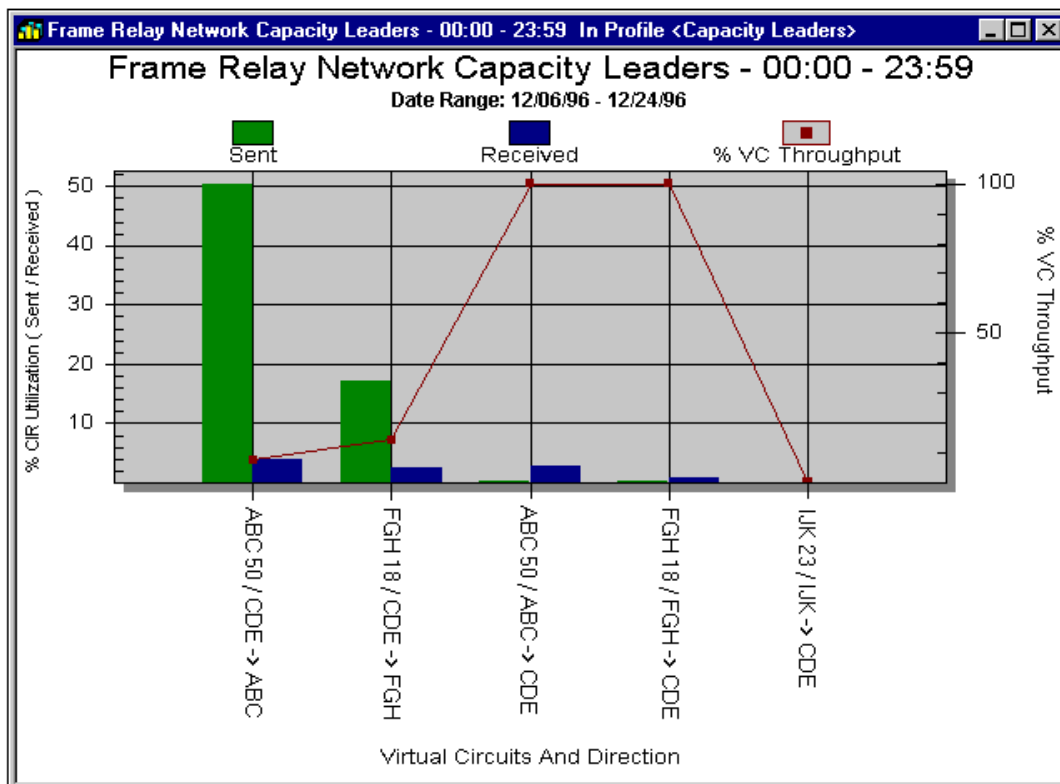
To view the next graph, click the down button on the scroll bar.

Data for this report is collected using the Background CIR Trending schedule in the Schedule Wizard.

## Frame Relay Network Capacity Leaders

This report displays the top N virtual circuits in terms of CIR utilization. N is the number of circuits reported on, determined by user selection when the report is run. The default value is top 10.

Reports show virtual circuit channel utilization plotted as a percentage of CIR (Committed Information Rate). The graph can be sorted based on either data "sent" or data "received" on the virtual circuit channel. This must be selected at the time the report is created.



In the above graph, % VC Throughput equals the data received on a virtual circuit channel as a percentage of the data sent. Note that the % VC Throughput scale is on the *right* side y-axis.

A virtual circuit channel is a full duplex line and has two directions of data

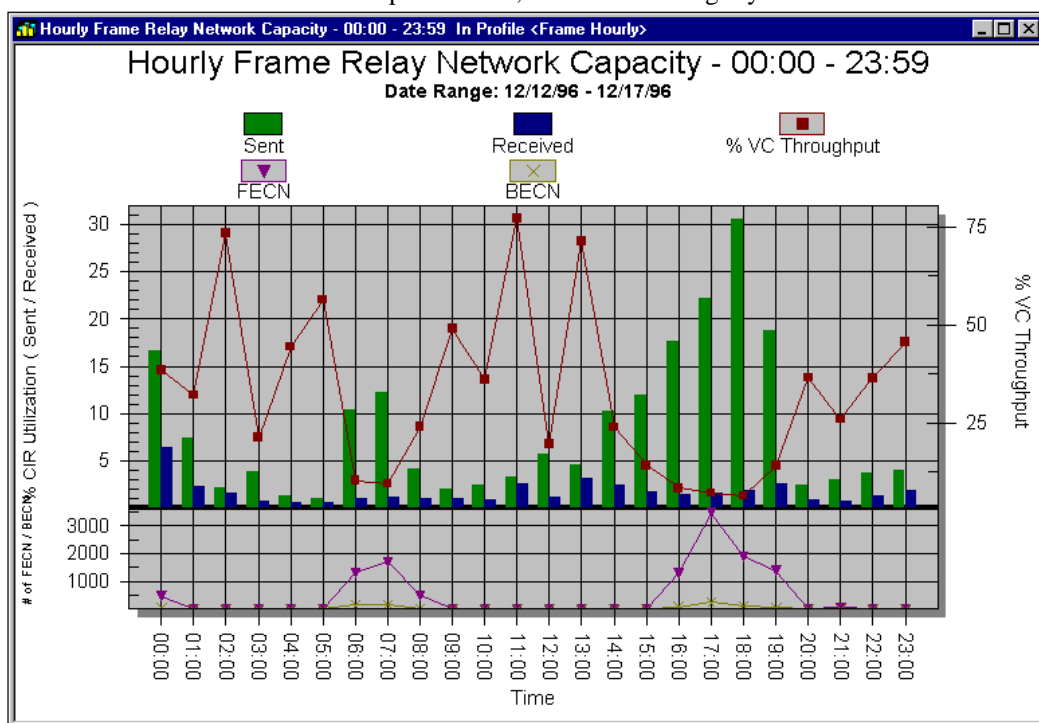
flow, from Device A to Device B, and from Device B to Device A. A virtual circuit channel represents either an A→B flow or a B→A flow. Each virtual circuit has two channels.

Data for this report is collected using the Background CIR Trending schedule in the Schedule Wizard.

## Frame Relay Hourly Network Capacity

This report generates a bar graph that plots the utilization of Frame Relay network capacity over a selected time of day. The bar graph plots the Sent and Received Frame Relay network capacity for each hour. Virtual circuit throughput is plotted as a line graph and *corresponds to the right-side Y-axis*. It may be scaled differently than the CIR utilization on the left Y-axis.

FECN and BECN statistics are plotted separately at the bottom of the graph, and also have a separate scale, located on the right y-axis.



The sample report above shows network capacity average during the hours between 7 a.m. and 6 p.m. each day from 12/12 to 12/17.

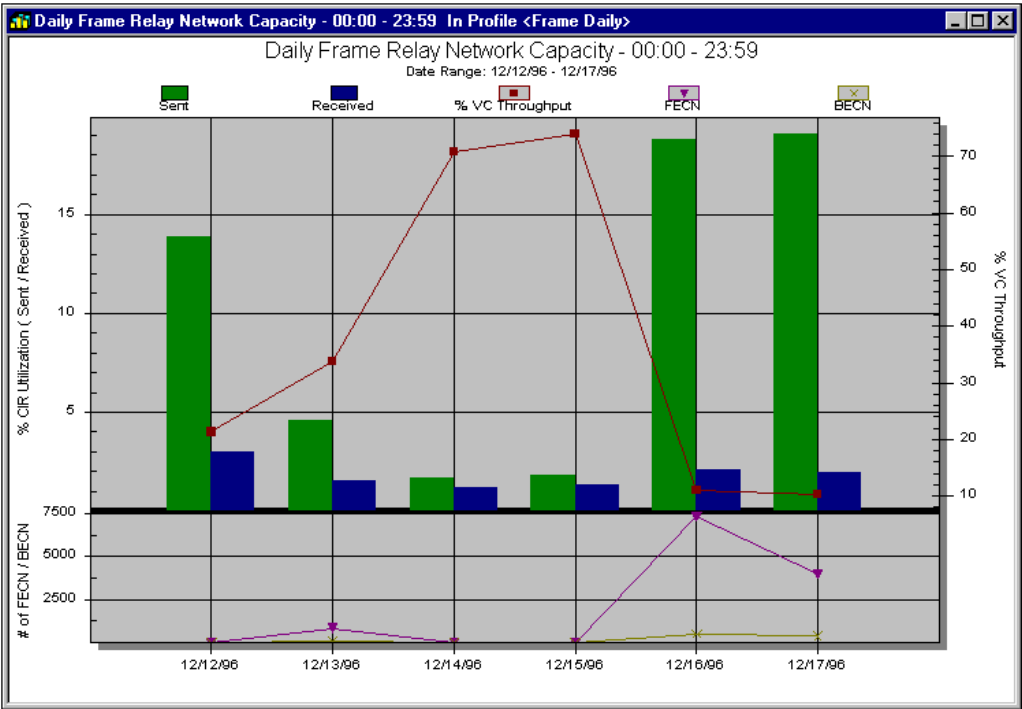
**FECN** (Forward Explicit Congestion Notification): The number of frames received from the network indicating forward congestion.

**BECN** (Backward Explicit Congestion Notification): The number of frames received from the network indicating backward congestion.

Data for this report is collected using the Background CIR Trending schedule in the Schedule Wizard.

Frame Relay Daily Network Capacity

This report generates a bar graph that plots the utilization of Frame Relay network capacity over a selected number of days. The bar graph plots the Sent and Received frame relay network capacity for each day. Virtual circuit throughput is plotted as a line graph and *corresponds to the right-side Y-axis. It may be scaled differently than the CIR utilization on the left Y-axis.* FECN and BECN statistics are plotted separately at the bottom of the graph, and also have a separate scale, located on the right y-axis.



**FECN** (Forward Explicit Congestion Notification): The number of frames received from the network indicating forward congestion.

**BECN** (Backward Explicit Congestion Notification): The number of frames received from the network indicating backward congestion.

Data for this report is collected using the Background CIR Trending schedule

## Database and Reporting

---


in the Schedule Wizard.

### Device Summary Report

The Device Summary Report displays a summary of each device that is selected. The summary includes the following information:

- Device Name
- Manufacturer (Personality)
- Software Version
- Address Managed From

A sample section of a Device report is shown below.

 <b>Device Summary Report</b> <span>7/31/97</span>			
Device Name	Manufacturer	Software Version	Managed IP Address
Bart	Digital	2.0	150.50.11.188
LinkNode	Wellfleet	8.0	150.50.10.23
Austria	3 Com	6.2	150.50.1.97
EAST_BLAIR	Wellfleet	5.0	150.50.22.99
NMD-GW	Ascend	5.0	25.1.1.1

To create a Device Summary Report, see "Creating a Device Summary report" on page 283.

## Address Summary Report

The Address Summary Report displays the interface name and network addresses for each interface on a device. Addresses are returned for the following:

- IP Address
- IPX Address
- AppleTalk Address

A sample section of an Address report is shown below.

# Address Summary Report

7/31/97

## 7507\_Test

Ethernet1/1	IP Address	150.50.23.201
Ethernet1/0	IP Address	150.50.1.253
Ethernet1/0	IP Address	75.1.3.2
Ethernet1/0	AppleTalk	4b050d04b050d14b0
Ethernet1/1	AppleTalk	4b053084b053094b0
Ethernet1/1	IP Address	192.168.30.187
Serial5/1	IP Address	150.50.97.2
Serial5/1	IP Address	150.50.96.2
Ethernet1/0	IP Address	75.1.1.2

---

## grf.grf.grf

lo0	IP Address	127.0.0.1
gs020	IP Address	25.2.1.1
de0	IP Address	25.1.1.39


To create an Address Summary Report, see "Creating an Address Summary

report" on page 277.

### Device Configuration Report

The Configuration Report allows you to specify phrases or parts of phrases that may be in the device configuration file, such as syntax parameters. This launches a search of all stored configurations to identify all devices which match the query.

The report returns the names of all devices that contain the string. A sample section is shown below:

	<h2>Device Configuration Report</h2>	7/31/97
<b><u>Device Name</u></b>		
NMD-GW EAST_BLAIR BigMAX ScottEMax		


To create a Device Configuration Report, see "Creating a Device Configuration report" on page 282.

## Chassis Report

The Chassis Report allows you to specify values for predetermined database fields. This launches a search through the database to find all devices which match these criteria. A Chassis Report is then generated for each device which matches the query.

Alternately, if no search strings are entered, the report will return full chassis information for all selected devices.

A sample section of a Chassis report is shown below. The Serial Number field has deliberately been altered.



### Chassis Search Results

7/31/97

**Router Name:** NMD-GW

**Type:** max4004      **Serial Number:** 1111111      **Hardware Version:**

**# of Slots:** 11      **Processor RAM:** 0      **nv RAM Size:** 0

**nv RAM Used:** 0

**ROM Version:**

**ROM Sys Version:**


Slot #	Card Type	Description	Hardware Vers	Software Vers
1	sysT1	Net/T1		
7	empty	Empty		
3	IanModemP12	Lan Modem/12P		
9	ethernet	Ethernet		
8	empty	Empty		
4	IanModemP12	Lan Modem/12P		
6	empty	Empty		
11	serialWan	Serial WAN		
10	ethernetData	Ether Data		
5	slotBriTE	Net/BRI		

To create a Chassis Report, see "Creating a Chassis Report" on page 280.

### Device Version Report

The Device Version Report allows you to specify values for version numbers of software running on devices. This launches a search through the database to find all devices which match this criteria.

A sample section of a Version report is shown below:

	<b>Device Version Report</b>	7/31/97
Device Name	Version	
BigMax	5.0	
MaxTest	5.0	
NMD-GW	5.0	
sbrook-gw	5.0	

To create a Device Version report, see "Creating a Device Version Report" on page 284.

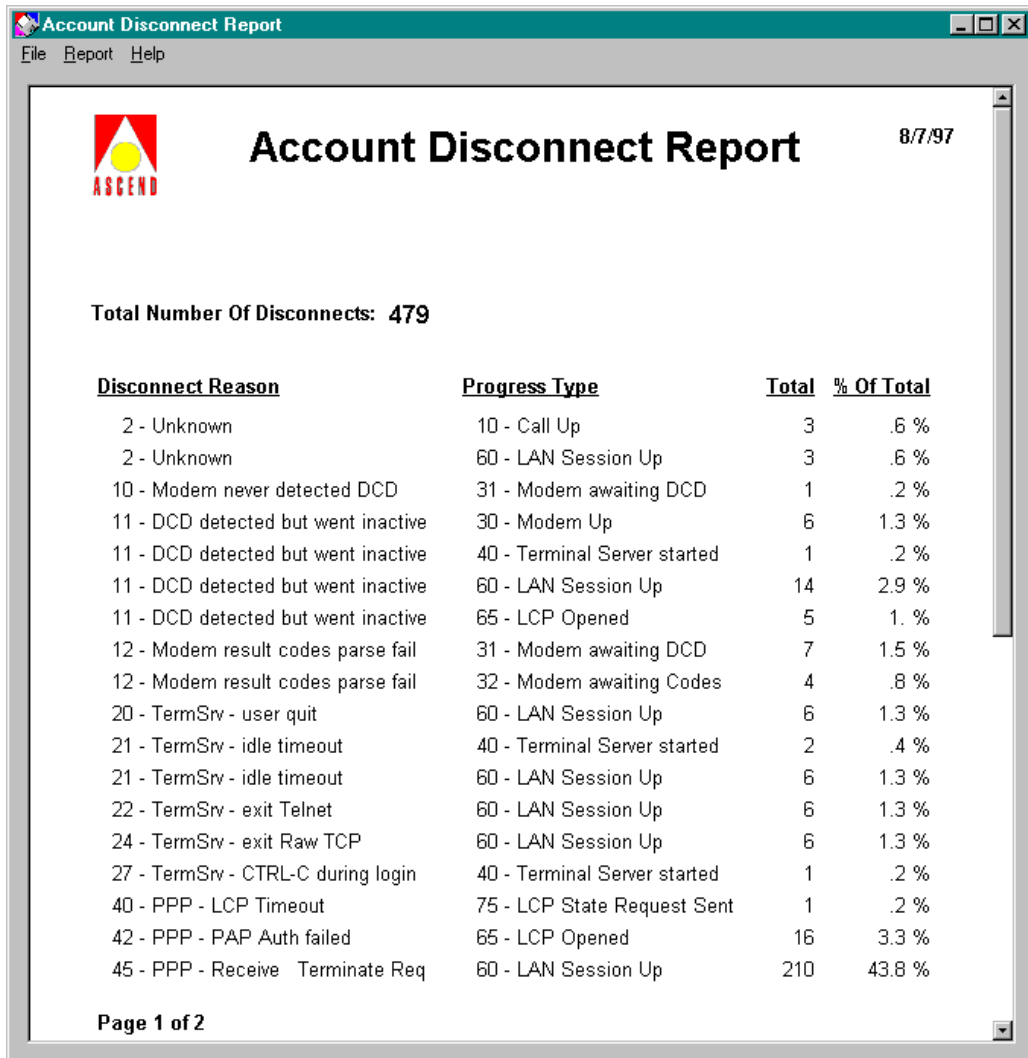
### Account Disconnect Report

The Account Disconnect report returns a list of all call disconnect reasons and progress types for a specified time period. The report also provides the number of times each disconnect reasons was reported, and the percentage in terms of all calls.

This report should be used in conjunction with the Dropped Calls cell in Access Watch in order to identify the reasons that calls are being dropped.

For information about dropped calls and a list of disconnect codes, see [More](#)

about Dropped Calls.



**Account Disconnect Report** 8/7/97

**Total Number Of Disconnects: 479**

<u>Disconnect Reason</u>	<u>Progress Type</u>	<u>Total</u>	<u>% Of Total</u>
2 - Unknown	10 - Call Up	3	.6 %
2 - Unknown	60 - LAN Session Up	3	.6 %
10 - Modem never detected DCD	31 - Modem awaiting DCD	1	.2 %
11 - DCD detected but went inactive	30 - Modem Up	6	1.3 %
11 - DCD detected but went inactive	40 - Terminal Server started	1	.2 %
11 - DCD detected but went inactive	60 - LAN Session Up	14	2.9 %
11 - DCD detected but went inactive	65 - LCP Opened	5	1. %
12 - Modem result codes parse fail	31 - Modem awaiting DCD	7	1.5 %
12 - Modem result codes parse fail	32 - Modem awaiting Codes	4	.8 %
20 - TermSrv - user quit	60 - LAN Session Up	6	1.3 %
21 - TermSrv - idle timeout	40 - Terminal Server started	2	.4 %
21 - TermSrv - idle timeout	60 - LAN Session Up	6	1.3 %
22 - TermSrv - exit Telnet	60 - LAN Session Up	6	1.3 %
24 - TermSrv - exit Raw TCP	60 - LAN Session Up	6	1.3 %
27 - TermSrv - CTRL-C during login	40 - Terminal Server started	1	.2 %
40 - PPP - LCP Timeout	75 - LCP State Request Sent	1	.2 %
42 - PPP - PAP Auth failed	65 - LCP Opened	16	3.3 %
45 - PPP - Receive Terminate Req	60 - LAN Session Up	210	43.8 %

**Page 1 of 2**

To create an Account Disconnect report, see "Creating an Account Disconnect report" on page 286.

### Graph functionality








If a graph contains too many data points, you may not be able to see every label on the x-axis or to distinguish between different graph lines. Use the zoom feature to expand specific areas of the graph to view contents more clearly.


To zoom in on a range of data, hold the right mouse button while you drag to the right over the area of the graph that you want to expand. Press the "Z" key to return to the original graph.

**NOTE:** Certain graphs have different information on each Y-axis (right side and left side). The scales used may also be different. It is very important to read both sides of a graph to make sure you are reading the information correctly.

#### Other buttons

The following options are available for a graph report. Please note that these options are also available from the Graph menu.

Button	Description
	<b>[Print] button</b> Prints the open graph.
	<b>[Print Preview] button</b> Previews how the graph will look when it is printed
	<b>[Toggle Grid Lines] button</b> Toggles the style of grid lines displayed on the graph.
	<b>[Toggle Graph Viewing Style] button</b> Toggle the viewing style of the graph, from color to black-and-white to black-and-white with graph line symbols.
	<b>[Toggle Font Size] button</b> Toggle the font size on the graph through several options.
	<b>[Toggle Forced Vertical Labels] button</b> Forces labeling of the graph's axes to be vertical.
	<b>[Export Graph Points] button</b> Exports graph data as a Metafile, Bitmap or text.

Button	Description
	<b>[Publish to Web] button</b> Generates reports in HTML format, including a pre-configured directory structure, for publication on web pages. See "Publishing Web Reports" on page 288 for details.

# Network Awareness:

## Fault Detection

11

### Fault detection

A key component of network management is to know when something is going wrong. NavisAccess provides a host of tools that let you know exactly what is happening on the network.

There are three basic kinds of fault detection tools. They include:

**Data Gathering Tools:** tools which examine network data for problems, such as error levels or interface up/down status. Information is sent from the data gathering tools to the fault reporting tools. Data gathering tools can be configured by the user. These tools include:

- **Threshold Manager**  
Monitors error levels on devices, based on errors per second. Threshold levels can be set based on protocol (IP, IPX, AppleTalk) or interfaces (Ethernet, Token Ring, etc.). Threshold alarms are reported by the Alarm Monitor in real-time, or can be gathered in the background using the Schedule Wizard.
- **Interface Utilization Thresholds applet**  
Monitors percentage of usage on device interfaces. Usage levels can be set separately for each device interface. Alarms are generated when a set usage level is surpassed. Utilization alarms are reported by the Event Viewer in real-time. This applet works in conjunction with the Schedule Wizard, and a *schedule must be created* for interface utilization to be monitored.
- **Interface Status Thresholds applet**  
Monitors up/down status on device interfaces. Separate up and down time thresholds are set for each interface, and alerts are generated if the threshold is surpassed. Status alerts are reported by the Alert applet in real-time. This applet works in conjunction with the Schedule Wizard, and a *schedule must be created* for interfaces to be monitored.

**Fault reporting tools:** tools which report fault information delivered from the data gathering tools. These tools include:

- **Alarm Monitor**

Reports real-time error information sent from the Threshold Manager applet. Errors are reported for single devices or devices within a group. Summary information is presented for all errors based on error category and severity level.

- **Alert**

Reports real-time up/down status information sent from the Interface Status Thresholds applet. Alerts are reported for single devices.

**Fault consolidation tools:** tools which consolidate data reported by other tools. These tools include:

- **Event Viewer**

Provides a central viewing point for a multitude of real-time information collected from data gathering applications, including error information, up/down interface status, and interface utilization. Summary information is provided based on error category and severity level. Event Viewer also reports errors from the Access Watch application, system traps, and automated upload/download configuration information.

- **Event Report**

Gathers data reported by data gathering tools (error threshold alarms, interface utilization, and interface up/down status) and Access Watch and retains a historical database. This allows you to access historical fault information for all monitored devices and device groups. The database is maintained from the date NavisAccess was installed. Event Report also provides data filtering options, to locate data based on specific criteria, such as date, device, error type, etc.

**Other tools** in the Fault Management system are:

- **Incident Monitor**

Allows you to start the Alarm Monitor and/or Event Report for a single device or a device group.

- **System Log Monitor**

Reports unsolicited network events. Can be configured to report based on severity levels, and can be set to forward messages to the Event Viewer.

- **Trap Forwarder**

Forwards all Traps received by NavisAccess to up to 20 other IP addresses.

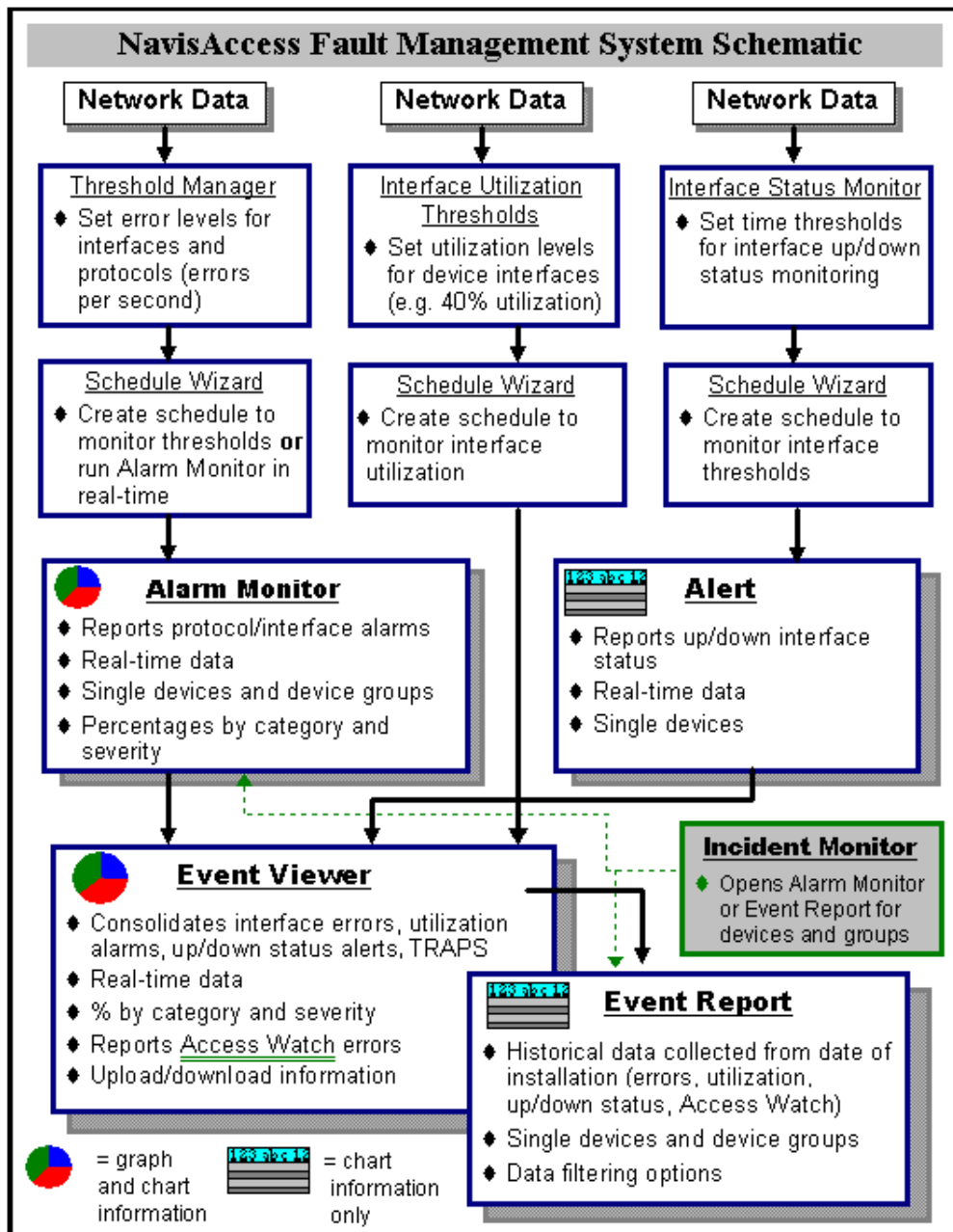
## **Fault Detection**

---

For a diagram outlining the Fault Management system, please see the NavisAccess Fault Management System Schematic below.

## **ACE - Event Correlation**

NavisAccess also provides intelligent monitoring of certain network events through use of the Ascend Correlation Engine (ACE). The ACE system monitors devices and interfaces for consistent patterns of events, rather than individual events. This is a more intelligent means of monitoring, allowing for automated detection of chronic problems that might otherwise go undetected in the midst of multiple network events.



## **Setting error thresholds**

### **The Threshold Manager**

The **Threshold Manager** is used to set alarm thresholds for the following device error classes:

**Protocols:**

- IP
- IPX/SPX (on most brands of device)
- AppleTalk

**Interfaces:**

- System/Interface
- Ethernet
- Token Ring
- FDDI
- Bridge
- Frame Relay

Alarm thresholds define the number of errors which must occur *before* an alarm record is triggered. That is, the number of *errors per second* that must be reached before an alarm is generated.

Thresholds are set based on experience with the actual operation of a specific network, and an understanding of the levels of a particular error which are acceptable for that network. Proper threshold settings reduce the vast number of possible alarms to only those that significantly affect network performance.

Due to the differences between networks, there are no "recommended" levels at which alarm thresholds should be set. However, determining and setting the proper threshold level is a critical step. If the thresholds are too high, warnings may pass unnoticed. If they are too low, an over abundance of "false alarms" will be generated by Alarm Monitor, thus detracting from alerting the user to potential problems.

### Protocols and Interfaces

Protocol-specific buttons are available on the Threshold Manager toolbar for each specific protocol supported. Threshold Manager scans for each protocol's presence on the device, and then checks the settings in Alarm Configuration. If the protocol is active on the device and alarm monitoring is selected in Alarm Configuration, then that protocol button will appear on the toolbar. Similarly, if the protocol is not available or deactivated in Alarm Configuration, it will *not* appear on the toolbar.

Interface buttons are available based upon device type, device version of software, etc. They appear on the toolbar only if they are supported according to the device's criteria. If available on the device, but not configured on an interface, the item button may still display on the toolbar. However, it will not necessarily activate a menu or other action.

### How alarms are reported

Alarms are sent based on two factors: the threshold setting and the polling interval for the device. The threshold setting is based on events per second, with a default setting of 0.5 events per second (or 1.0 events per 2 seconds), and can be adjusted on a per error basis. The polling interval has a default value of 60 seconds and may be adjusted on a per device basis.

For example, using the default values:

0.5 events per second \* 60 seconds = 30 events per minute

This is the default threshold level. If more than 30 events for a particular error type are generated in a minute of polling time, an alarm will be sent. The Alarm Monitor will report the per second level of event generation for the polling period. Therefore, longer polling periods will not necessarily report a higher error level.

## Setting the Threshold Level

Setting threshold levels involves two steps:

- Monitoring the current network to determine mean error levels
- Setting a threshold level based on the mean error levels

**To Set the threshold level:**

## Fault Detection










---

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Fault > Threshold Manager**. From the logical view, right-click on the Fault icon and select Threshold Manager.

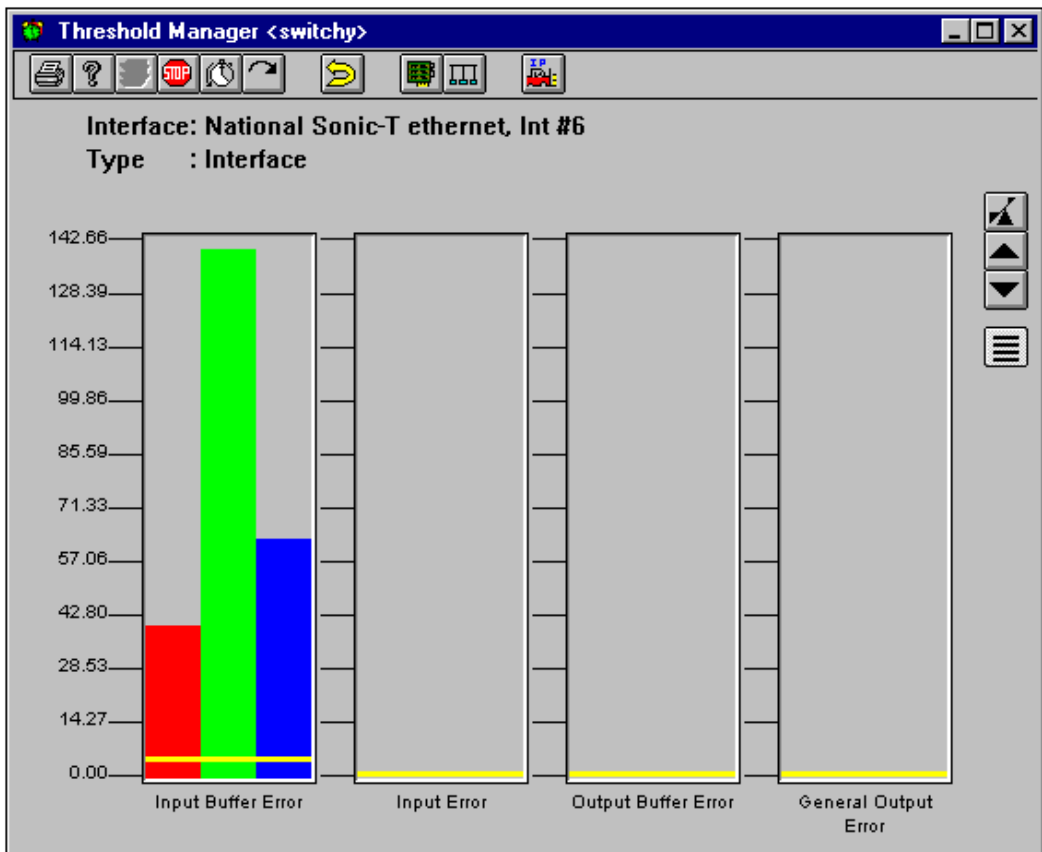
3. Choose the applet parameters and click OK

The Threshold Manager screen is initially blank and will not display information until an error class is selected.

4. Select an error class from the toolbar by clicking on one of the following buttons (they are device-specific and will vary with each device).

Click		To
	AppleTalk errors Icon	View the AppleTalk error gauges.
	IPX/SPX errors Icon	View the IPX/SPX error gauges. <b>Note-</b> 3Com Devices do not support IPX/SPX errors.
	IP errors Icon	View the IP error gauges.
	System/Interface errors Icon	View the System error gauges. When this button is pressed a pop-up menu will be displayed listing all of the available interfaces on the device. This allows for the selection of a specific interface to set threshold levels on.
	Show Token Ring Icon	View the Token Ring error gauges.
	Show Ethernet Icon	View the Ethernet error gauges.
	Show FDDI Icon	View the FDDI error gauges.
	Show Frame Relay	View the Frame Relay error gauges
	Show Bridge Icon	View the Bridge error gauges.

5. The Threshold Manager will begin to display error information in a series of gauges containing a 3-column graph. Information will be updated based on the polling interval.



Each type of error is displayed in a separate gauge. The error type is displayed at the bottom of the gauge, and can also be seen in a pop-up window by holding the mouse pointer in the gauge window. See "Threshold Manager Error Types" on page 333 for details on error types.

The bar values of the graph are:

- **Green:** Indicates the highest value the variable reached while being monitored.

## Fault Detection

---

- **Blue:** Indicates the average value of the variable during the course of monitoring.
- **Red:** Indicates the current value of the variable.

Hold the mouse pointer on a colored bar to see the exact value.

The yellow line drawn across the gauge is the **Alarm threshold marker**. By default it is set at 0.5 events per second.

6. Determine the threshold level. You should monitor the Threshold Manager for at least an hour during an average traffic period, prior to setting any threshold levels.

The ideal alarm threshold is the midpoint between the highest level of errors recorded and the average. For example, if the highest level of errors during the monitoring period is 10, and the average is 5, then the initial threshold should be set at 7.5.

7. After determining the threshold level, reset the threshold marker. To do so, click and hold the left mouse button on the threshold marker (yellow line) and move it to the threshold level desired. When the mouse button is released at the desired new level, a message will be displayed asking for confirmation.






Click on the [OK] button to set the alarm threshold to the indicated value. Or, click on the [Cancel] button to abort.

8. For NavisAccess to begin monitoring the threshold levels, you must do one of the following:
  - a. Open the Alarm Monitor for the device or group to report real-time threshold errors.
  - b. Setup and run a schedule to gather threshold data in the background. Data will be reported to the Event Viewer and the Event Report.

### Other buttons

In addition to the global toolbar buttons on its left side, the Threshold Manager has three specialized button functions:

Button	Description
	<b>[Reset] button</b> Resets the Highest and Average values for every displayed threshold gauge to zero, allowing you to restart calculations for a new monitoring period.
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## Creating a Threshold Manager schedule

Creating a schedule for threshold monitoring is an effective, hands-free means of monitoring your network. The major advantages of setting up a schedule are:

- **Consolidate multiple devices.** You can include as many devices as you wish in a schedule. By doing so, you only need to open one corresponding Alarm Monitor to view real-time data for the entire group.
- **Historical database.** All data gathered by the schedule will be sent to the Event Report, providing a historical record of errors.
- **Time-specific monitoring.** The schedule will gather data only for the date and time span you select. This allows you to monitor specific time periods.
- **Hands-free operation.** The schedule runs automatically whenever NavisAccess is running.

### To create a Threshold Manager schedule:

1. Make sure threshold levels are set for all devices to be included in the schedule. See "Setting the Threshold Level" on page 327 for details.

## Fault Detection

---

2. Open the Schedule Wizard by choosing **Config > Schedule** from the menu bar.
3. Select the time for the schedule to run by clicking in the Schedule Wizard calendar and dragging the mouse to highlight the desired time period.
4. Right-click in the highlighted area and choose **New Schedule**.
5. Select "Background Alarm Monitor" in the Choose Application window.
6. Click Application Parameters to set how often each device in the schedule should be polled. The default value is 15 minutes. Click Next when done.
7. In the Select Schedule Elements window you may either choose from a group that has already been defined, select a single device, or select a number of devices that will form a new group. Selecting more than one device individually will automatically create a group in the Group Wizard, with the default name "Group for Schedule: <user-defined schedule name>". Click Next when done.

This window uses standard Windows [Shift] and [Ctrl] key functions for multiple selections.

8. Enter a name for the Schedule. The name should help identify the schedule, such as "Alarm Monitor for NY Group."
9. Click [Next] and then [Finish]. Your schedule is now set. By default, it will begin to run as soon as the time period begins. If the time period has already started, the schedule will begin in a few moments. The schedule will run automatically at the preset time, whenever NavisAccess is running. See the Schedule Wizard for details on deactivating, stopping or editing the schedule.

To monitor the alarms in real-time, select **Fault > Incident Monitor** from the menu bar, select the group used for the schedule, and click [Alarm Monitor]. This will open a group-specific Alarm Monitor that will show all alarms for the devices in the group. You can also view alarms through the Event Viewer, but alarms for this schedule will be mixed in with many other messages.

For historical data, open the Event Report.

## Threshold Manager error types

The Threshold Manager sets error thresholds based on protocols and interfaces. The error type is indicated at the bottom of each error gauge. Displayed error types depend on the protocol/interface button selected on the Threshold Manager screen.

### AppleTalk errors

#### **Broadcast No Access To Destination**

An AppleTalk packet was discarded because this entity was not its final destination.

#### **Checksum Error**

An AppleTalk packet was discarded because it contained a checksum error.

#### **Failed Encapsulation**

An AppleTalk packet was discarded due to encapsulation failure.

#### **Header Error**

An AppleTalk packet was received with an invalid header.

#### **Hopcount Exceeded**

An AppleTalk packet was received which exceeded the maximum hop count.

#### **No Access to Destination**

An AppleTalk packet was discarded because this entity was not the final destination.

#### **No Router to Destination**

An AppleTalk packet was discarded because the destination network was unknown.

#### **Not Gateway**

An AppleTalk packet was discarded because the router was not the gateway to the destination network.

#### **Packet Discarded**

An AppleTalk packet was discarded by the router for some reason.

#### **Received Data length too long**

An AppleTalk packet was discarded because the received data length was too long.

#### **Received Data length too short**

## Fault Detection

---

An AppleTalk packet was discarded because the received data length was too short.

### **Unknown Protocol**

An AppleTalk packet was discarded due to an unknown or unsupported protocol.

## IP errors

### **Address Error**

An IP packet was received with an invalid IP address.

### **Fragmentation Error**

An IP packet could not be fragmented and was discarded.

### **Header Error**

An IP packet was received with an invalid header.

### **Input Discard Error**

An IP packet was discarded to free up buffer space.

### **No Route To Destination**

An IP packet was discarded because there was no route to its destination.

### **Output Discard Error**

An IP packet could not be sent due to lack of buffer space.

### **Reassembly Error**

An IP packet which was fragmented could not be reassembled (e.g. timeout).

### **Unknown Protocol Error**

An IP packet was received for an unknown or unsupported protocol.

## IPX errors

### **Address Error**

An IPX packet was received with an invalid destination field.

### **Checksum Error**

An IPX packet was discarded due to a checksum error.

### **Failed Encapsulation**

An IPX packet was discarded due to a bad level 2 encapsulation.

### **Header Error**

An IPX packet was received with an invalid header.

### **Hopcount Exceeded**

An IPX packet was discarded because the maximum hop count was exceeded.

### **Input Discard Error**

An IPX input packet was discarded to free up buffer space.

### **No Route To Destination**

An IPX packet was discarded due to unknown destination network.

### **Output Discard Error**

An IPX output packet was discarded to free up buffer space.

### **Socket Not Open**

An IPX packet was discarded because the destination was not open.

### **Unknown Protocol**

An IPX packet was discarded because it had an unknown or unsupported protocol field.

## **System/Interface errors**

### **Interface General Output Error**

Interface general output error.

### **Interface Input Buffer Error**

A packet was discarded to free up buffer space.

### **Interface Input Error**

A packet was received which could not be passed to a higher level protocol.

### **Interface Unknown Protocol**

Interface unknown protocol error.

### **Interface Output Buffer Error**

A packet was discarded to free up buffer space.

For Cisco devices, also see Cisco Specific errors on page 339.

## **TokenRing errors**

### **Abort Transmit**

The interface issued an abort delimiter while transmitting.

### **AC Error**

## Fault Detection

---

A station on the ring cannot set the AC bits properly.

### **Burst Error**

Interface detected an absence of transition for five half-bit timers.

### **Frame Copy Error**

A frame was detected that was addressed to the station that had the FS or A bits set (caused by line error or duplicate address).

### **Frequency Error**

The incoming signal exceeded expected signal loss.

### **Hard Error**

The interface detected an immediately fatal error (such as beacons).

### **Internal Error**

The interface experienced an internal error.

### **Line Error**

A token or frame was repeated with a non-data bit between the SD and ED, or with a FCS error.

### **Lobe Wire**

The interface detected an open, or short, circuit in the data lobe path. The adapter will be closed.

### **Lost Frame Error**

The TRR timer expired before a station received the trailer.

### **Receive Congestion**

A frame was detected that was addressed to the station, but no buffer space was available.

### **Recovery**

A Claim token was received or transmitted after a Ring Purge frame, while in recovery mode.

### **Remove**

The interface received a Remove Ring frame. The adapter will be closed.

### **Single Station**

The interface sensed that it is the only station on the ring.

### **Signal Loss**

The interface detected a loss of signal from the ring.

### **Soft Error**

A soft error was detected on the interface.

### **Token Error**

The active monitor recognized an error condition that required a new token to be generated.

### **Transmit Beacon**

The interface transmitted a beacon frame.

## **Ethernet Errors**

### **Alignment Error**

Received an Ethernet frame that did not contain an integral number of octets.

### **Carrier Sense Error**

Carrier Sense was lost or not asserted when transmitting an Ethernet frame.

### **Excessive Collisions**

Transmitted an Ethernet frame that failed due to excessive collisions (Excessive collisions is subjective).

### **Excessive Deferrals**

An Ethernet frame was deferred for transmission for an excessive period of time (Excessive is subjective).

### **FCS Error**

Received an Ethernet frame that failed the Frame Check Sequence.

### **Frame Too Long**

An Ethernet frame was received that exceeded the maximum frame size.

### **In Range Length Error**

An Ethernet frame was received with a length field between minimum unpadded and maximum LLC size and does not match the number of LLC data octets.

### **Internal MAC Receive Error**

A Receive failed due to an internal interface error.

### **Internal MAC Transmit Error**

A Transmit failed due to an internal interface error.

### **Late Collisions**

Transmitted an Ethernet frame that failed due to a late collision (collision occurring after 51.2 microseconds).

## Fault Detection

---

### **Multiple Collisions**

Transmitted an Ethernet frame that failed due to multiple collisions.

### **Single Collision**

Transmitted an Ethernet frame that failed due to one collision.

### **Out Of Range Length Field**

An Ethernet frame was received with a length field larger than the maximum allowed LLC data size.

### **SQE Test Error**

The interface failed an SQE Test.

## **FDDI errors**

### **General Error**

The FDDI interface detected an error with a frame.

### **Last Frame**

The FDDI interface detected a lost data frame.

## **Source Route Bridging errors**

### **SRB Duplicate Segment Discard**

A duplicate explorer frame was discarded.

### **SRB Duplication Error**

A duplicate LAN ID or Tree was detected.

### **SRB Hop Count Exceeded Discard**

An explorer frame was discarded because the RIF exceeded the maximum router descriptor length.

### **SRB Port Mismatch**

An ARE or STD was discarded because the last LAN ID in the routing information field didn't match the LAN-in ID.

### **SRB Segment Mismatch Discard**

An explorer frame was discarded because the routing descriptor field contained an invalid adjacent segment value.

## **Spanning Tree Protocol errors**

### **STP Delay Exceeds**

A frame was discarded due to excessive transmit delay though the bridge.

**STP MTU Exceeds**

A frame was discarded due to excessive size.

**CISCO specific errors**

**Carrier Signal Transition**

Interface received Carrier Detect Signal.

**Input Abort**

Packet(s) were aborted due to clocking problems.

**Input Overrun**

The serial hardware buffer was overrun.

**Input Queue Drop**

An input packet was dropped because the interface input queue overflowed.

**Output Collision**

An output collision was detected.

**Output Queue Drop**

An input packet was dropped because the interface output queue overflowed.

**Frame Relay errors**

**Forward Congestion**

Forward congestion was indicated on the network.

**Backward Congestion**

Backward congestion was indicated on the network.

## **Setting interface utilization levels**

### **The Interface Utilization Thresholds applet**

The **Interface Utilization Thresholds** applet is used to set utilization alarm levels on a per-interface basis. The default threshold levels are 40% for Ethernet/Token Ring, and 60% for Serial Interfaces. If utilization rises higher than these percentages, an alarm will be sent to the Event Viewer. The Event Viewer application must be running to view alarms in real-time.

All alarm information will also be logged to a historical database and can be viewed at any time using the Event Report applet.

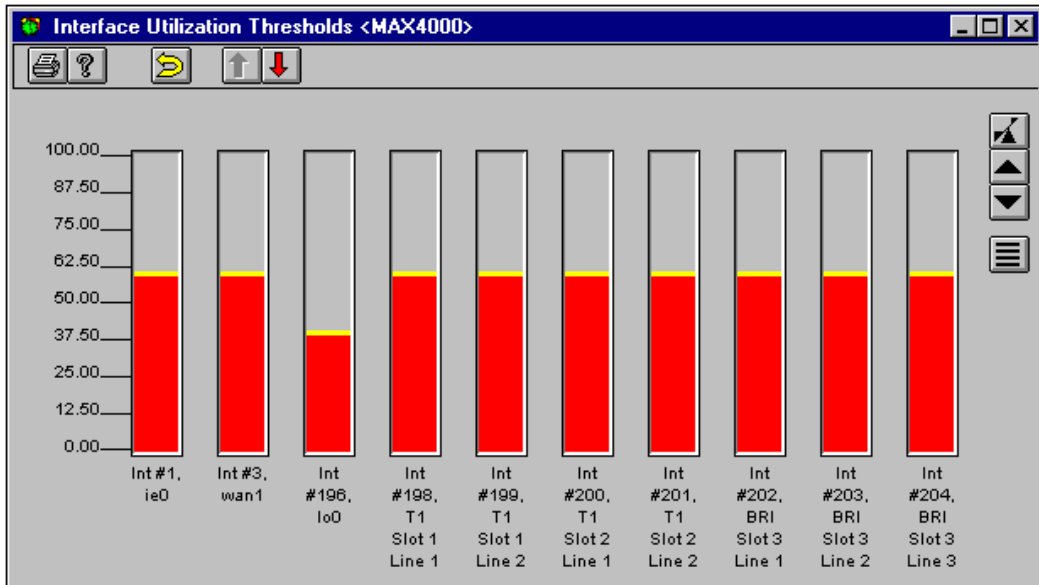
The Interface Utilization applet works in conjunction with the Schedule Wizard. You must create an Interface Utilization schedule in order for data to be delivered to the Event Viewer and Event Report.

For capacity planning needs and long-term utilization trends, specific utilization reports can be generated using the Device DB program.

### **Setting Interface Utilization Thresholds**

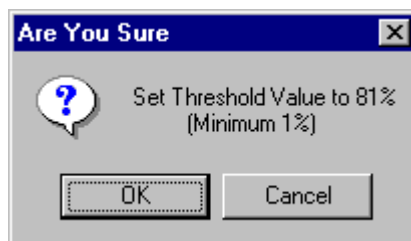
**To set the Interface Utilization threshold settings:**

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose Fault > Utilization Thresholds. From the logical view, right-click on the Fault icon and select Utilization Thresholds.



3. The utilization threshold levels are displayed in columns/gauges for each interface. Hold the mouse still on the column to read the threshold value.






Change the threshold levels by clicking and holding the yellow line, and dragging it up or down. The minimum value setting is 1%. The following sample confirmation message will display:



**NOTE:** For the system to send messages to the Event Viewer and Event Report, you must configure an Interface Utilization schedule for the selected devices and/or interfaces.

### Other buttons:

In addition to the global toolbar buttons on its left side, the Interface Utilization Thresholds applet has five specialized button functions:

Click	To
	<b>[Reset Thresholds to Default] button</b> To reset all thresholds to the default (40% for Ethernet/Token Ring, and 60% for Serial Interfaces).
	<b>[Previous Interface Page] button</b> Available only if the Interface Utilization Threshold Applet has multiple pages - goes to previous page.
	<b>[Next Interface Page] button</b> Available only if the Interface Utilization Threshold Applet has multiple pages - goes to next page
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## Creating an Interface Utilization Thresholds schedule

Creating a schedule for interface utilization monitoring is an effective, hands-free means of monitoring your network. The major advantages of setting up a schedule are:

- **Consolidate multiple devices.** You can include as many devices as you wish in a schedule.
- **Historical database.** All data gathered by the schedule will be sent to the Event Report, providing a historical record of errors.
- **Historical reporting:** Gathered data can be used to generate historical utilization reports.

- **Time-specific monitoring.** The schedule will gather data only for the date and time span you select. This allows you to monitor specific time periods.
- **Hands-free operation.** The schedule runs automatically whenever NavisAccess is running.

### To create an Interface Utilization Thresholds schedule:

1. Make sure interface utilization levels are set for all devices and/or interfaces to be included in the schedule. See "Setting Interface Utilization Thresholds" for details.
2. Open the Schedule Wizard by choosing **Config > Schedule** from the menu bar.
3. Select the time for the schedule to run by clicking in the Schedule Wizard calendar and dragging the mouse to highlight the desired time period.
4. Right-click in the highlighted area and choose **New Schedule**.
5. Select "Background Interface Util" in the Choose Application window.
6. Click Application Parameters to set how often each device in the schedule should be polled. The default value is 15 minutes. Click [Next] when done.
7. In the Select Schedule Elements window you may either choose from a group that has already been defined, select a single device, or select a number of devices that will form a new group. Selecting more than one device individually will automatically create a group in the Group Wizard, with the default name "Group for Schedule: <user-defined schedule name>".

You may also choose specific interfaces on a device. To do so, expand the device icon tree and select the specific devices that appear in the window.

This window uses standard Windows [Shift] and [Ctrl] key functions for multiple selections.

Click [Next] when done.

8. Click [Next]. The Select Logging Options dialog box displays.
9. Set the logging options:

#### **Set Number of Days**

Specify the number of days, from the current day, for which you want the

## Fault Detection

database to hold data. When the number of days is exceeded, the oldest data will begin to automatically be purged on a daily basis. For example, if you use the default 90 days, on the 91st day the data captured 90 days before (which is the day you created the schedule) will be purged.

### Do not purge Data

Select if you do not want the data to automatically be purged.

Click [Next] to continue.

10. The Select Automatic Reports dialog displays.

☒ Report Automation

1. All reports associated with the selected schedule are listed below. Reports can be run automatically at a pre-selected time, specified in the Time to Run Report field. To choose a frequency, highlight one or more reports, select Weekly and/or Daily, and click Apply.

Report(s)

Name	Weekly	Daily
Network Capacity Leaders	No	Yes
Daily Network Capacity	No	Yes
Hourly Network Capacity	No	Yes
Interface Utilization With Pro	No	Yes
Interface Utilization Versus T	No	Yes

2. Time to run report  
01:00

3. Frequency  
☐ Weekly ☒ Daily

< Back   Next >   Cancel

By default, the Schedule Wizard will automatically run reports. De-select the Report Automation check box if you do not want the reports to run automatically.

### Reports

Lists the report(s) available. Available reports are:

- **Network Capacity Leaders:** Plots the ten interfaces with the highest average capacity used for a selected time and date range.
- **Daily Network Capacity:** Generates a bar graph that plots the percentage of utilized network capacity over a number of days. A representative utilization number is generated by averaging the utilization from the different interfaces on the included devices over the complete set of days selected.
- **Hourly Network Capacity:** Generates a mountain graph that plots the percentage of utilized network capacity over a number of hours. A representative utilization number is generated by averaging the utilization from the different interfaces on the included devices over the complete set of hours selected.
- **Interface Utilization with Protocols:** Generates a line graph that plots the interface utilization and the individual protocol utilization for the specified hours of a day.
- **Interface Utilization Versus Time:** Generates a line graph that plots the interface utilization for the specified hours of a day.

### Time to run report

You can change the time the report will run using the "Time to run report" spin box. Reports run by default at 1:00 a.m., to avoid processor overhead during peak hours. The spin box uses a 24-hour clock (for example, 3:00 p.m. would be 15:00).

### Frequency

You can choose to run a given report daily and/or weekly. To change the settings, highlight the report(s), click the Weekly and/or Daily check box, and click [Apply].

Weekly reports run on Sunday, at the time selected in the Time to run report field.

When a report is run, the Schedule Wizard will print the report to your default printer. To view reports on screen, or to run additional reports, use the Device DB program.

Click [Next] to continue.

11. Enter a name for the Schedule. The name should help identify the schedule, such as "Interface Utilization for NY Group."
12. Click [Next] and then [Finish]. Your schedule is now set. By default, it will begin to run as soon as the time period begins. If the time period has already started, the schedule will begin in a few moments. The schedule will run automatically at the preset time, whenever NavisAccess is running. See "Using the Schedule Wizard" on page 224 for details on deactivating, stopping or editing the schedule.

To monitor the alarms in real-time, select **View > Events** from the menu bar. This will open the Event Viewer applet which will report when an utilization level of an interface surpasses the threshold.

For historical data, open the Event Report.

## Setting interface up/down status levels

### The Interface Status Thresholds applet

The **Interface Status Thresholds** applet sets the length of time that an interface may be Up and/or Down before an alert is sent. For example, you may configure the same interface to send an alert if it is down for more than 1 minute, and again if it is up for more than 1 week (useful for long-term network analysis). You can adjust the settings on a per-interface basis, allowing you to prioritize your interfaces, giving more critical ones very short down windows, and less critical ones longer time frames.

When an interface status up/down time period elapses, a message is sent to the Alert applet in real-time. Data is also sent to the Event Report for historical logging.

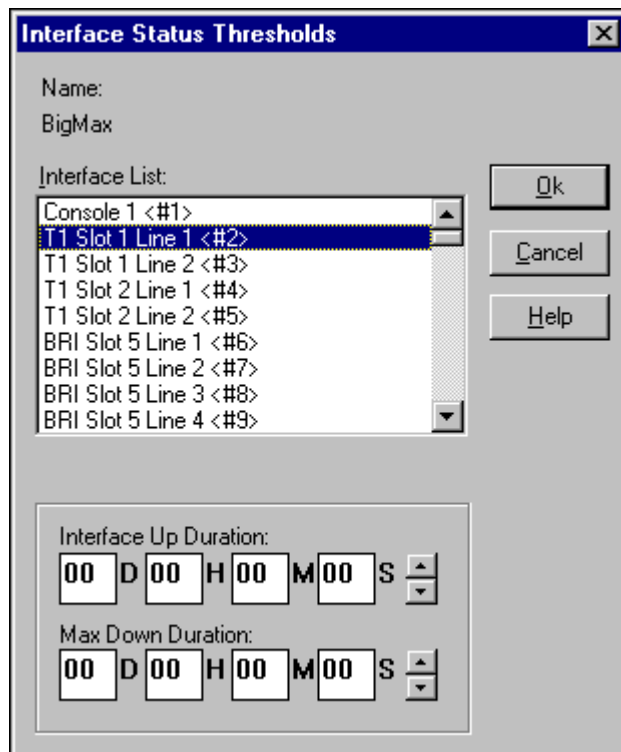
The Interface Status applet works in conjunction with the Schedule Wizard. You *must* create an Interface Status monitoring schedule in order for data to be delivered to the Alert and Event Report tools.

**NOTE:** By default, there are no status thresholds set on any devices. Interface status thresholds must be set before any alarms are generated, and a schedule must be created. If you do not set thresholds and schedules, a downed interface will not generate an alert.

## Setting the Interface Status Thresholds

To set the threshold:

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose Fault > Interface Status. From the logical view, right-click on the Fault icon and select Interface Status.



3. Select interfaces for which you want to set the threshold (use the [CTRL] key to select more than one).
4. Enter the Interface Up Duration and Max Down Duration times. Settings are for Days (D), Hours (H), Minutes (M), and Seconds (S).

For example, if you set the Interface Up Duration to 1 day, a notice will be sent for every day that passes and the interface remains up. If you set Max Down Duration to 5 minutes, an alert will be sent when the interface has

been down for more than 5 minutes.

5. Click [OK] to register your settings and close the Interface Status Thresholds dialog box.

**NOTE:** For the system to send messages to Alert, you must configure an Interface Status Monitoring schedule for the selected devices and/or interfaces.

### Creating an Interface Status Thresholds schedule

Creating a schedule for interface status monitoring is an effective, hands-free means of monitoring your network. The major advantages of setting up a schedule are:

- **Consolidate multiple devices.** You can include as many devices as you wish in a schedule.
- **Historical database.** All data gathered by the schedule will be sent to the Event Report, providing a historical record of errors.
- **Time-specific monitoring.** The schedule will gather data only for the date and time span you select. This allows you to monitor specific time periods.
- **Hands-free operation.** The schedule runs automatically whenever NavisAccess is running.

#### To create an Interface Status Thresholds schedule:

1. Make sure interface threshold up/down periods are set for all devices and/or interfaces to be included in the schedule. See "Setting the Interface Status Thresholds" 347 for details.
2. Open the Schedule Wizard by choosing **Config > Schedule** from the menu bar.
3. Select the time for the schedule to run by clicking in the Schedule Wizard calendar and dragging the mouse to highlight the desired time period.
4. Right-click in the highlighted area and choose **New Schedule**.
5. Select "Interface Status Monitor" in the Choose Application window.
6. Click Application Parameters to set how often each device in the schedule should be polled. The default value is 15 minutes. Click [Next] when

done.

7. In the Select Schedule Elements window you may either choose from a group that has already been defined, select a single device, or select a number of devices that will form a new group. Selecting more than one device individually will automatically create a group in the Group Wizard, with the default name "Group for Schedule: <user-defined schedule name>".

You may also choose specific interfaces on a device. To do so, expand the device icon tree and select the specific devices that appear in the window.

This window uses standard Windows [Shift] and [Ctrl] key functions for multiple selections.

Click [Next] when done.

8. Enter a name for the Schedule. The name should help identify the schedule, such as "Interface Status for NY Group."
9. Click [Next] and then [Finish]. Your schedule is now set. By default, it will begin to run as soon as the time period begins. If the time period has already started, the schedule will begin in a few moments. The schedule will run automatically at the preset time, whenever NavisAccess is running. See the Schedule Wizard for details on deactivating, stopping or editing the schedule.

To monitor the alarms in real-time, select **Fault > Alert** from the menu bar. This will open the Alert applet which will report any interface up or down messages. You can also view alarms through the Event Viewer, but alerts for this schedule will be mixed in with many other messages.

For historical data, open the Event Report.

# **Monitoring for device errors**

## **Alarm Monitor: Overview**

### **What is the Alarm Monitor?**

The Alarm Monitor reports and organizes network errors based on user-configurable threshold levels which are set in the Threshold Manager applet. Errors are categorized by severity (critical, minor, etc.) and family (IP, IPX, Frame Relay, etc.) and reported in real-time.

Alarms can be generated for many reasons, such as a packet being received without a header or with an invalid address, or a data frame exceeding the maximum frame size. Alarm thresholds can be set for each type of error within each protocol or interface family. See "Threshold Manager Error Types" on page 333 for details about error types.

Devices can be monitored individually or in groups, and a separate Alarm Monitor can be opened for each device or device group.

Alarm data sent to the Alarm Monitor is also sent to the Event Report, which maintains a historical database.

**NOTE:** The Alarm Monitor must be open and running for alarms to be reported.

### **Setting Alarm levels**

It is essential to correctly set the threshold levels for the Alarm Monitor. See "Setting the Threshold Level" on page 327 for details.

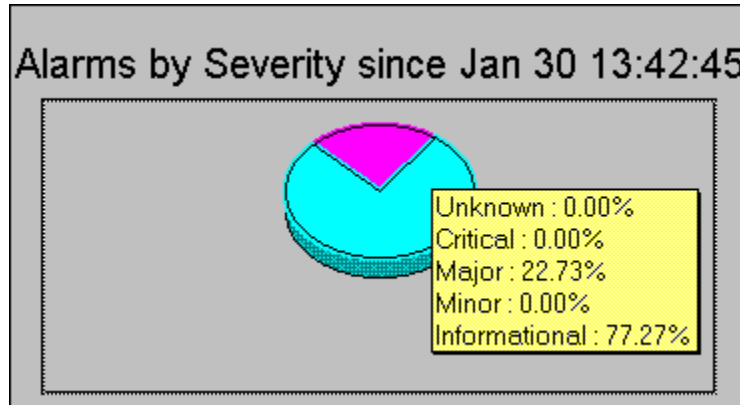
An alarm goes off (is reported) only when the number of errors per second crosses the threshold level. By default, all alarms that are received are reported in the Alarm Monitor.

### **Alarm Levels and Categories**

Alarms are classified and displayed in two categories:

- Alarms by Severity
- Alarms by Family

The pie chart in the upper left of the Alarm Monitor window displays the alarms based on severity.



To view the statistics for the pie chart, press the left mouse button on the pie chart to display the yellow informational box.

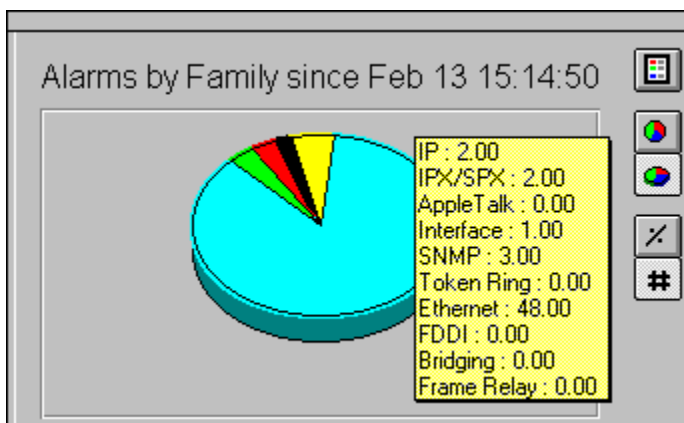
The alarm severity category definitions are:

Level of Severity	Description
<b>Critical - Red</b>	Primary component failure
<b>Major - Magenta</b>	Logical component failure
<b>Minor - Yellow</b>	Logical component error condition
<b>Informational - Cyan</b>	Normal event occurred
<b>Unknown - White</b>	Unknown event

The pie chart in the upper right of the Alarm Monitor window displays the alarms based on family.

## Fault Detection

---



The alarm family categories are varied and dependent on type of device, software installed, protocols enabled, etc. By default, Alarm Monitor reports alarms of all types. To report specific types only, configure the Alarm tab settings, found under **Configure > System Options**.

Some Families types might include, IP, IPX/SPX, AppleTalk, Interface, SNMP, Token Ring, Ethernet, FDDI, Bridging and Frame Relay.

### Alarm Monitor fields

The bottom pane of the Alarm Monitor gives detailed information about each alarm received.

The following information is displayed in the Alarm Monitor:

Heading	Description
Alarm Time	The date and time the alarm was generated.
Device Name	The name of the device that generated the error.
Alarm Type	A short description of the type of alarm generated. Alarm types are normalized within SNMP variable groups. This simplifies the task of identifying problems. For a description of alarm types, see Threshold Manager Error Types.

Heading	Description
<b>Interface</b>	The connection to the network (only available for interface alarms).
<b>Per/Sec</b>	The number of alarms per second between this and the last polling interval.
<b>Thresh</b>	The currently configured threshold for the alarm.
<b>Alarm Summary</b>	Describes the error in more detail than the Alarm Type field described above.
<b>Severity</b>	The classification of the alarm (e.g. critical, informational, etc.).
<b>Family</b>	The family of the alarm (e.g. IP, AppleTalk etc.).
<b>State</b>	The current state of the device after this error (e.g. Operational, Nonoperational).
<b>Device Type</b>	The type (make) of device which generated the error.
<b>Address</b>	The IP Address of the device which generated the error.

## Starting the Alarm Monitor

### To start the Alarm Monitor:

1. Start the Alarm Monitor using one of the following:

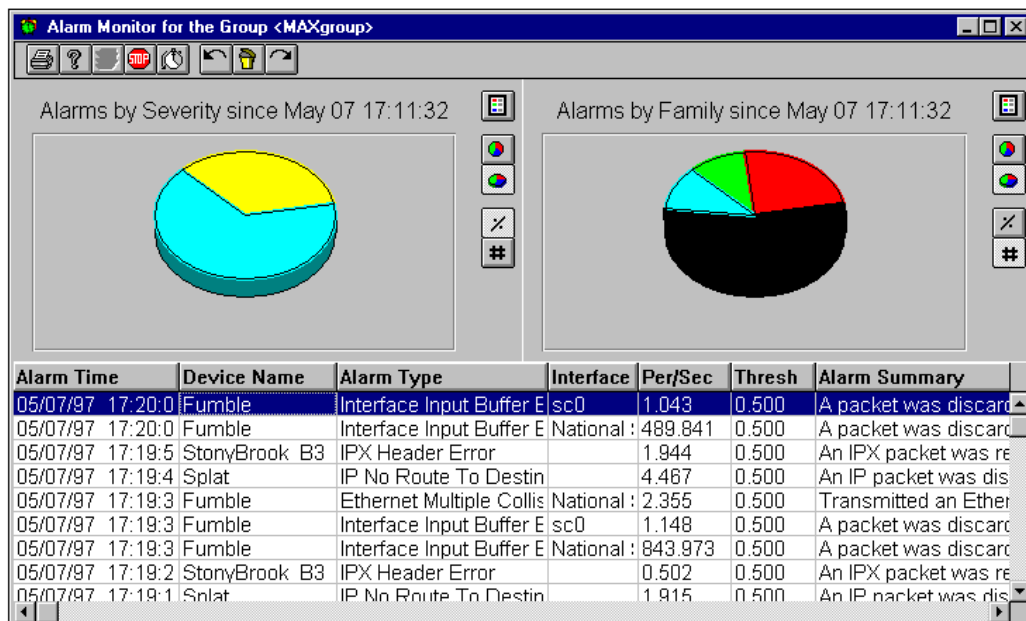
#### For single devices:

- a. Right-click on a device icon and select Boxmap.
- b. From the physical view, right-click on a blank area in the window and choose Fault > Alarm Monitor. From the logical view, right-click on the Fault icon and select Alarm Monitor.

For device groups:

- a. Open the Incident Monitor by selecting Fault > Incident Monitor from the menu bar. Select a device or device group and click the [Alarm Monitor] button.

## Fault Detection










Alarms will be reported based on the polling interval.

To monitor alarms, simply minimize the Alarm Monitor. The device(s) will continually be polled at the specified interval, until the Alarm Monitor Applet is closed.

Automatic scheduling for Alarm data collection is available via the Scheduler.

**Other buttons:**

In addition to the global toolbar buttons on its left side, the Alarm Monitor applet has six specialized button functions:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.
	<b>[Clear Data] button</b> Clears data from the screen. Does not affect data being sent to the Event Report database.
	<b>[Rescan Configuration] button</b> Updates the Alarm Monitor to reflect changes made in the system configuration. For example, you can configure the system to report only IP alarms. If you then reconfigure to report both IP and IPX, the Alarm Monitor will not begin reporting IPX alarms until the [Rescan] button is pressed. Alternately, you can close and restart the Alarm Monitor, but this would lose any data currently on the screen.
	<b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coding in the pie charts. For example: 
	<b>[Show/Hide 3D Effect] buttons</b> Toggles the pie chart between a 2D and 3D image.
	<b>[Show Values/Show Percent] buttons</b> Toggle the pie charts between displaying information as an integer value (e.g., 10 alarms sent) or as a percentage (e.g. 10% of all alarms sent). Click on the pie chart to see the precise values.

## Monitoring interface up/down status

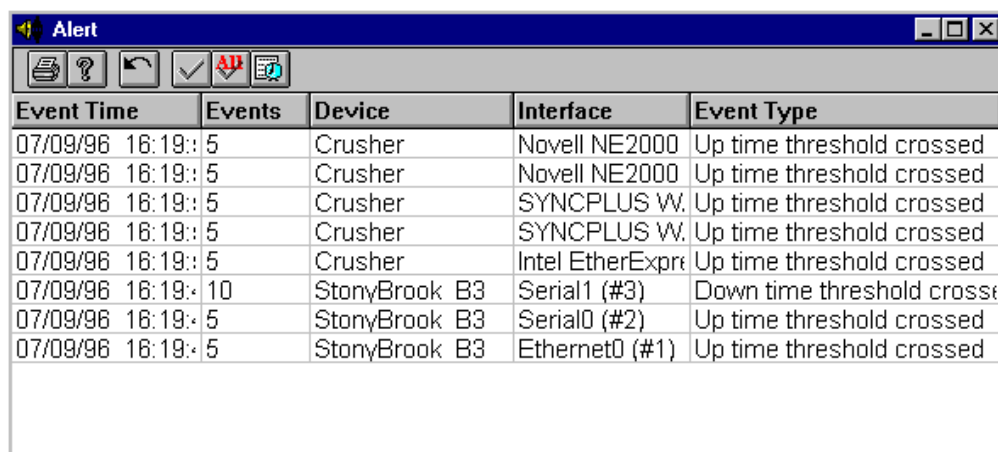
### Alert overview

#### Menu Bar: Fault > Alert

The Alert applet reports real-time up/down interface status. This is a critical application for knowing when a device interface has stopped operating.

Alert works in conjunction with the Interface Status Thresholds applet (used to set the up/down threshold time periods) and the Schedule Wizard (creates a schedule to monitor interfaces).

**NOTE:** Alert *will not report information* on an interface until the interface threshold has been set and the interface has been included in a schedule which is running.



Event Time	Events	Device	Interface	Event Type
07/09/96 16:19: 5		Crusher	Novell NE2000	Up time threshold crossed
07/09/96 16:19: 5		Crusher	Novell NE2000	Up time threshold crossed
07/09/96 16:19: 5		Crusher	SYNCPUS W.	Up time threshold crossed
07/09/96 16:19: 5		Crusher	SYNCPUS W.	Up time threshold crossed
07/09/96 16:19: 5		Crusher	Intel EtherExpre	Up time threshold crossed
07/09/96 16:19: 10		StonyBrook B3	Serial1 (#3)	Down time threshold crossi
07/09/96 16:19: 5		StonyBrook B3	Serial0 (#2)	Up time threshold crossed
07/09/96 16:19: 5		StonyBrook B3	Ethernet0 (#1)	Up time threshold crossed

The following information is displayed in the Alert window:

Heading	Description
Event Time	The date and time the event was generated.
Events	The number of events identical to the one listed.
Device	The name of the device which generated the event.

Heading	Description
Interface	The connection to the network.
Event Type	A description of the event, indicating if an up or a down time threshold was passed.

## Using the Alert applet




The following steps are needed to generate data in Alert.

1. Set Interface Status Thresholds for the device or devices you wish to monitor.
2. Create a schedule to monitor the devices you selected in step 1. For details, see Creating an Interface Status Thresholds schedule on page 348.
3. When you have set threshold levels and created a scheduled, open the Alert window from the main menu bar by selecting **Fault > Alert**, or right-click on a device icon in the Internet Map and select **IntraNet/WAN Services > Fault > Alert**. Alerts will only be reported if a schedule is running.

Alert information will also be logged to the historical database of the Event Viewer.

### Other buttons:

In addition to the global toolbar buttons on its left side, the Alert applet has three specialized button functions:

Button	Description
	<b>[Clear Event] button</b> Clears an individual event from Alert.
	<b>[Clear All Events] button</b> Clears all events from Alert.
	<b>[Event Report button]</b> Displays the Event Report for the device.

## **Comprehensive system events**

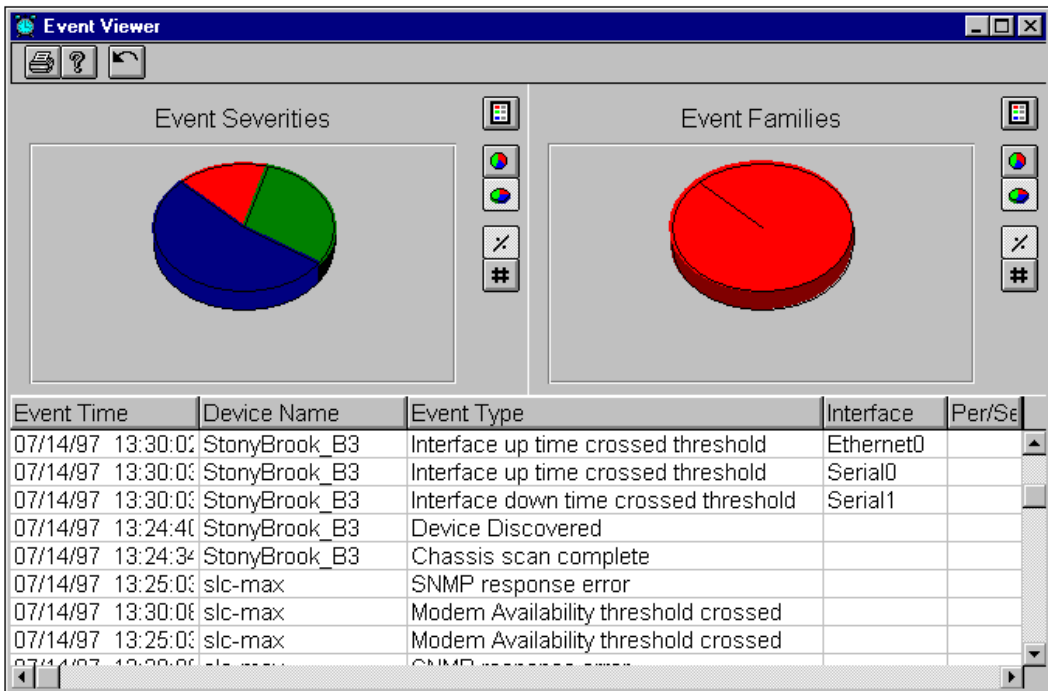
### **The Event Viewer: Overview**

#### **Menu Bar: View > Event**

The Event Viewer is the central viewing point for a multitude of real-time network data, including:

- Error information sent from the Threshold Manager applet.
- Up/down interface status information sent from the Interface Status Thresholds applet.
- Interface utilization information sent from the Interface Utilization Thresholds applet.
- Automatic configuration downloading/uploading information.
- Network Traps.
- Errors reported by the Access Watch application.

**NOTE:** The information sent to the Event Viewer depends on the configuration of the applets mentioned above. Please refer to the individual applets for more details.



### About Traps

The Event Viewer reports traps generated by devices on the network which are configured to send them to the IP address of the workstation running NavisAccess. For information on how to configure your devices to send TRAPS to NavisAccess, please see the appropriate section on *Special Considerations for (your device)*. For information on how to forward these TRAPS and other messages received by the Event Viewer to other IP addresses, please see the "Trap Handler" (page 371).

### Event Levels and Categories

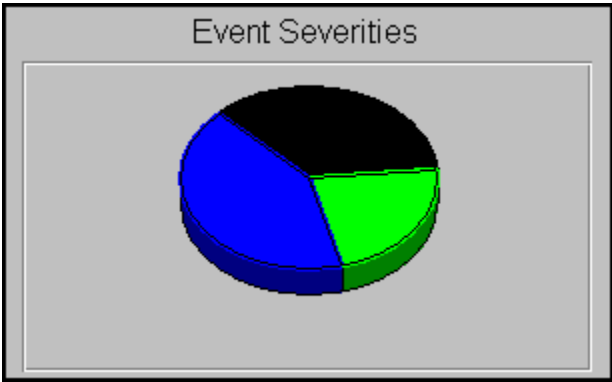
Events are classified and displayed in two categories:

- Events by Severity
- Events by Family

The pie chart in the upper left of the Event Monitor window displays the events based on severity.

**Fault Detection**

---

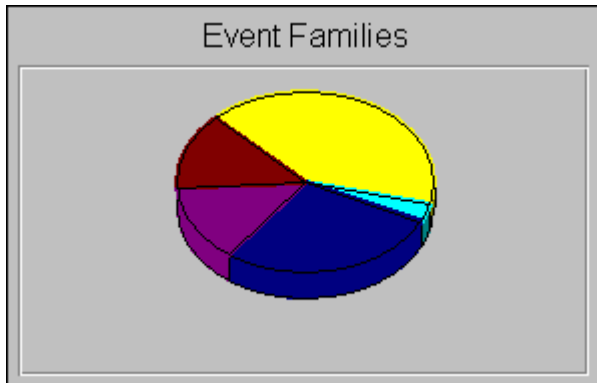


To view the statistics for the pie chart, press the left mouse button on the pie chart to display the yellow informational box.

The event severity category definitions are:

Level of Severity	Description
Critical	Primary component failure
Major	Logical component failure
Minor	Logical component error condition
Informational	Normal event occurred

The pie chart in the upper right of the Event Viewer window displays the events based on family.



The Event Family categories are varied and dependent on the type of device, protocols enabled, and software used. They may include System, FR Virtual Element, Device Discovery, SNMP, IP, Config Downloader, Config Uploader, Clear Alarm, AppleTalk, Interface, IPX/SPX, Token Ring, FDDI, MIB-II, etc.

### Event Viewer fields

The bottom pane of the Event Viewer gives detailed information about each event received.

The following information is displayed in the Event Viewer:

Heading	Description
<b>Event Time</b>	The date and time the event was generated.
<b>Device Name</b>	The name of the device which generated the event.
<b>Event Type</b>	A short description of the type of event generated. Event types are normalized within SNMP variable groups. This simplifies the task of identifying problems. These are available in protocol or interface descriptions.
<b>Interface</b>	The connection to the network (only available for interface alarms).
<b>Per/Sec</b>	The number of events per second between this and the last polling interval.

## Fault Detection

---

Heading	Description
<b>Thresh</b>	The currently configured threshold for the event.
<b>Event Summary</b>	Describes the error in more detail than the Event Type field described above.
<b>Severity</b>	The classification of the severity (e.g. critical, informational etc.).
<b>Family</b>	The family of the alarm (e.g. IP, AppleTalk etc.).
<b>State</b>	The current state of the device after this event (e.g. Operational, Nonoperational).
<b>Device Type</b>	The brand of device which generated the error.
<b>Address</b>	The IP Address of the device which generated the event.






## Using the Event Viewer applet

### To start the Event Viewer:

1. From the main menu bar, select View > Events. The Event Viewer will open and events will be reported in real-time based on system configurations and the other fault monitoring applications that are running.

### Other buttons:

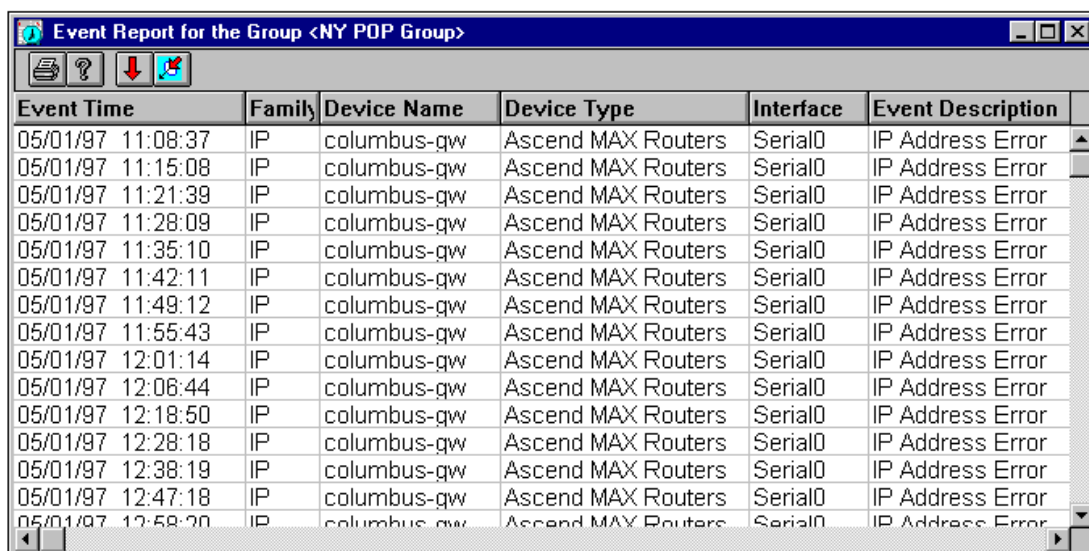
In addition to the global toolbar buttons on its left side, the Event Viewer applet has four specialized button functions:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.
	<b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coding in the pie charts. For example: 
	<b>[Show/Hide 3D Effect] buttons</b> Toggles the pie chart between a 2D and 3D image.
	<b>[Show Values/Show Percent] buttons</b> Toggle the pie charts between displaying information as a integer value (e.g., 10 events reported) or as a percentage (e.g. 10% of all events). Click on the pie chart to see the precise values.

## Historical event data

### Event Report: Overview

The **Event Report** applet gathers data reported by data gathering tools (error threshold alarms, interface utilization, and interface up/down status) and the Access Watch application and retains a historical database. This allows you to access historical fault information for all monitored devices and device groups. The database is maintained from the date NavisAccess was installed. Event Report also provides data filtering options, to locate data based on specific criteria, such as date, device, error type, etc.



Event Time	Family	Device Name	Device Type	Interface	Event Description
05/01/97 11:08:37	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:15:08	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:21:39	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:28:09	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:35:10	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:42:11	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:49:12	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 11:55:43	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:01:14	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:06:44	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:18:50	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:28:18	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:38:19	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:47:18	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error
05/01/97 12:58:20	IP	columbus-gw	Ascend MAX Routers	Serial0	IP Address Error

The following information is displayed in the Event Report:

Heading	Description
Event Time	The date and time the event was generated.
Family	The family (type) of the event (e.g. IP, Device Discovery, SNMP, etc.)

Heading	Description
<b>Device Name</b>	The name of the device which generated the event.
<b>Device Type</b>	The brand of device which generated the event.
<b>Interface</b>	The connection to the network (only available for interface events).
<b>Event Description</b>	A short description of the type of event generated.
<b>Severity</b>	<p>The classification of the event. Classifications are as follows:</p> <p><b>Critical:</b> primary component failure.</p> <p><b>Major:</b> logical component failure</p> <p><b>Minor:</b> logical component error condition</p> <p><b>Notice:</b> normal but significant conditions exist</p> <p><b>Informational:</b> normal event occurred</p>
<b>State</b>	The current state of the device after this event (e.g. Operational, Nonoperational).
<b>Per/Sec</b>	The number of events per second between this and the last polling interval. Applies only to network errors.
<b>Thresh</b>	The currently configured threshold for the alarm. Applies only to network error thresholds.
<b>Address</b>	The IP Address of the Device which generated the event.
<b>Event Summary</b>	Describes the event in more detail than the Event Description

## Using the Event Report

### To start the Event Report:

1. Start the Event Report using one of the following:

#### For single devices:

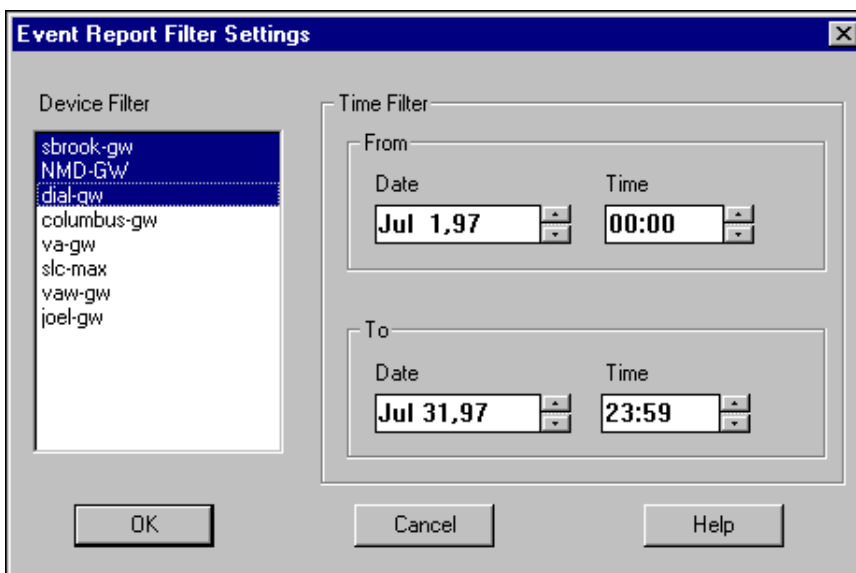
- a. Right-click on a device icon and select Boxmap.
- b. From the physical view, right-click on a blank area in the window and choose Fault > Event Report. From the logical view, right-click on the Fault icon and select Event Report.

#### For device groups:

- a. Open the Incident Monitor by selecting Fault > Incident Monitor from the menu bar. Select a device or device group and click the [Event Report] button.

### Filtering Data

2. The Event Report provides extensive filtering options to help you find the data you need. Click on the [Filter Settings] button to open the Filter window.






3. Select the devices you wish to include in the Event Report, and the From and To date ranges.

Note that the Time filter designates a start and end time for the entire date range, not for within each day of the range. For example, start/end dates of Jan. 1 to Jan. 10 with a time of 06:00 to 16:00 would return events from Jan. 1 at 6 a.m. to Jan. 10 at 8 p.m. (16:00), and *not* for each day between the hours of 6 a.m. and 8 p.m.

### Other buttons:

In addition to the global toolbar buttons on its left side, the Event Report applet has two specialized button functions:

Button	Description
	<b>[Sort Events by Descending Time] button</b> Sorts Event Record entries by descending time order.
	<b>[Sort Events by Ascending Time] button</b> Sorts Event Record entries by ascending time order.
	<b>[Filter ] button</b> Filters data based on user selections. See above for details.

## Miscellaneous fault tools

### Incident Monitor

#### **Menu Bar:** Fault > Incident Monitor

The Incident Monitor provides quick access to the Alarm Monitor and the Event Report for single devices or for device groups.



#### **Using the Incident Monitor**

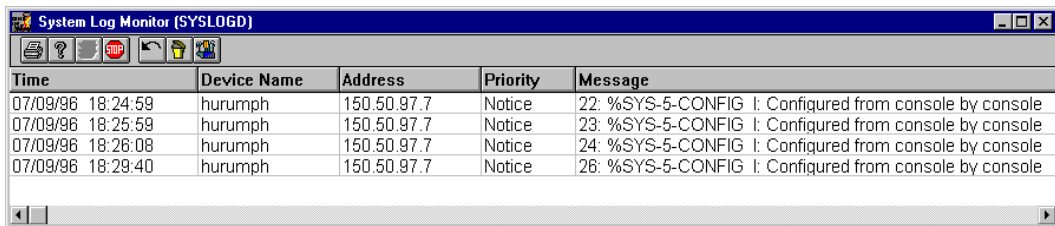
1. Open the Incident Monitor by selecting Fault > Incident Monitor from the main menu bar.
2. Device groups are displayed by default. To view individual devices, click the Devices radio button. Only preconfigured device groups are available. You cannot select multiple single devices.
3. Click the [Alarm Monitor] button to start the Alarm Monitor for the device or device group. Or click the [Event Report] button to access the event report for the device or group.
4. When selecting a group, the [Group...] button is activated. Click the button to access the Device Groups window, which will show you what

devices are in the group and allow you to edit the group to add or delete members. Note that if you redefine a group, the new definition will apply in all instances, not just for the purposes of the Incident Monitor.

## System Log Monitor

Use the System Log Monitor to monitor unsolicited events that occur within your network. This feature is analogous to the UNIX “syslog” function, and uses well-known service port 514.

In order for messages to be sent to the System Log Monitor, logging must be enabled on network devices. The details for doing so are specific to the devices. Please consult your device documentation for information.



Time	Device Name	Address	Priority	Message
07/09/96 18:24:59	hurumph	150.50.97.7	Notice	22: %SYS-5-CONFIG I: Configured from console by console
07/09/96 18:25:59	hurumph	150.50.97.7	Notice	23: %SYS-5-CONFIG I: Configured from console by console
07/09/96 18:26:08	hurumph	150.50.97.7	Notice	24: %SYS-5-CONFIG I: Configured from console by console
07/09/96 18:29:40	hurumph	150.50.97.7	Notice	26: %SYS-5-CONFIG I: Configured from console by console

The following information is reported in the System Log Monitor:

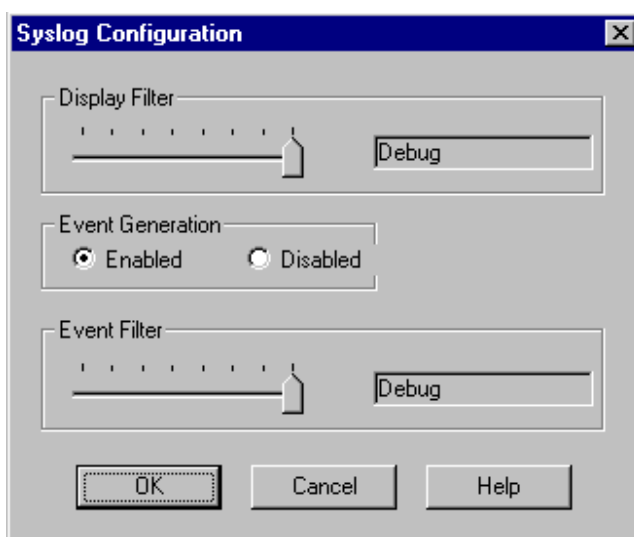
Heading	Description
Time	The date and time the event was generated.
Device Name	The name of the device which generated the event.
Address	The IP Address of the device which generated the event.
Priority	The classification of the event (e.g. critical, informational, etc.).
Event Description	A short description of the type of event generated.

### Using the System Log Monitor

By default, the System Log Monitor is started automatically when NavisAccess is launched, and is located on the NavisAccess desktop in minimized form. However, it is necessary to configure the error reporting levels, and whether or not System Log errors will also be reported to the Event Viewer.

#### To start and configure the System Log Monitor:

1. If it is not already open, start the System Log Monitor by selecting **Tools > System Log Monitor** from the NavisAccess main window toolbar.
2. Click the [Configure] button to open the Syslog Configuration dialog.



3. Specify the level of severity of unsolicited events which you want displayed in the System Log Monitor. The level of severity is determined by the Display Filter sliding scale, with 0 on the left side being the most severe, and 7 on the right side being the least severe.

Scale Number	Severity Level	Description
0	Emergency	System is unusable
1	Alert	Immediate action is required or system will traverse into Emergency state
2	Critical	Primary component failure
3	Error	Abnormal conditions exist
4	Warning	Temporary abnormal conditions exist
5	Notice	Normal but significant conditions exist
6	Informational	Normal event occurred
7	Debug	Configured debugging event

4. If you wish to also have errors logged to the Event Viewer, click the "Enabled" radio button.
5. Set the level of severity of messages you wish to have reported to the Event Viewer. This level need not be the same as the Display Filter level, but it must be equal to or less than the Display Filter level. For example, if you select severity level 5 in Display Filter, you can only select severity levels 0-5 in Event Filter. In this example, you cannot select severity level 6 or 7.

## Trap Handler

All events received by NavisAccess can be forwarded to a maximum of twenty IP addresses. This is accomplished through the use of the Trap Handler. The Trap Handler is configured using the IMC Configuration applet.

### To use the Trap Handler:

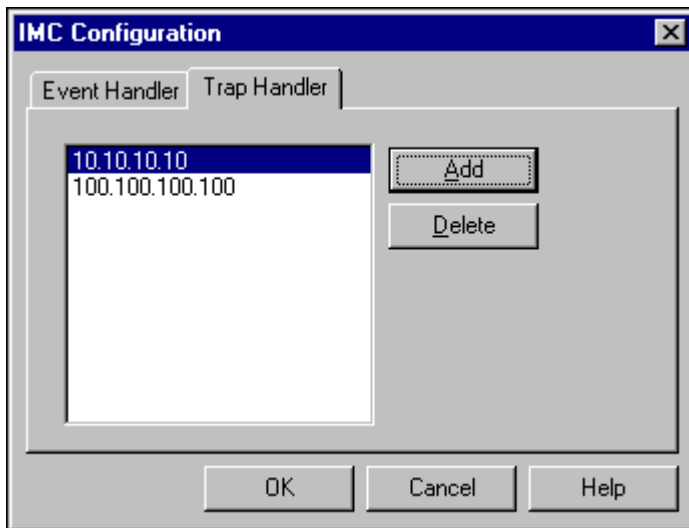
1. Launch the IMC Configuration applet by clicking the IMC Configuration icon in the NavisAccess program group, or from the Windows NT start button select **Programs > NavisAccess > Intermachine Configuration**.

The IMC Configuration applet opens.

## Fault Detection

---

2. Click the Trap Handler tab. This screen is used to enter up to 20 IP addresses to which Traps are to be sent.



3. To enter IP addresses, click the [Add] button, enter an address and click [OK]. The Port setting should not be changed.

## **Ascend Correlation Engine: Overview**

The **Ascend Correlation Engine (ACE)** is used to intelligently process certain types of events, thereby generating more precise and useful event messages.

Using sets of configurable algorithms, ACE monitors devices at the interface level to determine if certain behavior patterns indicate a problem condition or if they are in fact benign. ACE also monitors for new interfaces being added to the network.

There are four configurable algorithms:

- **New Interface Detection**  
Sends notification when new interfaces are added to a device on the network.
- **Interface Status Monitor**  
Monitors up/down status changes on interfaces. If the number of up/down changes surpasses the configured threshold level, an event is generated.
- **Chronic Unstable Interface**  
Monitors interfaces to detect unreliable links, i.e., those that change state frequently.
- **Chronic Link Overload**  
Monitors interfaces to detect those which are chronically overloaded (exceeding a configurable utilization limit).

ACE also allows you to set parameters for multiple devices, and for specific interfaces on individual devices.

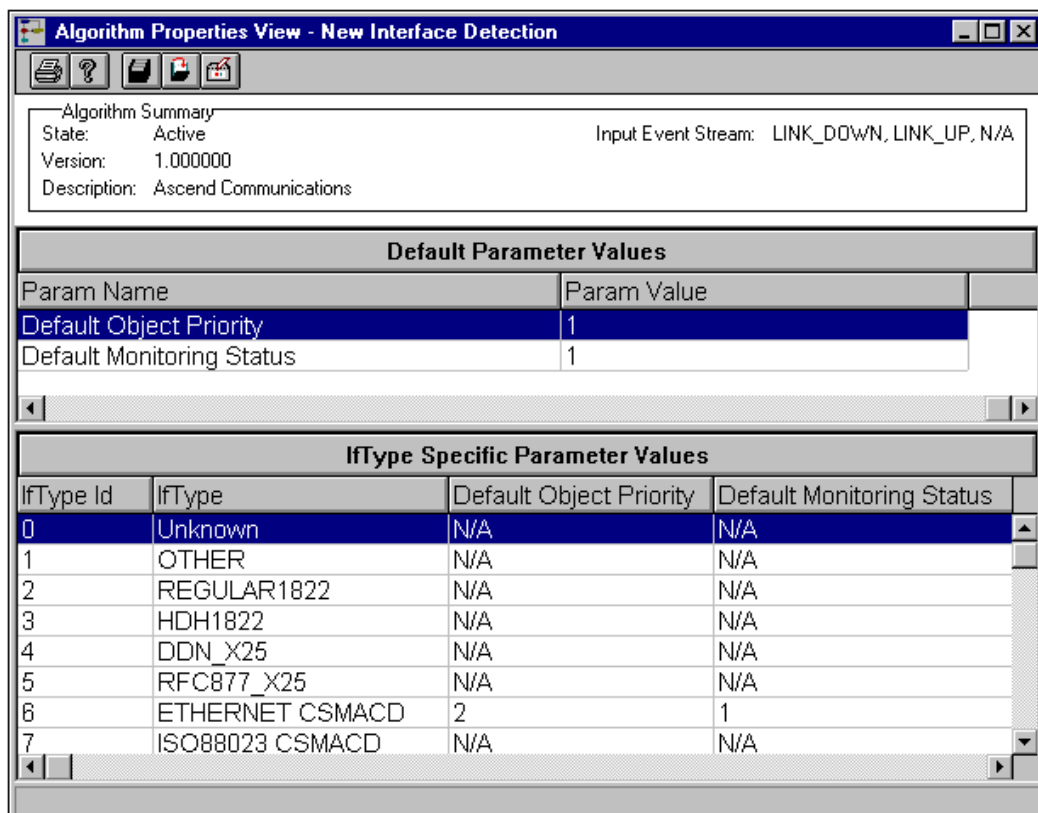
### ACE - New Interface Detection

The ACE **New Interface Detection** algorithm monitors system traps and generates an event when:

- A new device is added to the network
- A new interface is added to an already discovered device

ACE *does not* generate events when devices are discovered using the NavisAccess Explorer function or when they are manually added.

ACE also allows you to modify algorithm parameters on a single device or on a group of devices. See Device Specific Configuration for details.



The top pane of the window indicates if the algorithm is active or not.

The middle pane displays the default parameter values.

Parameter	Description
<b>Default Monitoring Status</b>	Indicates whether or not the network should be monitored for new devices/interfaces. A parameter setting of 1 = yes, a setting of 0 = no.
<b>Default Object Priority</b>	This field is reserved for future functionality. Do not change this setting.

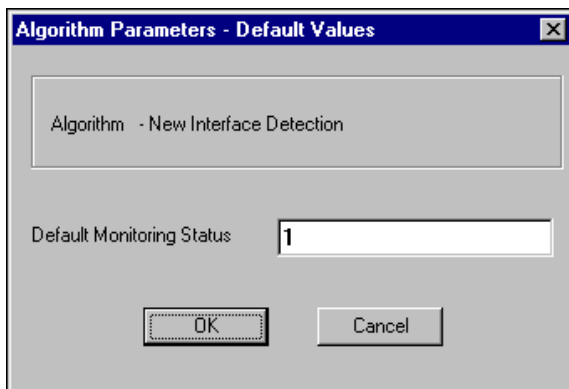
The bottom pane is used to individually configure specific interface types. By default, all interfaces use the values configured in the Default Parameter Values section unless otherwise specified.

Parameter	Description
<b>IfTypeID</b>	The Interface Type ID, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
<b>IfType</b>	The Interface Type, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
<b>Default Monitoring Status</b>	Indicates whether or not the interface type should be monitored for new interfaces. A parameter setting of 1 = yes, a setting of 0 = no.
<b>Default Object Priority</b>	This field is reserved for future functionality. Do not change this setting.

### Configuring Default Values

Default values are used for all interfaces which do not have IfType Specific values set for them (i.e., display a value of N/A).

1. Open the Algorithms View by selecting **File > Algorithms View** from the main menu bar.
2. Double-click the [New Interface Detection] button or right-click and select **Properties**. The Algorithm Properties View window appears (see sample above).
3. To change the Default Monitoring Status, double-click the table cell to open the Algorithms Parameters window.

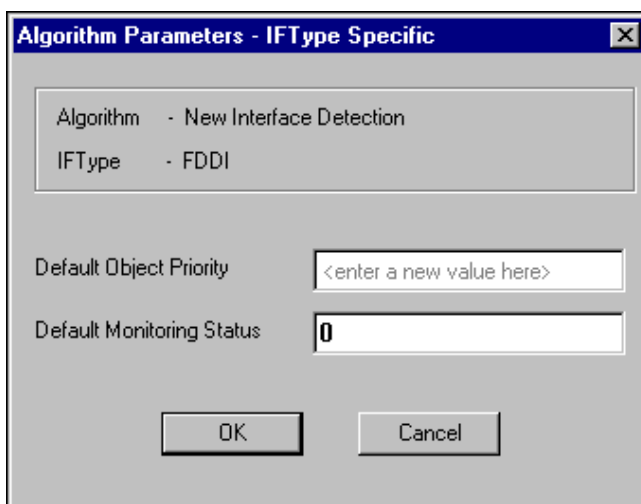


4. Enter 1 to turn interface detection on. Enter 0 to turn interface detection off. Click [OK] when done.
5. Click the [Save Changes] button to store your new settings.

### Configuring IfType Specific Values

You can set monitoring on and off for specific interface types. For example, if you set IfType FDDI to NO, when an FDDI interface is added to the network an event will *not* be generated.

1. Double-click on the table cell corresponding to the IfType you wish to modify. The IfType Specific window appears.



2. In the Default Monitoring Status cell, enter 1 to turn interface detection on. Enter 0 to turn interface detection off. Click [OK] when done.

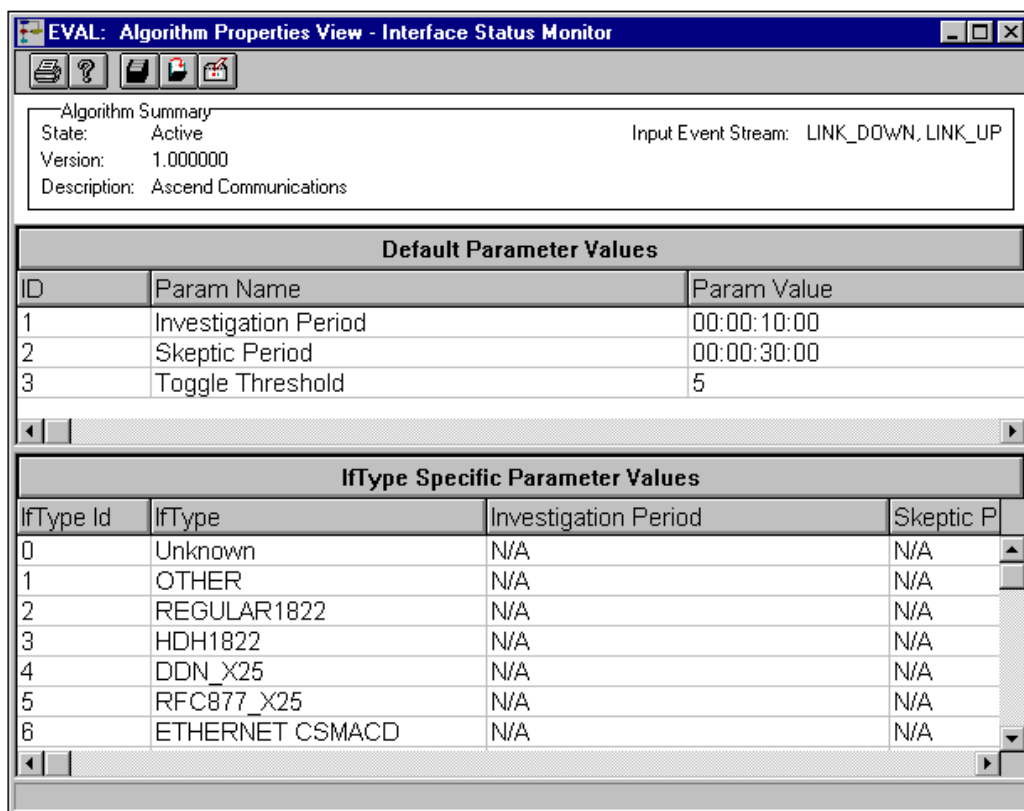
If an interface type is not modified, it will use the default value set in the Default Parameter Values table.

3. After modifying the interfaces you wish to change, click the [Save Changes] button to store your new settings.

### ACE - Interface Status Monitor

The ACE **Interface Status Monitor** monitors up/down status of interfaces over a predefined period of time. Unlike typical interface monitors that report every change in up/down status, ACE only generates an event when a time- and number-based threshold level is surpassed. For example, ACE can be set to generate an event if an interface changes status up or down six times in 20 minutes. If the interface switches less than six times in 20 minutes, no event is generated.

ACE also allows you to modify algorithm parameters on a single device or on a group of devices. See Device Specific Configuration for details.



The top pane of the window indicates if this algorithm is active or not.

The middle pane displays the default parameter values.

Parameter	Description
<b>Investigation Period</b>	The length of time ACE will monitor an interface for up/down status, in D:HH:MM:SS format.
<b>Skeptic Period</b>	An extended monitoring period used only when an event is generated based on the Investigation Period. Once an event is generated, the interface will continue to be monitored for the length of the Skeptic Period in order to more fully determine if the situation is chronic or only a passing problem.
<b>Toggle Threshold</b>	The numbers of times an interface must change status (up/down) within the designated Investigation Period in order to generate an event. Each change of status is counted as 1, e.g. if an interface goes down and then up, that is counted as 2 toggles.

The bottom pane is used to individually configure specific interface types. By default, all interfaces use the values configured in the Default Parameter Values section unless otherwise specified.

Parameter	Description
<b>IfTypeID</b>	The Interface Type ID, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
<b>IfType</b>	The Interface Type, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
<b>Investigation Period</b>	Sets the Investigation Period for the specific Interface Type.
<b>Skeptic Period</b>	Sets the Skeptic Period for the specific Interface Type.

### Configuring Default Values

Default values are used for all interfaces which do not have IfType Specific values set for them (i.e., display a value of N/A).

1. Open the Algorithms View by selecting **File > Algorithms View** from the main menu bar.
2. Double-click the [Interface Status Monitor] button or right-click and select **Properties**. The Algorithm Properties View window appears (see sample above).
3. To change the default Investigation Period, Skeptic Period or Toggle Threshold, double-click the table cell to open the Algorithms Parameters window.
4. Enter new settings and click [OK] when done.
5. Click the [Save Changes] button to store your new settings.

### Configuring IfType Specific Values

You can set parameters values for specific interface types.

1. Double-click on the table cell corresponding to the IfType you wish to modify. The IfType Specific window appears.
2. Enter new values for the Investigation Period, Skeptic Period and/or Toggle Threshold. Click [OK] when done.

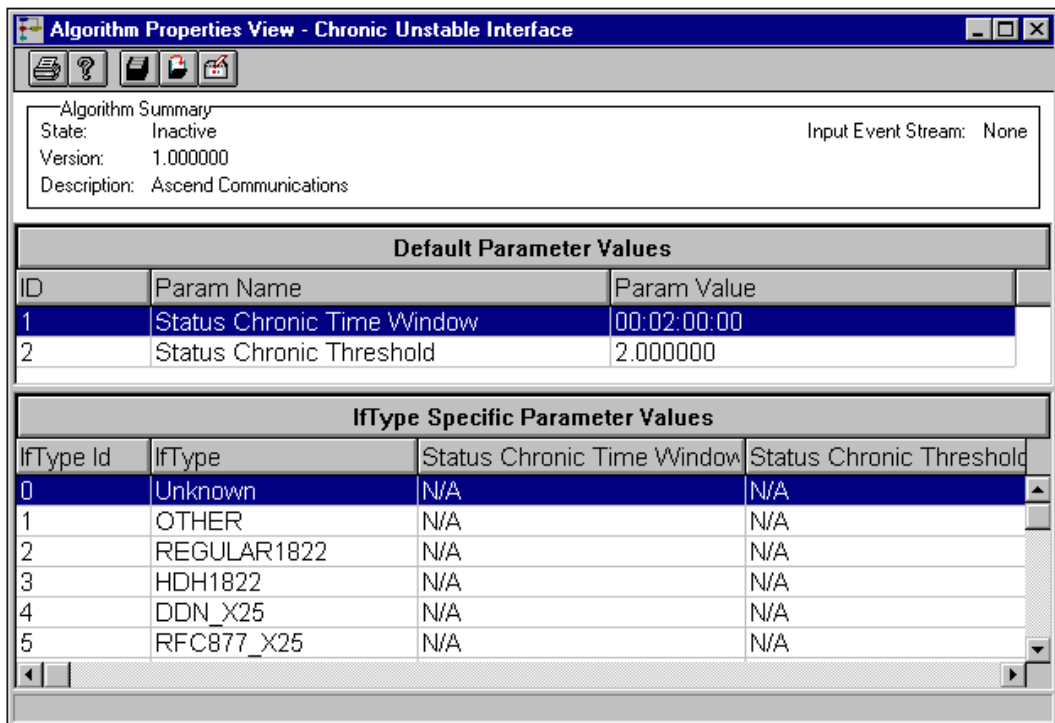
If an interface type is not modified, it will use the default value set in the Default Parameter Values table.

3. After modifying the interfaces you wish to change, click the [Save Changes] button to store your new settings.

## ACE - Chronic Unstable Interface

The ACE **Chronic Unstable Interface** applet monitors interface up/down status over a period of time to locate interfaces which are chronically unstable.

While all interfaces will fluctuate, it is not typically a problem. However, when an interface is chronically unstable and changes state frequently, it can have a serious impact on network performance. ACE is designed to locate these potentially troublesome interfaces.



The top pane of the window indicates if this algorithm is currently active or not.

## Fault Detection

---

The middle pane displays the default parameter values.

Parameter	Description
Status Chronic Time Window	The length of time ACE will monitor an interface for up/down status, in D:HH:MM:SS format.
Status Chronic Threshold	The numbers of times an interface must change status (up/down) within the designated Chronic Time Window in order to generate an event. Each change of status is counted as 1, e.g. if an interface goes down and then up, that is counted as 2 toggles. Possible values range from 1 to 10,000.

The bottom pane is used to individually configure specific interface types. By default, all interfaces use the values configured in the Default Parameter Values section unless otherwise specified.

Parameter	Description
IfTypeID	The Interface Type ID, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
IfType	The Interface Type, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
Status Chronic Time Window	Sets the Chronic Time Window for the specific Interface Type.
Status Chronic Threshold	Sets the Chronic Time Threshold for the specific Interface Type.

### Configuring Default Values

Default values are used for all interfaces which do not have IfType Specific values set for them (i.e., display a value of N/A).

1. Open the Algorithms View by selecting **File > Algorithms View** from the main menu bar.
2. Double-click the [Chronic Unstable Interface] button or right-click and select **Properties**. The Algorithm Properties View window appears (see sample above).
3. To change the default Status Chronic Time Window and/or Status Chronic Threshold, double-click the table cell to open the Algorithms Parameters window.
4. Enter new settings and click [OK] when done.
5. Click the [Save Changes] button to store your new settings.

### Configuring IfType Specific Values

You can set parameters values for specific interface types.

1. Double-click on the table call corresponding to the IfType you wish to modify. The IFTYPE Specific window appears.
2. Enter new values for the Status Chronic Time Window and/or Status Chronic Threshold. Click [OK] when done.

If an interface type is not modified, it will use the default value set in the Default Parameter Values table.

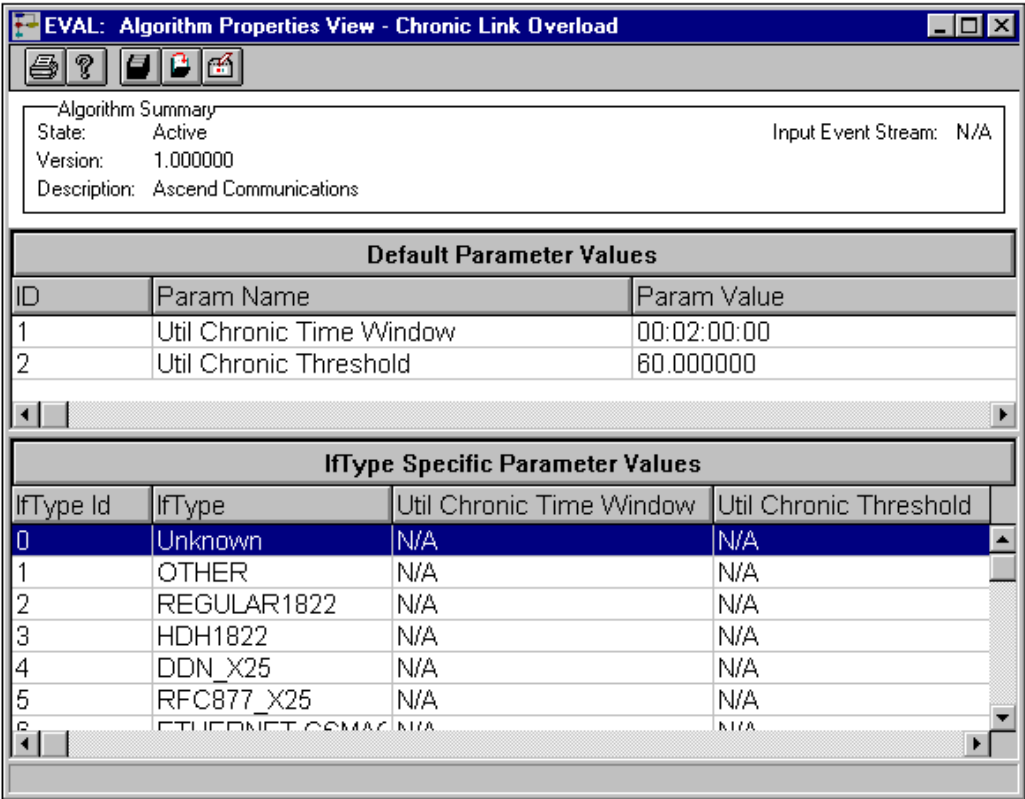
3. After modifying the interfaces you wish to change, click the [Save Changes] button to store your new settings.

ACE - Chronic Link Overload

The ACE **Chronic Link Overload** applet monitors interfaces over a period of time to locate interfaces which are chronically overloaded, i.e. consistently surpass a pre-configured utilization level.

While utilization on all interfaces will fluctuate, it is not typically a problem. However, when an interface is chronically overloaded it can have a serious impact on network performance. ACE is designed to locate these potentially troublesome interfaces.

**NOTE:** This applet works in conjunction with the Background Interface Utilization schedule. You must create and run a schedule for the devices you wish to monitor or else ACE will not receive any data.



The top pane of the window indicates if this algorithm is active or not.

The middle pane displays the default parameter values.

Parameter	Description
<b>Util Chronic Time Window</b>	The length of time ACE will monitor an interface for utilization overload, D:HH:MM:SS format.
<b>Util Chronic Threshold</b>	The accumulated utilization level which must be surpassed in order to generate an event. For example, if the time window is 2 hours and the Chronic Threshold is 60%, an interface must average 60% or greater utilization over the 2 hour time period. Temporary utilization spikes will not generate an event if the average utilization for the monitoring period remains below the threshold limit.

The bottom pane is used to individually configure specific interface types. By default, all interfaces use the values configured in the Default Parameter Values section unless otherwise specified.

Parameter	Description
<b>IfTypeID</b>	The Interface Type ID, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
<b>IfType</b>	The Interface Type, as defined by the Internet Assigned Numbers Authority in the ianaiftype MIB.
<b>Util Chronic Time Window</b>	Sets the Chronic Time Window for the specific Interface Type.
<b>Util Chronic Threshold</b>	Sets the Chronic Utilization Threshold for the specific Interface Type.

### Configuring Default Values

Default values are used for all interfaces which do not have IfType Specific values set for them (i.e., display a value of N/A).

1. Open the Algorithms View by selecting **File > Algorithms View** from the main menu bar.
2. Double-click the [Chronic Link Overload] button or right-click and select **Properties**. The Algorithm Properties View window appears (see sample above).
3. To change the default Util Chronic Time Window and/or Util Chronic Threshold, double-click the table cell to open the Algorithms Parameters window.
4. Enter new settings and click [OK] when done.
5. Click the [Save Changes] button to store your new settings.

### Configuring IfType Specific Values

You can set parameters values for specific interface types.

1. Double-click on the table cell corresponding to the IfType you wish to modify. The IfType Specific window appears.
2. Enter new values for the Util Chronic Time Window and/or Util Chronic Threshold. Click [OK] when done.

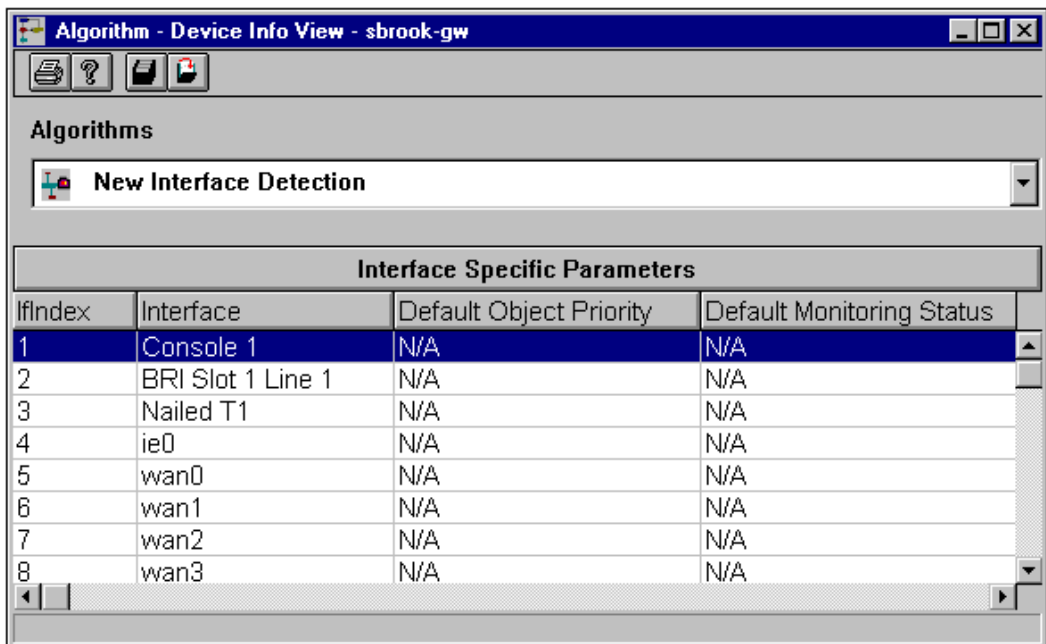
If an interface type is not modified, it will use the default value set in the Default Parameter Values table.

3. After modifying the interfaces you wish to change, click the [Save Changes] button to store your new settings.

## ACE - Device Specific Configuration

ACE allows you to configure parameter values for specific interfaces on a device.

1. From the Boxmap, click the ACE icon to open the Device Info View window.



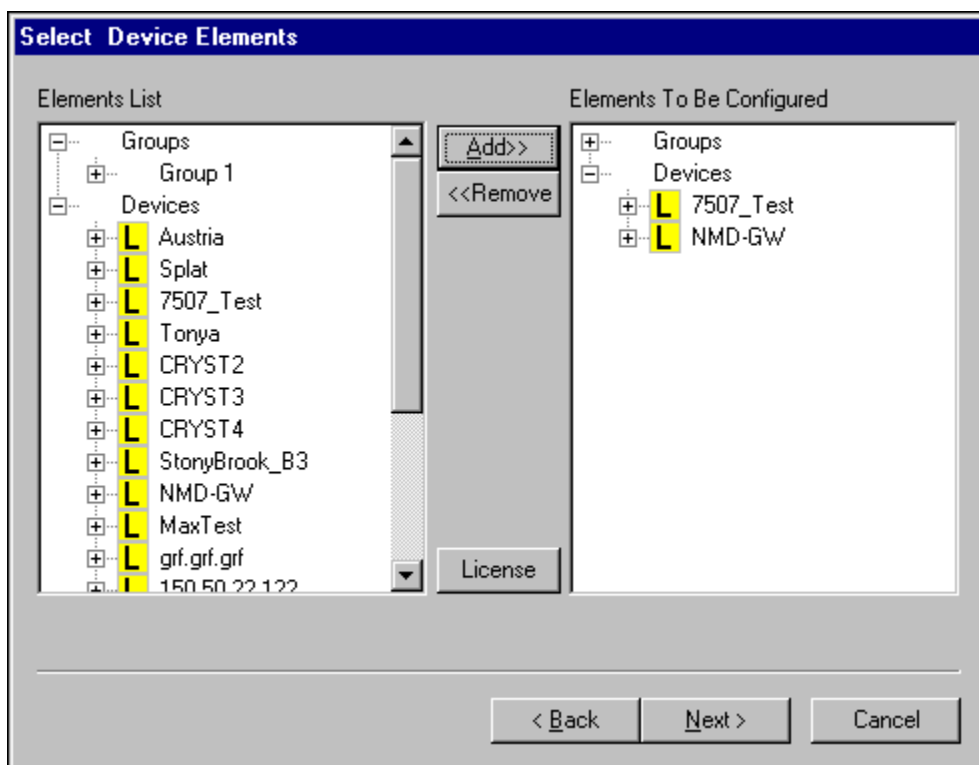
The window displays all interfaces found on the device.

2. From the Algorithms drop-down, select the algorithm you wish to configure. The Interface Specific Parameters window will change based on the selection.
3. To set a specific interface, double-click on the table cell in the Interface Specific Parameters window to open the Device Specific parameters dialog.
4. Enter new values and click [OK] when done.
5. Click the [Save Changes] button to store your new settings.

## ACE - Multiple Device Configuration

ACE allows you to configure default values on multiple devices or groups of devices.

1. From an ACE Algorithm Properties window, click the [Configure Devices for this Algorithm] button to open the Select Device Elements window.



2. Choose devices and/or device groups by highlighting them and clicking the [Add] button to move them to the Elements To Be Configured pane.
3. Click [Next] to open the Enter Parameter Values window.
4. Configure the default values for the selected devices. Click [Finish] when done.

## Menu Bar: File > Pathfinder

PathFinder allows you to determine the route between any two (SNMP) devices.

PathFinder displays the flow pattern for data being transmitted between two devices over a WAN or LAN. The line that traces the path connecting the devices turns a different color to indicate possible trouble spots, allowing you to tell at a glance whether or not thresholds along the path are being exceeded. Other information presented by PathFinder helps you make informed decisions about eliminating bottlenecks for traffic, establishing alternative paths, and locating more efficient paths.

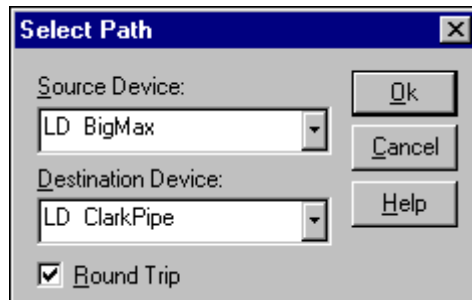
You can start PathFinder from the main window, or from the Internet Map. PathFinder is highly configurable, allowing you to specify threshold warning levels, display names and colors, whether or not to show bandwidth information, and more.

PathFinder's Virtual Element feature allows you to create a virtual element that gives you quick access to a path you check frequently.

## Starting PathFinder from the main window

1. Select PathFinder from the File menu.

The Select Path dialog box displays.



Selections for Source Device and Destination Device can be any device listed. “L” and “D” designations before the device name indicate that the device is Licensed and/or Discovered by the database. All known objects are listed (and automatically licensed) for Source and Destination

## The PathFinder

---

selections. Any device object that appears in red is a device that has *not* been discovered. As SNMP objects are discovered on the path, they will be automatically added to the Source and Destination lists for use with the next PathFinder operation.

2. Select the starting point device in the Source Device combo box.
3. Select the ending point device in the Destination Device combo box.
4. Check the Round Trip check box if you want the PathFinder Tool to display the return path as well as the forward path.

By default, PathFinder displays both the forward path and the return path. If Round Trip is not selected, only the forward path will be displayed. Round Trips are either Asymmetrical (different forward and back) or Symmetrical (the same in both directions).

5. Click [OK].

The PathFinder window will display the path traced between the default network addresses of the two devices you selected.

## Starting PathFinder from the Internet Map window

1. Select a device using your mouse or pointing tool.

Selections for Source Device and Destination Device can be any device (e.g. router, switch, bridge, etc.). You can not select segments for use with PathFinder.

2. Hold the [SHIFT] key or the [CTRL] key and select another device using your mouse or pointing tool.
3. Click the [Launch Pathfinder] button in the Internet Map toolbar.

PathFinder will build the path between the default network addresses of the two devices you selected. To change the default network address of a device, please see Source and Destination Combo Boxes.

When launched from the Internet Map, PathFinder displays the Round Trip, which is both the forward path and the return path. Round Trips are either Asymmetrical (different forward and back) or Symmetrical (the same in both directions).

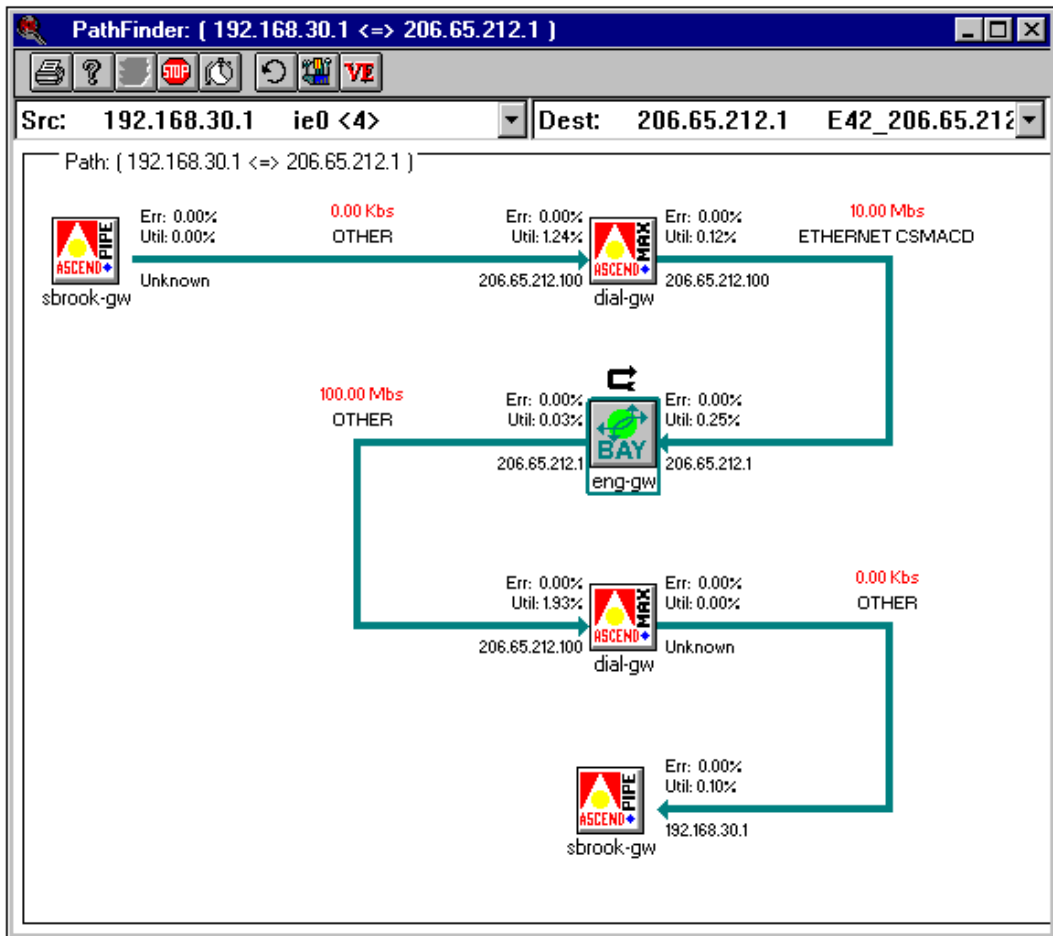
**NOTE:** When PathFinder is launched from the Internet Map, you cannot specify which device is the Source Device and which device is the

Destination Device. Therefore you do not have the option of specifying whether or not you want to display the Round Trip. To specify these parameters, launch PathFinder from the main window.

## Understanding the PathFinder results

After PathFinder is activated, the PathFinder window displays the path traced between the default network addresses of the devices you selected.

Below is an example of the PathFinder window, followed by information to help you understand the valuable information the window displays:



## The PathFinder

---


### Visual indicators



The color of the path line indicates the line status with regard to utilization and error thresholds. The default settings for the color are Green for Healthy, Blue for Warning, and Red for Alarm. Please see "Configuring Pathfinder" for information on setting the threshold percentages and colors.

Color/Object	Description
<b>Green / Path line</b>	Connection between devices is healthy.
<b>Blue / Path line</b>	A warning has been issued due to line utilization or error thresholds being exceeded.
<b>Red / Path line</b>	An alarm has been issued due to line utilization or error thresholds being exceeded.
<b>Red / Line speed number</b>	Output and input speeds of connected objects do not match (a device's interface bandwidth configuration is incorrectly set). You must have the Show IF Bandwidth option selected to see this.
<b>Yellow / Device Icon Background</b>	Enter and exit network addresses of the device are not symmetrical. You must have Detection by Address selected to see this.
<b>Red / Device Icon Background</b>	Path trace has terminated. Either a hop is down, or the object has not been discovered. Please see Termination of the Path below for more information.

### Other buttons

In addition to global toolbar buttons , there are three specialized buttons on the PathFinder toolbar:

Button	Description
	<b>[Rescan Path] button</b> Rescans the path. For use after changing the network address.

Button	Description
	<b>[Config PathFinder] button</b> Displays the PathFinder Configuration dialog box which allows you to configure PathFinder.
	<b>[Create Virtual Element] button</b> Creates a Virtual Element. Please see "Creating a PathFinder Virtual Element" for more information.

### Changing network addresses

The Source and Destination combo boxes list the network addresses for each interface of the Source and Destination devices, respectively. This allows you to scan the path for any interface on the devices.

When the PathFinder window first appears, the boxes display the default network address for each device (the addresses used during the initial scan. To scan the same devices using different network addresses, use the combo box arrows to select the interface you want to scan, then click the [Rescan Path] button.

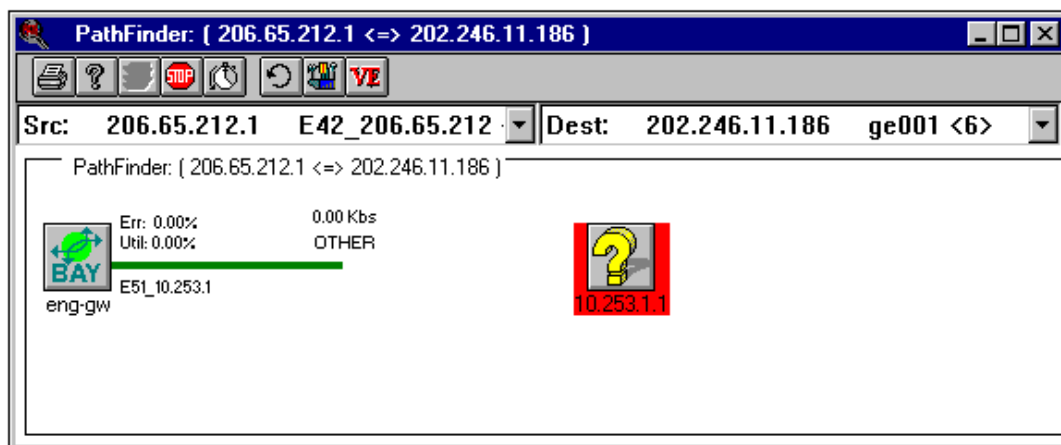
To change the default network address, right-click the device and select **Device Information**. If a Source or Destination combo box is empty when the PathFinder window first appears, the default network address has not been discovered.

### Termination of the Path

In general, if any hop is down, the path terminates, and the ending icon appears on a red background. However, if the beginning SNMP object has been configured for an alternate route, the second (alternative) path displays.

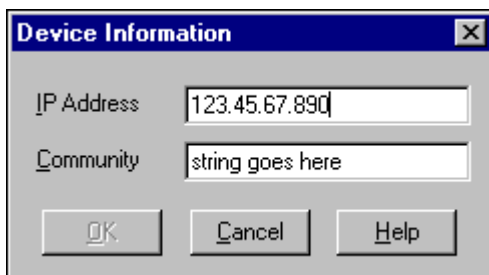
If a device cannot get discovered and is on the path, the path terminates and the object appears on a red background, as shown in the example below:

## The PathFinder



The discovery did not proceed in the above illustration because the Read Only Community string was incorrect. To correct this:

1. Right-click the selected object and choose **Device Information**.
2. Enter the read-only community string in the **Community** field.



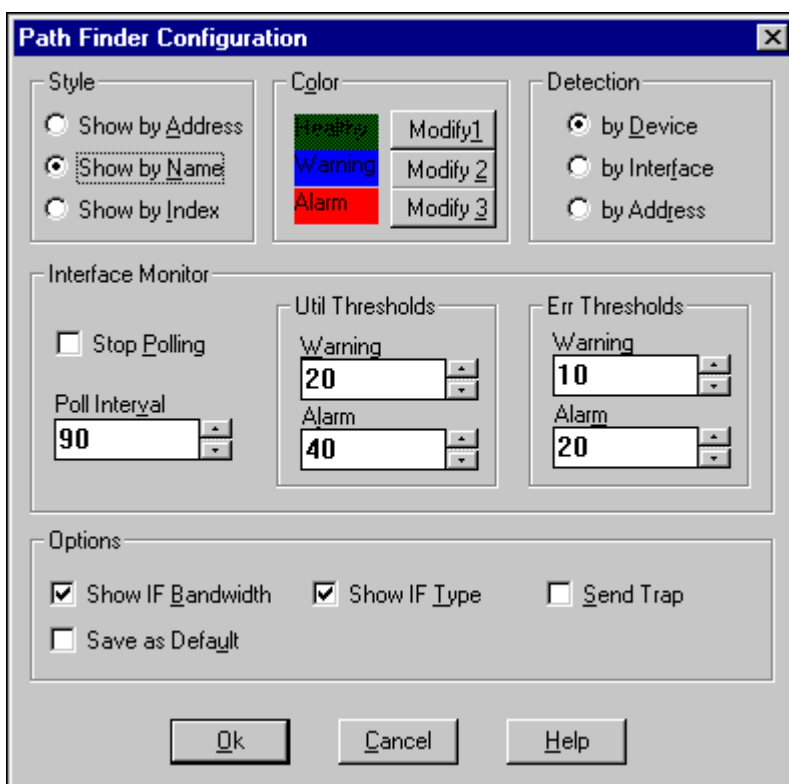
3. Click [OK].

The discovery and path will then continue to evolve.

## Configuring PathFinder

### To configure PathFinder:

1. Click the [Config PathFinder] button to open the PathFinder Configuration dialog box.



2. Select a Style option.

#### Show by Address

The device interface will be identified by network address (i.e., IP number).

#### Show by Name

The device interface will be identified by name (e.g. Ethernet0).

### **Show by Index**

The device interface will be identified by interface index (in most cases this is the interface number).

#### **3. Select Color options.**

The color of the path line indicates the status of the line with regard to utilization and error thresholds. The default settings for the status colors are:

**Green** for Healthy

**Blue** for Warning

**Red** for Alarm.

Click the [Modify] button to the right of each state to modify the color associated with that state. This displays the color palate for customization of the color for the selected state. All colors are available from the color palate.

#### **4. Select a Detection option.**

The Detection choice determines which method will be used to detect devices on the path. The selected method is used when determining whether or not a Round Trip is Symmetrical or Asymmetrical. These choices are hierarchical, with By Device being the most general method of detection and By Address being the most specific.

##### **By Device**

The return trip is checked to see whether or not it is made via the same devices that were used for the forward trip. A return trip via a different device causes asymmetry.

##### **By Interface**

The return trip is checked to see whether or not it is made via the same interfaces that were used for the forward trip. A return trip via a different interface causes asymmetry.

##### **By Address**

The return trip is checked to see whether or not it is made via the same IP addresses that were used for the forward trip. A return trip via a different address causes asymmetry.

The first device that causes asymmetry is marked by placing its icon on a yellow background.

5. Choose Interface Monitor options.

**Stop Polling**

Stops the currently displayed path from being automatically refreshed. This presents a static view of the path.

**Poll Interval**

Sets the amount of time between each redetermination of the path.

**Utilization Threshold**

Set the Warning and Alarm levels to indicate the percentage of maximum utilization the connecting line must exceed to issue a warning or alarm and trigger a change in the color of the traced path. For example, setting Warning at 20 and Alarm at 40 would generate a warning if utilization surpasses 20 percent, and an alarm if it surpasses 40 percent.

**Error Threshold**

Set the Warning and Alarm levels to indicate the percentage of allowable errors the connecting line must exceed to issue a warning or alarm and trigger a change in the color of the traced path. For example, setting Warning at 20 and Alarm at 40 would generate a warning if allowable errors exceed 20 percent, and an alarm if they exceed 40 percent.

6. Choose Interface Options.

**Show IF Bandwidth**

Select to display the bandwidth of the line connecting two objects. Bandwidth is displayed above the path line.

Line speed must match at both ends to observe correct line utilization statistics. Therefore, if you have the *Show IF Bandwidth* option selected, any connecting line between two objects where the output speed of one does not match the input speed of the other will have its line speed number appear in red. This serves as an alert as to when a device's interface bandwidth configuration is incorrectly set.

**Show IF Type**

Select to display the type of interface connection between two objects. Type is displayed above the path line.

**Send Trap**

Select to trap the Utilization or Error Thresholds being exceeded and display the events in the Event Viewer.

## The PathFinder

---

### Save as Default

Select to have your Path Finder settings apply each time you use the Path Finder tool.

7. Click [OK] for settings to take effect.

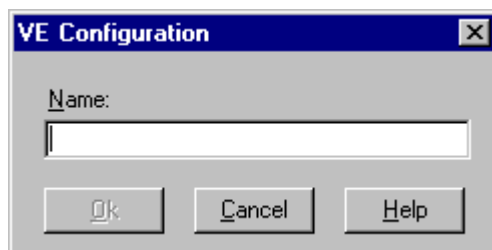
## Creating a PathFinder Virtual Element

PathFinder allows you to create a Virtual Element for any path that you need to check frequently. The Virtual Element icon will appear in the Show Device(s) window. Double-clicking on the icon will automatically bring up the PathFinder window and rescan the path, without your having to re-select the devices.

### To create a PathFinder Virtual Element:

1. Create a path using the steps shows in Starting PathFinder from the Main Window.
2. Click the PathFinder [Create Virtual Element] button.

The VE Configuration dialog box displays:



3. Specify the name you want to use to identify the virtual element.

A PathFinder Virtual Element icon is added to your Show Device(s) screen, with the name you specified. For example:



Austria to Tonya

### Using the PathFinder Virtual Element icon

The PathFinder Virtual Element icon you create for any two devices appears in the Show Device(s) screen. You can use the virtual element to:

- Trace the path between the two devices
- Configure, or rename, the virtual element

To trace the path between the two devices, either double-click the icon or right-click the icon and select **Path Finder**.

To configure, or rename, the virtual element, right-click the icon and select **Configuration**.

## **The PathFinder**

---

# Network Performance: Monitoring Tools

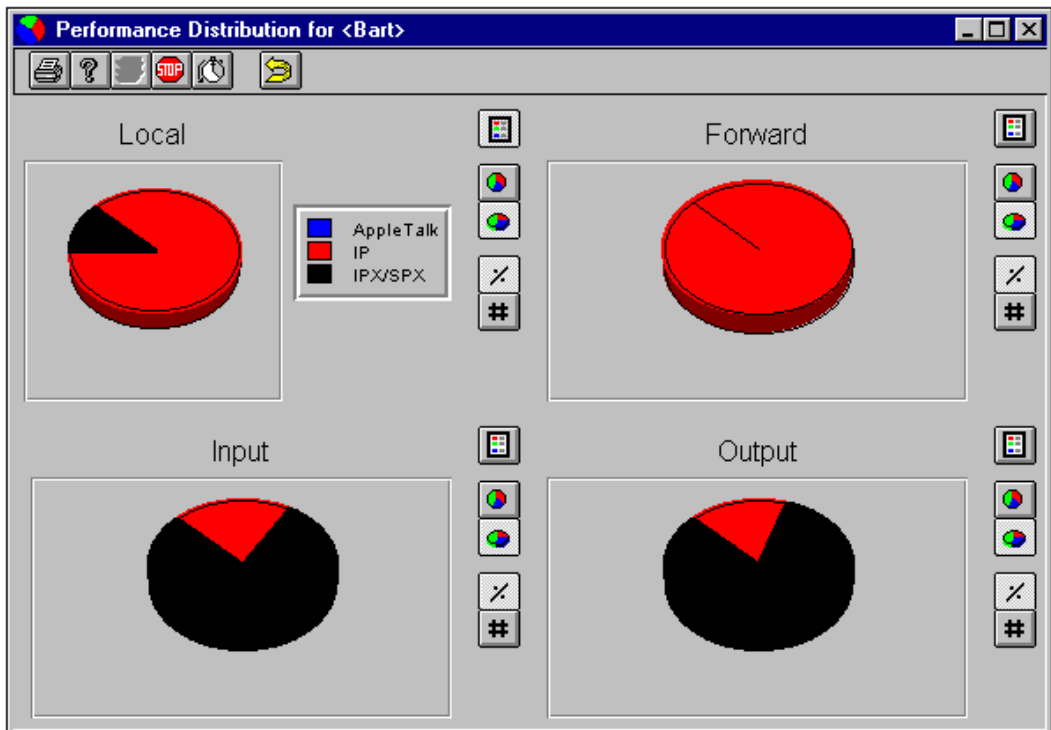
13

## Performance Distribution

### The Performance Distribution applet: Overview

The **Performance Distribution** applet shows the breakdown of a device's active protocols.

Performance information is displayed by packet type in pie chart format. Four pie charts are updated on the screen based on the polling interval. Data may be displayed in either count or percentage format. The default display is by count.



## Network Performance

---

Each of the four pie charts graphically depicts the through-put for one specific packet type:

- Input
- Local
- Forward
- Output

Each packet type is further broken down by color-coded protocol. Click the left mouse button on the pie chart to see the current values for each protocol.

This information allows an administrator to determine which protocols are being utilized most/least and gives a general idea of where each is being utilized (on the LAN/WAN).






## Using the Performance Distribution applet

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Perf Distribution > Performance Distribution**. From the logical view, right-click the Performance Distribution icon and choose **Performance Distribution**.
3. Reset the polling interval if desired, and click [OK]. The Performance Distribution window will appear.

**Note for Wellfleet:** The applet will work with Wellfleet Software Version 5.XX. In Wellfleet Software Version 7.XX and above, find this Applet under the Interface Icon as the Performance Distribution Applet.

### Other buttons

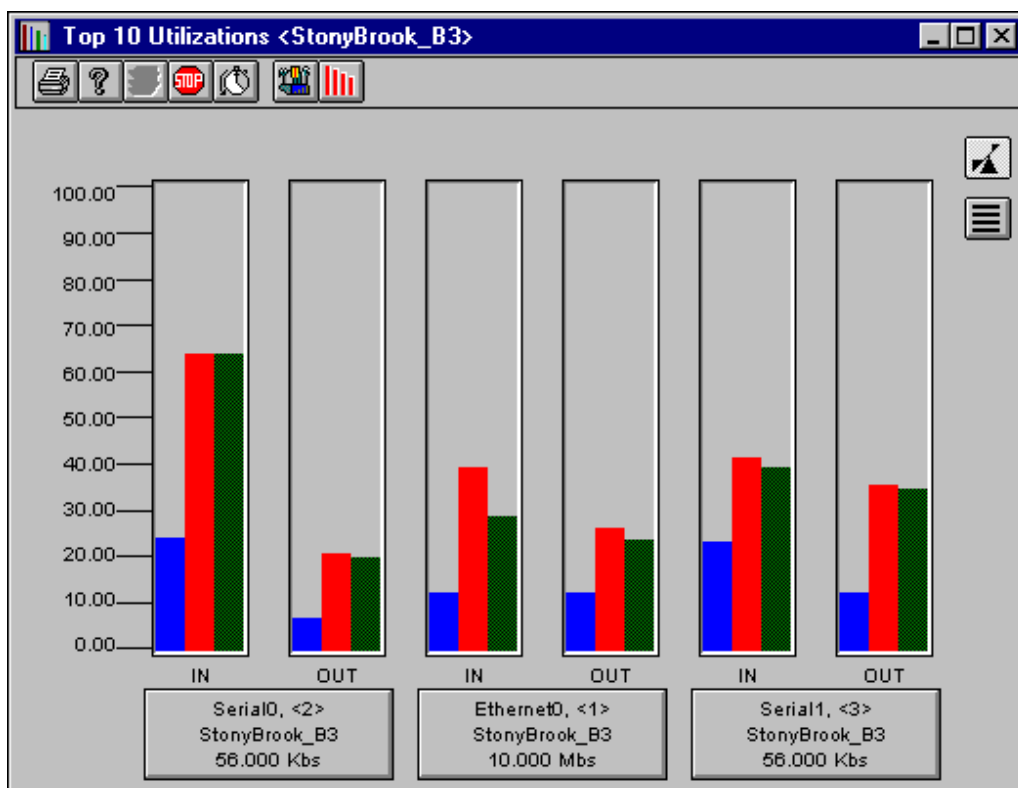
In addition to the global toolbar buttons , there are several other button functions available for the Performance Distribution applet.

Button	Description
	<p><b>[Show/Hide Pie Legend] button</b> Displays the key to the color-coded protocols, such as seen below.</p> <div data-bbox="548 730 719 830"></div> <p><b>NOTE:</b> 3Com routers do not support the IPX/SPX protocol for Performance Distribution.</p>
	<p><b>[Show/Hide 3D Effect] buttons</b> Toggles the pie chart between a 2D and 3D image.</p>
	<p><b>[Show Values/Show Percent] buttons</b> Toggle the pie charts between displaying information as a integer value (e.g., 10 alerts sent) or as a percentage (e.g. 10% of all alerts sent).</p>
	<p><b>[Zero Performance Distribution] button</b> Clears pie charts (provides zeros for variables) for information to regather. After clicking, a message will prompt you to confirm your selection.</p>

## Top 10 Utilization

### The Top-10 Utilization applet: Overview

The **Top-10 Utilization** applet allows you to quickly view the 10 most active interfaces connected to a device. Each interface has a separate graph showing the average, maximum and current utilization for both input and output.



In the example above, the Top 10 Utilization graph is for a router named StonyBrook\_B3 which has three interfaces: 2 serial and 1 Ethernet. The graph colors correspond to the following:

**Blue bar**

Average utilization over the monitoring period.

**Red bar**

Maximum utilization reached during the monitoring period.

**Green bar**





Current utilization.

## Using the Top 10 Utilization applet

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Top 10 Utilization > Top 10 Utilization**. From the application view, right-click the Top 10 Utilization icon and choose **Top 10 Utilization**.
3. Reset the polling interval if desired, and click [OK]. The Top 10 Utilization window will appear.

**Other buttons**

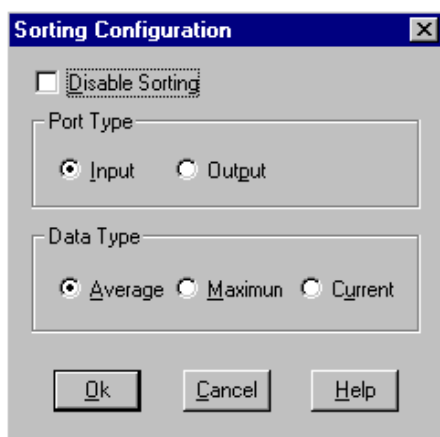
In addition to global toolbar buttons , there are four other button functions available for the Top 10 Utilization applet.

Button	Description
	<b>[Sort Configuration] button</b> Allows you to configure the parameters used to sort the data.
	<b>[Sort Data] button</b> Sorts data according to the parameters set in Sort Configuration
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

### Sorting data

To sort data:

1. Click the [Sort Configuration] button, to open the **Sorting Configuration** dialog box.



2. Click **Disable Sorting** if you do not want data to be sorted.
3. If you wish to sort data, choose from the following options:

#### Port Type

This will sort data based on **Input** or **Output**. For example, if you select Input, the graphs will sort themselves based on input utilization, with the highest input utilization being first.

#### Data Type

This will sort data based on **Average**, **Maximum** or **Current** utilization numbers. For example, if you choose Maximum, the graphs will sort themselves with the highest Maximum utilization level being first.

Port Type and Data Type work together. For example, if you choose Output and Current, graphs will be sorted based on Current Output statistics.

4. After making your selections, click [OK] to save your settings.
5. To arrange the graphs based on your configuration settings, click the [Sort Data] button .

## **IP Tools**

### **IP Tools: Overview**

The IP tools provide information about the IP protocol on your system.

Available tools are:

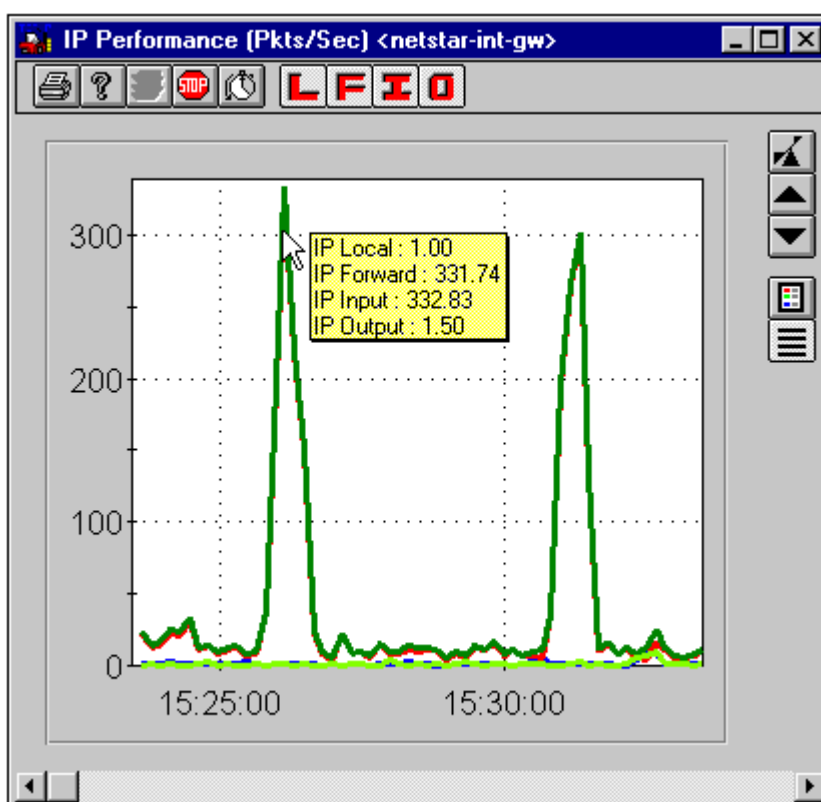
- **IP Performance applet**  
Provides performance information for IP devices.
- **IP Route Table applet**  
Provides route table information for IP devices, such as Next Hop Name and Hop Count.
- **IP Address Table applet**  
Provides address table information for IP devices, such as IP Address, Subnet Mask and Interface name.
- **IP Translation Table applet**  
Provides translation table information for IP devices, such as Physical Address and IP Address.
- **ICMP Statistics applet**  
Provides ICMP statistics for IP devices, such as number of messages sent/received, number of messages that couldn't be delivered, etc.
- **SNMP Statistics applet**  
Provides SNMP statistics for IP devices, such as number of input/output packets, number of get requests, etc.
- **Clear ARP applet (CISCO specific)**  
Allows you to clear the router's IP address table (CISCO devices only).

### The IP Performance applet

The **IP Performance** applet monitors Input, Forward, Local and Output packet statistics for the IP protocol. Data is displayed in packets per second, either in Delta format, which is the default setting, or Per Second format. Data is updated on the screen based on the polling interval selected.

The graph can be displayed in Line or Mountain style.

**NOTE:** For Bay/Wellfleet software version 7.XX and above, the IP performance is displayed on a per interface basis.



#### Reading the chart

The chart above shows IP Performance statistics using a Per Second format. At

the peak of the graph, a mouse click shows IP Forward at 331.74 packets per second and IP Input at 332.83 packets per second. Because the numbers are so close, it is hard to see the IP Forward line (red) behind the Input line (dark green). The Input line can be turned off by clicking the [Show/Hide Input Graph] button.

IP Local and Output and considerably less, and their lines are barely visible.

### Using the IP Performance applet



**To start the IP Performance applet:**








1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IP > Performance**. From the application view, right-click on the IP icon and select **Performance**.
3. Choose the applet parameters and click OK. The applet opens and IP performance statistics will begin to appear in the window, based on the polling interval.

Click the mouse on any point in the graph to view the precise statistics at that point.

#### Other buttons

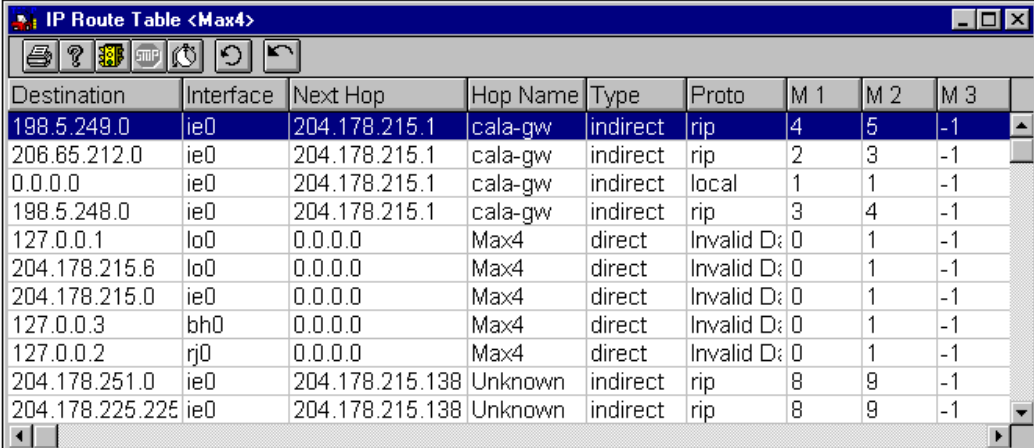
In addition to the global toolbar buttons, the IP Performance applet has the following specialized buttons:

Button	Description
 	<p><b>[Autoscale Graph] buttons</b></p> <p>Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.</p>

Button	Description
	<p><b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coded protocols, such as seen below.</p> 
	<p><b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.</p>
	<p><b>[Show/Hide Local Graph] button</b> Show and hide the graph for Local packet statistics.</p>
	<p><b>[Show/Hide Forward Graph] button</b> Show and hide the graph for Forward packet statistics.</p>
	<p><b>[Show/Hide Input Graph] button</b> Show and hide the graph for Input packet statistics.</p>
	<p><b>[Show/Hide Output Graph] button</b> Show and hide the graph for Output packet statistics.</p>

## The IP Route Table applet

The **IP Route Table** gives a list of known routes for the selected device.



The screenshot shows a window titled "IP Route Table <Max4>". It contains a table with the following columns: Destination, Interface, Next Hop, Hop Name, Type, Proto, M 1, M 2, and M 3. The table lists several routes, including indirect routes to 198.5.249.0, 206.65.212.0, and 0.0.0.0, and direct routes to 127.0.0.1, 204.178.215.6, 204.178.215.0, 127.0.0.3, 127.0.0.2, 204.178.251.0, and 204.178.225.225.

Destination	Interface	Next Hop	Hop Name	Type	Proto	M 1	M 2	M 3
198.5.249.0	ie0	204.178.215.1	cala-gw	indirect	rip	4	5	-1
206.65.212.0	ie0	204.178.215.1	cala-gw	indirect	rip	2	3	-1
0.0.0.0	ie0	204.178.215.1	cala-gw	indirect	local	1	1	-1
198.5.248.0	ie0	204.178.215.1	cala-gw	indirect	rip	3	4	-1
127.0.0.1	lo0	0.0.0.0	Max4	direct	Invalid D	0	1	-1
204.178.215.6	lo0	0.0.0.0	Max4	direct	Invalid D	0	1	-1
204.178.215.0	ie0	0.0.0.0	Max4	direct	Invalid D	0	1	-1
127.0.0.3	bh0	0.0.0.0	Max4	direct	Invalid D	0	1	-1
127.0.0.2	rj0	0.0.0.0	Max4	direct	Invalid D	0	1	-1
204.178.251.0	ie0	204.178.215.138	Unknown	indirect	rip	8	9	-1
204.178.225.225	ie0	204.178.215.138	Unknown	indirect	rip	8	9	-1

The following information is displayed in the IP Route Table:

Route Table Field	Description
Destination	The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table.
Interface	Interface name of the link to next device.
Next Hop	The IP address of the next hop of this route.
Hop Name	The name of the next device on the interface path.
Type	The type of route (See list of Route Types below).
Proto	How the route is discovered (see list below).
M1	Routing Metric 1.
M2	Routing Metric 2.

Route Table Field	Description
M3	Routing Metric 3.
M4	Routing Metric 4.
Age	Number of seconds since the last update to this route table entry.
Mask	IP subnet mask.

### Type Field:

The **Type** field contains the type of route. The values direct and indirect refer to the notion of direct and indirect routing in the IP architecture. Possible values for the Type field are:

Type	Description
Direct	Straight to destination device.
Indirect	Route goes through at least one other device.
Invalid	Destination device is currently unreachable.

### Proto Field:

The **Proto** field displays the routing mechanism used to learn this route. Possible values for the Proto field are:

Protocol	Description
local	Direct to destination device
rip	Router Information Protocol
netmgmt	Sent via a network management protocol
icmp	Obtained via ICMP-- e.g., Redirect
egp	A gateway routing protocol
ggp	A gateway routing protocol
hello	A gateway routing protocol

---

Protocol	Description
is-is	A gateway routing protocol
es-is	A gateway routing protocol
ciscoIgrp	A gateway routing protocol
bbnSpfIgp	A gateway routing protocol
ospf	A gateway routing protocol
bgp	A gateway routing protocol

## Using the IP Route Table applet

**To start the IP Route Table applet:**

1. Use one of the following:
  - a. Right-click on a device icon or backpanel and select IP Route Table.
  - b. Right-click on the IP icon in the Boxmap and select Route Table.
2. Choose the applet parameters and click OK. The applet opens and route table information will begin to appear in the window.

Depending on the number of entries, it may take some time to finish building the table.

### Viewing the Next Hop Route Table: Device Hopping

You can easily view the Route Table for the device in the Next Hop field by double-clicking on the respective row in the route table. This will launch Device Hopping and present the Next Hop Route Table. All listed devices can be launched in this way. Note, however, that if the device in the Next Hop field is the same device that you are monitoring, double-clicking will have no effect.

If a device in the route table has not been previously discovered, Device Hopping will discover the device and add it to the Group Wizard window.

### What if it fails?

After double-clicking in the IP Route Table row, if for some reason the table

## Network Performance

---

fails to appear filled in with route table detail, the MIBII button will be present on the toolbar and you will receive a message saying that the device could not be communicated with.

Pressing the MIBII button will open the configuration box for the device, allowing you to edit the read/write community strings.



After the community strings are edited correctly, you will be asked if you wish to update the device database. After clicking the [Yes] button, press the rescan button to fill in the table detail immediately, or wait for the next SNMP request.

### Viewing the Interface Table

You can launch the Interface applet for the current device by double-clicking any column heading. The Interface applet aids in mapping the interface number listed in the Route Table to the actual interface on the device.

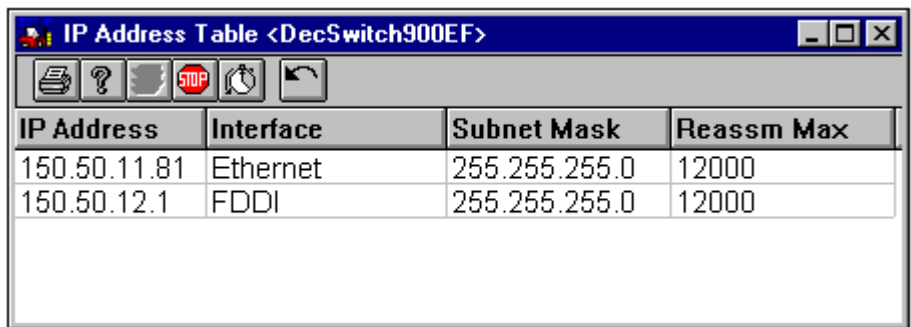
### Other buttons

In addition to the global toolbar buttons, the IP Route Table applet has two specialized buttons on the right hand side of the toolbar:

Button	Description
	<b>[Rescan Table] button</b> When the Stop Default is set in the System Options Configuration dialog box, polling is stopped (the Stop button on the toolbar is grayed out). This button rescans the table.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The IP Address Table applet

The **IP Address Table** applet displays the IP addresses of each interface the device contains. If Interface with Other Type is checked (active) in the System Options dialog box, interfaces with type “other” will also be displayed.



IP Address	Interface	Subnet Mask	Reassm Max
150.50.11.81	Ethernet	255.255.255.0	12000
150.50.12.1	FDDI	255.255.255.0	12000

The following information is displayed in the IP Address Table window:

Address Table Field	Description
IP Address	Network address of the interface
Interface	Interface name of the link to next device
Subnet Mask	IP subnet mask
Reassm Max	Reassembly Maximum—largest single packet that can be sent on this interface

## Using the IP Address Table applet

To start the IP Address Table applet:

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose IP > Address Table. From the application view, right-click on the

## Network Performance


---

IP icon and select Address Table.

3. Choose the applet parameters and click OK. The applet opens and address table information will appear in the window.







### Other buttons

In addition to the global toolbar buttons, the IP Address Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The IP Translation Table applet

The **IP Translation Table** applet gives a logical-to-physical mapping of all destination devices for the current device for a given (non-serial) media:

IP Translation Table <switchy>			
     			
Interface	Physical Addr	IP Address	Media Type
sc0	00000C096E6A	50.2.11.1	dynamic
sc0	00805FAA16AB	150.50.23.19	dynamic
sc0	00C07B6B5224	150.50.23.91	dynamic
sc0	00001D01B708	150.50.23.123	dynamic
sc0	008029EDC7B6	204.97.112.226	dynamic
sc0	00AA005FE803	204.97.112.230	dynamic
sc0	00AA00D30020	204.97.112.234	dynamic
sc0	0020AF0E3C63	204.97.112.247	dynamic
sc0	00AA00BB2B6E	204.97.112.251	dynamic
sc0	00AA0057D441	204.97.112.253	dynamic

The following information is displayed in the IP Translation Table window:

Translation Table Field	Description
Interface	Interface name of link to the next device
Physical Addr	MAC address
IP Address	Network address of the interface
Media type	Type of network (see list of values below)

### Media Type

The Media Type field displays the type of mapping performed. Possible values are:

Media Type	Description
dynamic	This usually means the interface was learned via Address Resolution Protocol (ARP), i.e., via a dynamic protocol discovery process.
Other	Not otherwise defined; this usually means that there is a direct interface to the destination device.
Static	The address was statically entered into the device.
Invalid	The destination device is currently unreachable.

## Using the IP Translation Table applet

To start the IP Address Table applet:

1. Right-click on a device icon and select Boxmap.


## Network Performance

---

2. From the physical view, right-click on a blank area in the window and choose IP > Address Table. From the application view, right-click the IP icon and select Address Table.
3. Choose the applet parameters and click OK. The applet opens and translation table information will appear in the window.

### Other buttons

In addition to the global toolbar buttons the IP Address Table applet has one specialized button on the right hand side of the toolbar:

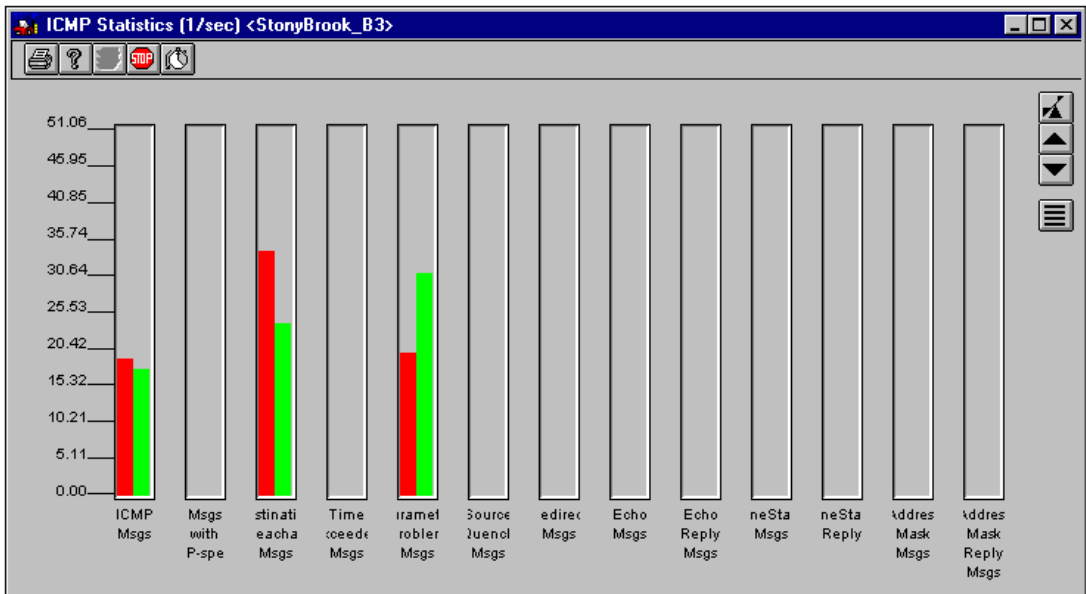
Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The ICMP Statistics applet

The **Internet Control Message Protocol (ICMP)** is an error reporting mechanism that enables devices to control the flow of IP information throughout a network. When a problem is encountered in delivering an IP packet, the device sends an ICMP message to the source device.

### Ping

A more familiar use of ICMP to most administrators is the PING utility which sends ICMP Echo requests. Any IP host may send an ICMP Echo Request (PING) to any other IP host and expect an Echo Response. The PING utility is very useful for checking if a remote host can be reached.



The ICMP Statistics applet uses color-coded bars to show statistics in an easy-to-read format (**red** = messages received, **green** = messages sent). Position the mouse on any bar and the value of the bar and name of the error will be reported.

ICMP error conditions monitored by the **ICMP Statistics** applet include:

Gauge Name/ Definition	Description
ICMP Msgs Received/Sent	The total of ICMP messages received/sent.
Msgs with ICMP Specific Errors	The total errors in ICMP messages.
Destination Unreachable Msgs	A destination unreachable message signifies that an IP packet could not be delivered. Two of the most frequent causes are a temporary hardware problem or an unknown destination network address.

Gauge Name/ Definition	Description
Time Exceeded Msgs	A time exceeded condition denotes that a device has processed a packet that has a hop count of zero.
Parameter Problem Msgs	A device sends a parameter problem when it detects a problem not covered by other error conditions.
Source Quench Msgs	A source quench message is used by a device to inform an IP host that it is experiencing temporary congestion problems. This is often caused by a saturated WAN link or a lack of interface buffers. Upon receiving a source quench message, an IP host slows down its transmit rate until it stops receiving further source quench messages.
Redirect Msgs	Informs (Redirects) host that a better route was available.
Echo Msgs	PING requests.
Echo Reply Msgs	PING responses.
TimeStamp Msgs	Requests required time stamping.
TimeStamp Reply Msgs	Replies to time stamp requests.
Address Mask Msgs	Requests for Address Masks.
Address Mask Reply Msgs	Replies to Address Mask requests.

### Using the ICMP Statistics applet

To start the ICMP Statistics applet:



1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IP > ICMP Statistics**. From the application view, right-click on the IP icon and select **ICMP Statistics**.

3. Choose the applet parameters and click OK. The applet opens and ICMP statistics will appear in the window based on the polling interval.

Note that graph readings depend on the polling interval. The graph displays the number of errors recorded during each polling interval. For example, if the polling interval is 60 seconds, the graph will display the total number of messages in the previous 60 seconds. The graph will redraw itself at the end of each polling interval.

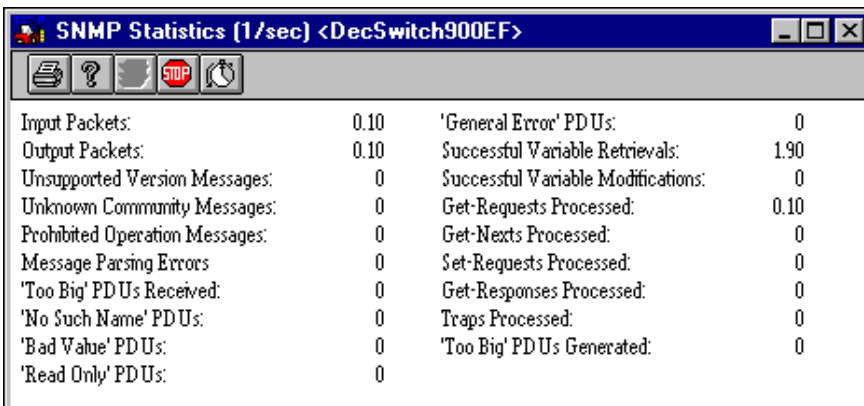
#### Other buttons

In addition to the global toolbar buttons, the ICMP Statistics applet has two specialized button functions:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## The SNMP Statistics applet

The **SNMP Statistics** applet presents statistical information related to SNMP.



## Network Performance

---

The following information is displayed in the SNMP Statistics window:

SNMP Field	Definition
<b>Input Packets</b>	The number of SNMP packets received.
<b>Output Packets</b>	The number of SNMP packets transmitted.
<b>Unsupported Version Messages</b>	The number of Unsupported Version Messages.
<b>Unknown Community Messages</b>	The number of Unknown Community Messages.
<b>Prohibited Operation Messages</b>	The number of Prohibited Operation Messages.
<b>Message Parsing Errors</b>	The number of errors detected while parsing SNMP messages.
<b>‘Too’ Big PDUs Received</b>	The number of SNMP messages received which were too large to process.
<b>‘No Such Name’ PDUs</b>	The number of SNMP messages received which contained a request for information not present on the device.
<b>‘Bad Value’ PDUs</b>	The number of SNMP messages received which contained a bad value.
<b>‘Read Only’ PDUs</b>	The number of SNMP set messages received which did not have read/write privilege.
<b>‘General Error’ PDUs</b>	The number of SNMP messages received which could not be processed for other than the above reasons.
<b>Successful Var Retrievals</b>	The number of SNMP variables responded to.
<b>Successful Var Modifications</b>	The number of SNMP variables modified on the device.

<b>Get-Request Processed</b>	The number of SNMP get messages processed by the device.
<b>Get-Next Processed</b>	The number of SNMP get-next messages processed by the device.
<b>Set-Request Processed</b>	The number of SNMP set messages processed by the device.
<b>Get-Response Processed</b>	The number of SNMP responses sent by the device.
<b>Traps Processed:</b>	The number of Trap messages sent by the device.
<b>'Too Big' PDUs Generated</b>	The number of SNMP messages generated where the PDU was too big to send.

## Using the SNMP Statistics applet

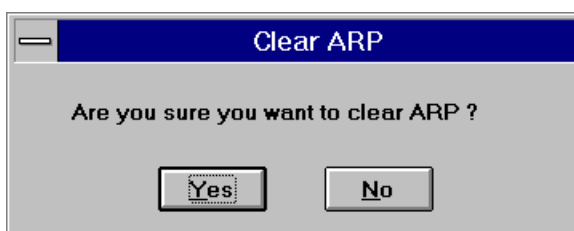
To start the IP Address Table applet:

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose IP > SNMP Statistics. From the application view, right-click on the IP iconICON\_IP and select SNMP Statistics.
3. Choose the applet parameters>main and click OK. The applet opens and SNMP statistics will appear in the window based on the polling interval.

The SNMP Statistics applet also utilizes global toolbar button functions.

### The Clear ARP Applet: Cisco specific

Specific for Cisco Routers using 9.2 and above software, is the Clear ARP (Address Resolution Protocol) Applet. When the applet is opened, the following message box is presented:



Clicking on [Yes] will clear the router's IP address table and refresh the table.

## **IPX tools**

### **IPX/SPX Tools: Overview**

The IPX/SPX tools provide information about the IPX/SPX protocol on your system.

Available tools are:

- **The IPX/SPX Performance applet**  
Provides performance information for IPX/SPX devices.
- **IPX/SPX Route Table applet**  
Provides route table information for IPX/SPX devices, such as Next Hop Name and Hop Count.
- **IPX/SPX SAP Table applet**  
Provides SAP information for IPX/SPX devices, such as Service Type, Name and Node Number.
- **IPX/SPX Overview applet**  
Provides system and circuit information for IPX/SPX devices, such as System Address, number of known networks and circuits, network number, interface name, throughput, etc. Also provides NLSP Circuit information and IPX Compression information.

### **NLSP Tools**

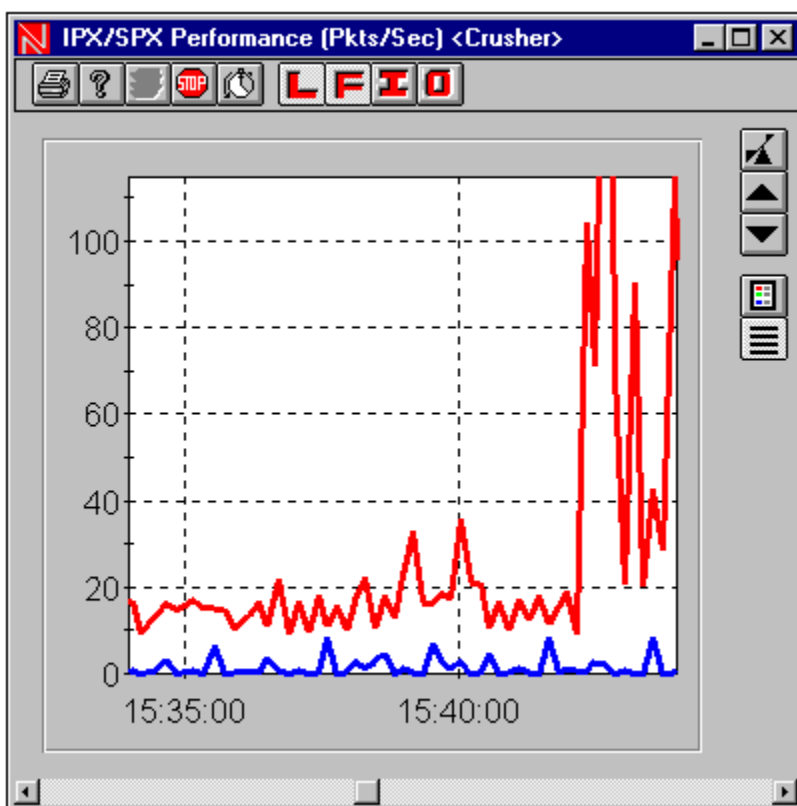
There are also specific tools that provide information for NLSP (NetWare Link Services Protocol). See "NLSP Tools: Overview" on page 442 for details.

### The IPX/SPX Performance applet

The **IPX/SPX Performance** applet monitors Input , Forward , Local , and Output packet statistics for the IPX/SPX protocol . Data may be displayed either in Delta , which is the default setting, or Per Second format. Data is updated on the screen based on the polling interval selected.

The graph can be displayed in Line or Mountain style.

**NOTE:** Not available for 3Com. Not available for Wellfleet version 7.XX and 8.XX.



## Using the IPX/SPX Performance applet



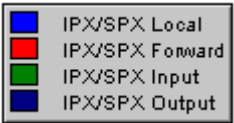


### To start the IPX/SPX Performance applet:




1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose IPX > Performance. From the application view, right-click the IPX icon in the Boxmap and choose Performance.
3. Choose the applet parameters and click OK. The applet opens and IPX/SPX performance statistics will begin to appear in the window, based on the polling interval .

Click the mouse on any point in the graph to view the precise statistics at that point.

### Other buttons

In addition to the global toolbar buttons , the IPX/SPX Performance applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coded protocols, such as seen below.  
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.
	<b>[Show/Hide Local Graph] button</b> Show and hide the graph for Local packet statistics.

Button	Description
	<b>[Show/Hide Forward Graph] button</b> Show and hide the graph for Forward packet statistics.
	<b>[Show/Hide Input Graph] button</b> Show and hide the graph for Input packet statistics.
	<b>[Show/Hide Output Graph] button</b> Show and hide the graph for Output packet statistics.

### The IPX/SPX Route Table applet

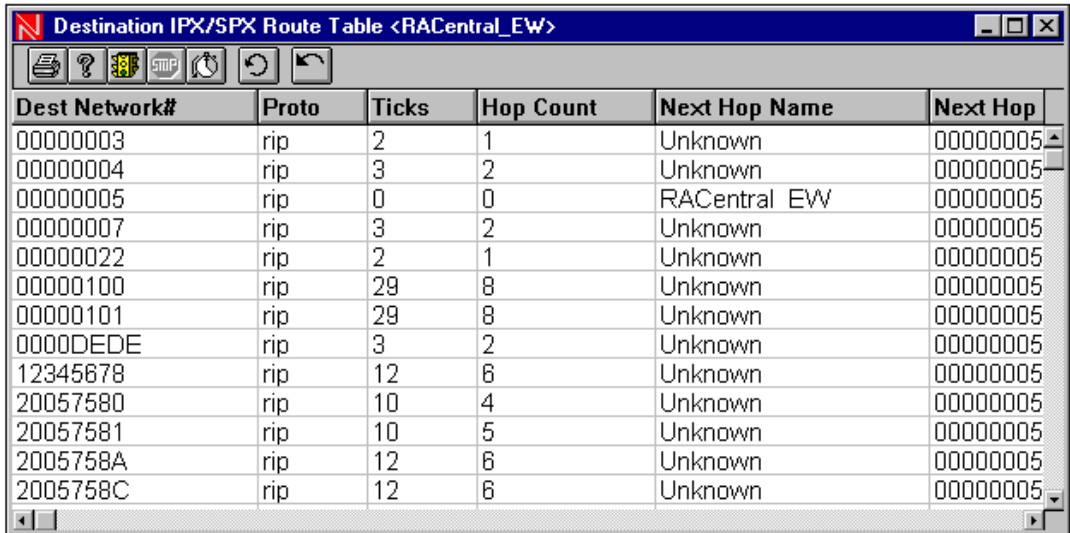
The **IPX/SPX Route Table** contains information about each known IPX destination.

There are two types of route tables: Destination and Static.

#### The Destination Route Table

The Destination Table contains all known IPX destinations regardless of how the route was learned. The Destination Table is useful in determining the current path between any two networks.

IPX destination networks are sorted in ascending order initially. (You can switch to descending order by clicking the column heading.)



Dest Network#	Proto	Ticks	Hop Count	Next Hop Name	Next Hop
00000003	rip	2	1	Unknown	00000005
00000004	rip	3	2	Unknown	00000005
00000005	rip	0	0	RACentral_EW	00000005
00000007	rip	3	2	Unknown	00000005
00000022	rip	2	1	Unknown	00000005
00000100	rip	29	8	Unknown	00000005
00000101	rip	29	8	Unknown	00000005
0000DEDE	rip	3	2	Unknown	00000005
12345678	rip	12	6	Unknown	00000005
20057580	rip	10	4	Unknown	00000005
20057581	rip	10	5	Unknown	00000005
2005758A	rip	12	6	Unknown	00000005
2005758C	rip	12	6	Unknown	00000005

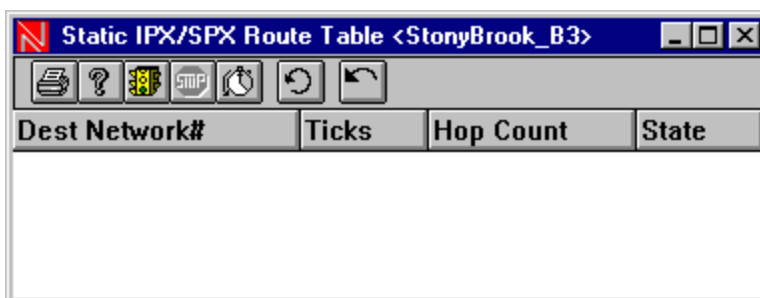
The following information is displayed in the Destination IPX/SPX Route Table:

Route Table Field	Description
<b>Dest Network #</b>	The IPX network number of the destination network.
<b>Proto</b>	The method by which the route was learned. (Possible values include Other, Local, RIP, NLSP and Static.)
<b>Ticks</b>	The delay in ticks (1/18th sec) to reach this destination.
<b>Hop Count</b>	The number of hops needed to reach this destination.
<b>Next Hop Name</b>	The device name of the next hop.
<b>Next Hop Network #</b>	The network address of the next hop.
<b>Next Hop Node #</b>	The node number of the next hop.

### The Static Route Table

The Static Table is a subset of the Destination Table and lists all static routes manually defined for the IPX instance. Static routes are often used for dial-up and ISDN connections. They are manually entered through INETCFG. If there is more than one entry for a static route, only the active route is presented to the Destination Table.

If there are no static routes defined for the device, this table is empty.



The following information is displayed in the Static IPX/SPX Route Table:

Route Table Field	Description
<b>Dest Network#</b>	The IPX network number of the destination network.
<b>Ticks</b>	The delay in ticks (1/18th sec) to reach this destination.
<b>Hop Count</b>	The number of hops needed to reach this destination.
<b>State</b>	The validity of the route.(Possible values are On and Off).

### Using the IPX/SPX Route Table applet

To start the IPX/SPX Route Table applet:

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and

choose IPX > Route Table > Destination/Static. From the application view, right-click the IPX icon in the Boxmap and choose Route Table > Destination/Static.

3. Choose the applet parameters and click OK. The applet opens and route table information will begin to appear in the window.

Depending on the number of entries, it may take some time to finish building the table.

### Viewing the Next Hop Route Table: Device Hopping

You can easily view the Route Table for the device in the Next Hop Name field by double-clicking on the respective row in the route table. This will launch Device Hopping and present the Next Hop Route Table. All listed devices can be launched in this way. Note, however, that if the device in the Next Hop field is the same device that you are monitoring, double-clicking will have no effect.



If a device in the route table has not been previously discovered, Device Hopping will discover the device and add it to the Show Device(s) window.

### Viewing the Interface Table

You can launch the Interface Table applet for the current device by double-clicking any column heading. The Interface Table applet aids in mapping the interface number listed in the Route Table to the actual interface on the device.

### Other buttons

In addition to the global toolbar buttons, the IPX/SPX Route Table applet has two specialized buttons on the right hand side of the toolbar:

Button	Description
	<b>[Rescan Table] button</b> When the Stop Default is set in the System Options Configuration dialog box, polling is stopped (the Stop button on the toolbar is grayed out). This button rescans the table.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

### The IPX/SPX SAP Table applet

The **IPX/SPX SAP Table** applet lists all of the services known to the device through SAP messages received from other routers on the Internet.

On a Novell LAN, systems that provide network services, like faxing, backup, printing, etc. inform other systems of their availability through the Service Advertisement Protocol (SAP). Each service has a different SAP type number. When workstations want to access a particular service, they send a SAP request to a server or router. The server or router responds with the address of the requested service.

Two common occurrences on Novell networks are duplicate SAP entries and ghosting of services.

- **Duplicate SAP entries** are caused by two of the same SAP types having the same name. When a workstation makes a request for the service, the first entry is given in the response. This can lead to significant problems.

For example, suppose a workstation in New York requests an SNA gateway (type 21) named SNAGATE and there are two entries for SNAGATE in the SAP table, one located in Chicago and one in New York. If Chicago is listed before New York, then the New York workstation will connect to the Chicago SNA gateway. Unless the network is composed of very high speed WAN links, the workstation will suffer transmission delays connecting to Chicago as opposed to the local gateway in New York. If there are duplicate entries in the SAP table, consider changing the name of one.

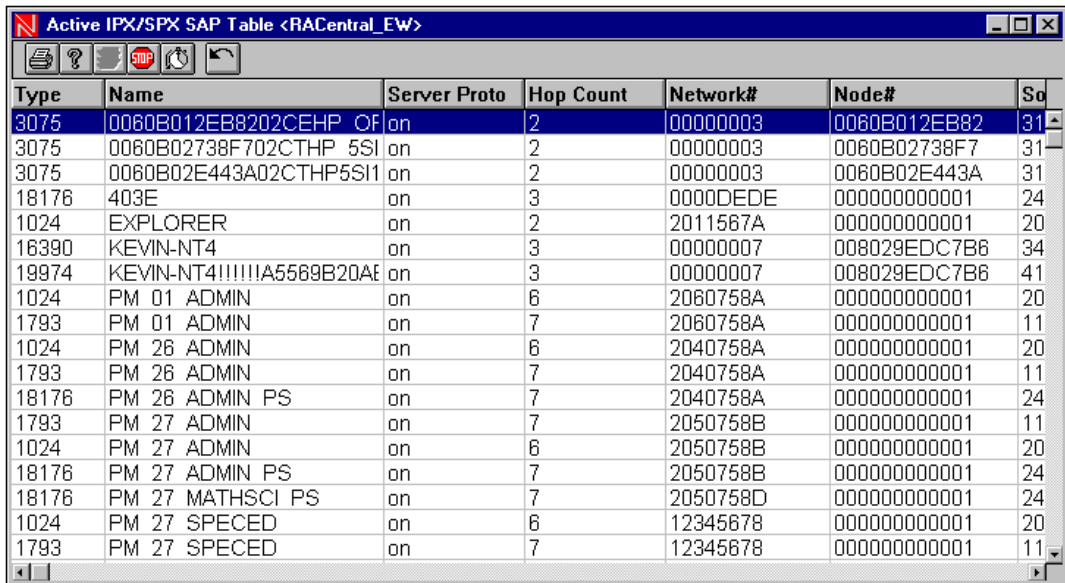
- **Ghosting** occurs when a server or router is overrun with packets, causing SAP updates to be lost. If consecutive service updates are lost, the router or server declares the service(s) unavailable. When an update does get through, the service is re-marked available. Thus, the effect of having services appear and then disappear, or ghosting.

Use the IPX/SPX SAP Table applet to find entries for ghosting services. When dropped packets are detected, alarm messages are sent into the Alarm Manager. If this occurs continuously, increase the number of receive buffers or upgrade to LSP.

There are two types of SAP tables: Active and Static.

### The Active SAP Table

The Active Table lists all services regardless of how the service was learned. The table shown below lists the available services indexed by type and name.



Type	Name	Server Proto	Hop Count	Network#	Node#	Socket
3075	0060B012EB8202CEHP_QF	on	2	00000003	0060B012EB82	31
3075	0060B02738F702CTHP_5SI	on	2	00000003	0060B02738F7	31
3075	0060B02E443A02CTHP5SI1	on	2	00000003	0060B02E443A	31
18176	403E	on	3	0000DEDE	000000000001	24
1024	EXPLORER	on	2	2011567A	000000000001	20
16390	KEVIN-NT4	on	3	00000007	008029EDC7B8	34
19974	KEVIN-NT4!!!!!!A5569B20AE	on	3	00000007	008029EDC7B8	41
1024	PM_01_ADMIN	on	6	2060758A	000000000001	20
1793	PM_01_ADMIN	on	7	2060758A	000000000001	11
1024	PM_26_ADMIN	on	6	2040758A	000000000001	20
1793	PM_26_ADMIN	on	7	2040758A	000000000001	11
18176	PM_26_ADMIN_PS	on	7	2040758A	000000000001	24
1793	PM_27_ADMIN	on	7	2050758B	000000000001	11
1024	PM_27_ADMIN	on	6	2050758B	000000000001	20
18176	PM_27_ADMIN_PS	on	7	2050758B	000000000001	24
18176	PM_27_MATHSCI_PS	on	7	2050758D	000000000001	24
1024	PM_27_SPECED	on	6	12345678	000000000001	20
1793	PM_27_SPECED	on	7	12345678	000000000001	11

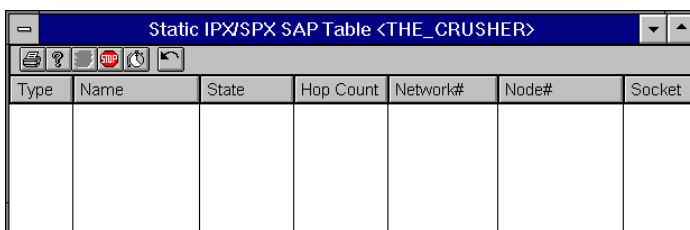
The following information is displayed in the Active IPX/SPX SAP table window:

Heading	Description
Type	The SAP type provides the numerical type of service provided.
Name	The alphanumeric name of the service.
Server Proto	The protocol by which the service was learned.
Hop Count	The number of hops to reach the service.
Network #	The IPX network number that the service is attached to.
Node #	The IPX node number of the service.
Socket	The IPX socket that the service is available on.

### The Static SAP Table

The Static Table is a subset of the Active table. It lists all services manually defined to the system.

If there are no static routes defined, this table is empty.



Type	Name	State	Hop Count	Network#	Node#	Socket
------	------	-------	-----------	----------	-------	--------

The following information is displayed in the Static IPX/SPX SAP table window:

Heading	Description
Type	The SAP type provides the numerical type of service provided.
Name	The alphanumeric name of the service.
State	The validity of the entry. The possible values are On and Off.
Hop Count	The number of hops to reach the service.
Network #	The IPX network number that the service is attached to.
Node #	The IPX node number of the service.
Socket	The IPX socket that the service is available on.

### Using the IPX/SPX SAP Table applet

To start the IPX/SPX SAP Table applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and



choose **IPX > SAP Table > Active/Static**. From the application view, right-click the IPX icon in the Boxmap and choose **SAP Table > Active/Static**.

3. Choose the applet parameters and click OK. The applet opens and SAP table information will begin to appear in the window.

Depending on the number of entries, it may take some time to finish building the table.

### Other buttons

In addition to the global toolbar buttons, the IPX/SPX Route Table applet has two specialized buttons on the right hand side of the toolbar:

Button	Description
	<b>[Rescan Table] button</b> When the Stop Default is set in the System Options Configuration dialog box, polling is stopped (the Stop button on the toolbar is grayed out). This button rescans the table.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The IPX/SPX Overview applet

The **IPX/SPX Overview** applet presents a consolidated view of the IPX configuration of the device. The top pane lists system information. The bottom table lists the known IPX circuits. The two local buttons in the toolbar provide access to NLSP Circuit and Compression information.

**NOTE:** Not available for 3Com, Wellfleet, and Cisco software versions under 10.3.

## Network Performance

IPX/SPX Overview for <Crusher>					
Configuration Summary					
Name:	THE_CRUSHER	State:	On		
Address:	2D6C140A:000000000001	Num of Known Circuits:	3		
Num of Known Networks:	163	Num of Known Services:	297		
Net #	Interface Name	State	Oper State	Media Type	Type
00000007	Intel EtherExpress(tm) PRO C	on	up	Ethernet II	broadc
00000003	Novell NE2000	on	up	Ethernet II	broadc
00000004	Novell NE2000	on	up	IEEE 802.3 wi	broadc

The following information is displayed in the top pane of the IPX/SPX Overview window:

Topic	Definition
Name	The alphanumeric name for this system.
State	The state of this IPX process (possible values are On and Off).
Address	The IPX address of the device in Network:Node format.
Num of Known Circuits	The total number of circuits defined on the device.
Num of Known Networks	The total number of IPX networks known by the device.
Num of Known Services	The number of known services (SAP ) known by the device.

The following information is displayed in the bottom pane of the IPX/SPX Overview window:

Heading	Definition
<b>Net #</b>	The IPX network number.
<b>Interface Name</b>	The name of the interface.
<b>State</b>	The state of the circuit (possible values are On and Off).
<b>Oper State</b>	The operational state.
<b>Media Type</b>	The Media type.
<b>Type</b>	The type of circuit
<b>Throughput</b>	The amount of data, in bits per second, that may flow through the interface.
<b>Delay</b>	The time period, expressed in micro seconds, one byte of data takes to transverse the link and be received by the destination.
<b>Neighbor Name</b>	The name of the neighboring device on a WAN circuit.
<b>Neighbor Net #</b>	The internal IPX number of the neighbor device on a WAN circuit.
<b>State Changes</b>	The number of times the circuit has changed state.
<b>Init Fails</b>	The number of times the circuit has failed initialization.
<b>Circ Index</b>	The unique identifier of the circuit.

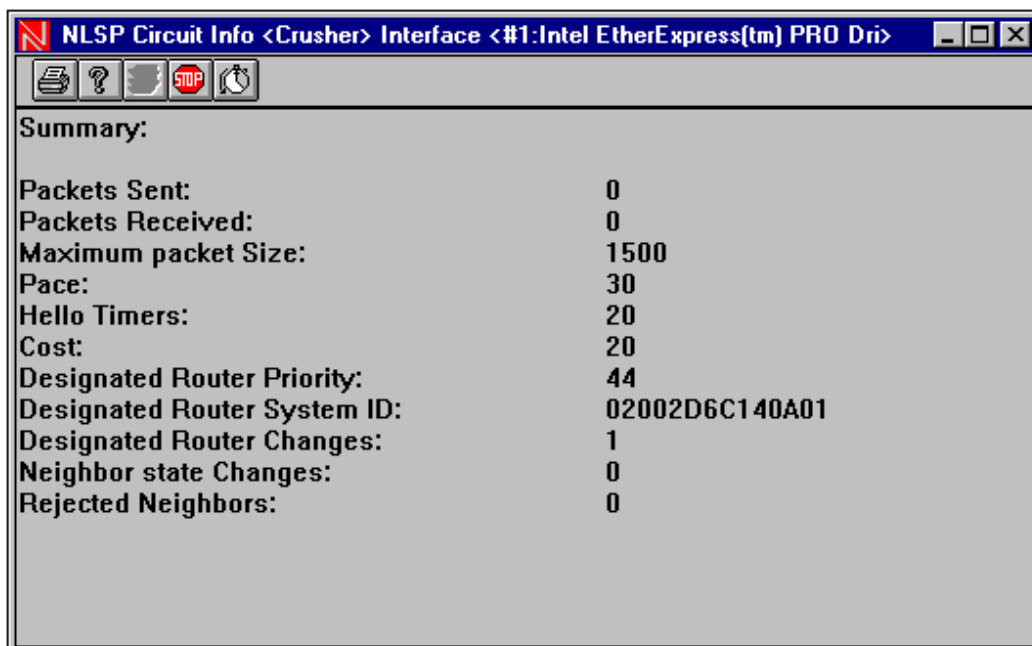
### Using the IPX/SPX Overview applet

#### To start the IPX/SPX Overview applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IPX > Overview**. From the application view, right-click the IPX icon in the Boxmap and choose **Overview**.
3. Choose the applet parameters and click **OK**. The applet opens and information will appear in the window.

#### Checking NLSP Circuit information

4. Click on the [NLSP] button to present the NLSP Circuit Information for the selected row (circuit). It displays NLSP configuration and counters for the selected circuit. This button will not be available if NLSP is not configured on the router.



NLSP LAN and WAN circuits exhibit different error conditions. Problems on NLSP LAN circuits usually cause the Designated Router or the Neighbor State to change. Normally, the designated router remains fairly static. If the “Designated Router Changes” counter increases more than 3 times a day, or the “Neighbor State Changes” counter increases more than once every five minutes, it needs to be explored.

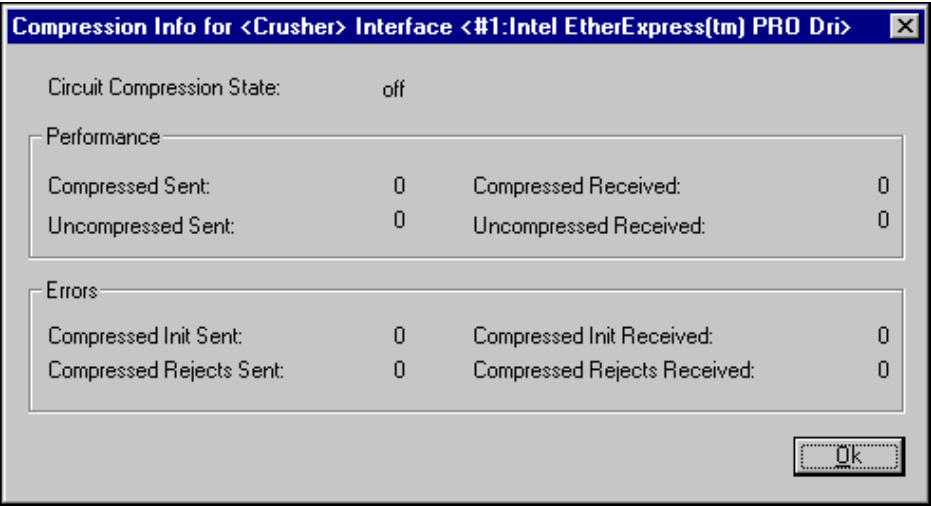
Each Designated Router and Neighbor State Change causes network disruption that can affect an entire area. NLSP WAN circuits that are not configured correctly will detect a large number of Rejected Neighbors.

The Summary Information in the NLSP Circuit Information window includes:

Heading	Definition
<b>Packets Sent</b>	The number of NLSP packets sent.
<b>Packets Received</b>	The number of NLSP packets received.
<b>Maximum Packet Size</b>	The maximum packet size, including heading, that this interface supports.
<b>Pace</b>	The maximum rate, in packets per second, that NLSP information is sent.
<b>Hello Timers</b>	The interval, in seconds, between NLSP Hello packets.
<b>Cost</b>	The Default NLSP Cost.
<b>Designated Router Priority</b>	The defined priority for becoming the Designated Router on a broadcast circuit.
<b>Designated Router System ID</b>	The system ID number for the NLSP router.
<b>Designated Router Changes</b>	The number of times the designated router has changed.
<b>Neighbor State Changes</b>	The number of times the NLSP neighbor state has changed.
<b>Rejected Neighbors</b>	The number of times an NLSP neighbor has been rejected.

Checking IPX Compression information

- 5. Click on the [Compression Information] button to present the **IPX Compression Information** for the selected row (circuit). IPX header compression is a feature of the IPXWAN 2 specification.



The Compression Information is divided into two sections Performance and Errors.

Performance information:

Heading	Definition
Circuit Compression State	The state of IPX header compression on this circuit.
Compressed Sent	The number of compressed packets sent.
Uncompressed Sent	The number of uncompressed packets sent.
Compressed Received	The number of compressed packets received.
Uncompressed Received	The number of uncompressed packets received.

Errors information:

Heading	Definition
<b>Compressed Init Sent</b>	The number of compression initialization packets sent.
<b>Compressed Rejects Sent</b>	The number of compression reject packets sent.
<b>Compressed Init Received</b>	The number of compression initialization packets received.
<b>Compressed Rejects Received</b>	The number of compression reject packets received.

## **NLSP Applets**

### **NLSP Tools: Overview**

The **NLSP tools** (NetWare Link Services Protocol) provide detailed information on the status of the NLSP process.

All MPR 3.X routers and NetWare servers running IPXRTR support the NLSP tools. If the NLSP process is not configured for the router, the tools will return blank tables.

There are five NLSP tools:

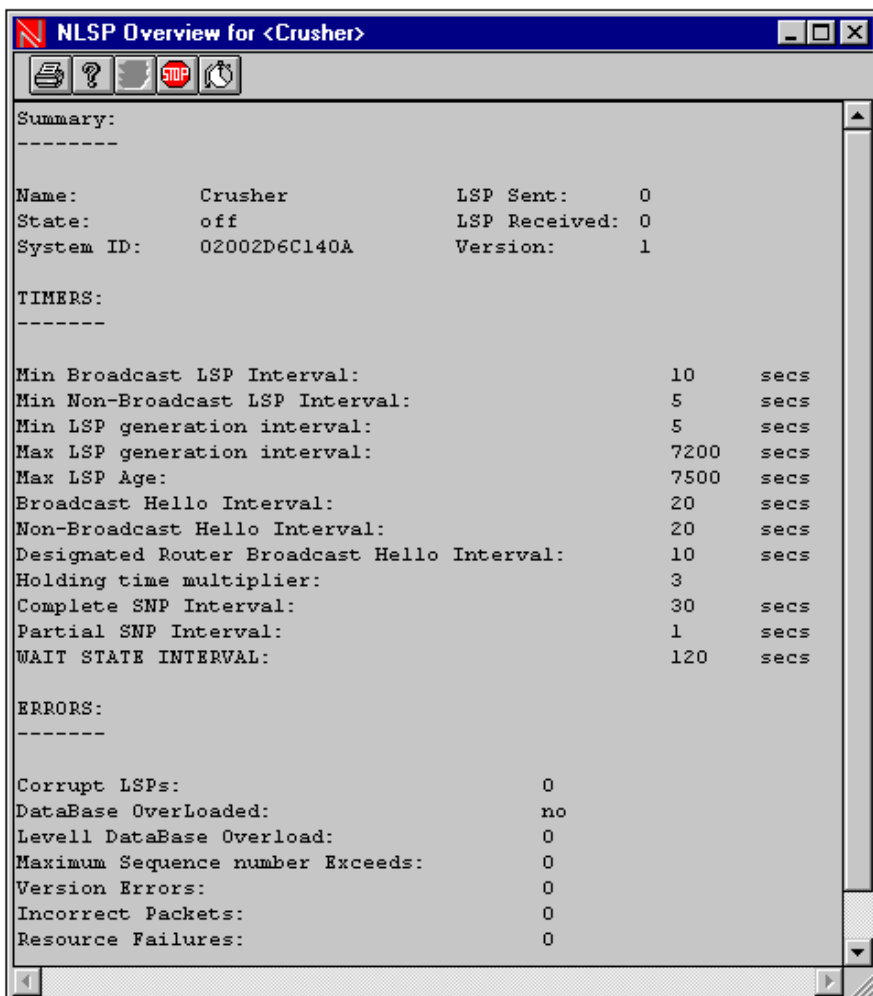
- **The NLSP Overview applet**  
Provides a comprehensive summary of the NLSP protocol on the router.
- **The NLSP Area Addresses applet**  
Provides information on NLSP Areas configured and used by the router.
- **The NLSP Neighbors Table applet**  
Displays all known NLSP neighbors for the router.
- **The NLSP Learned Routers applet**  
Correlates NLSP IDs to the router name.
- **The NLSP Learned Networks Table applet**  
Displays all IPX networks learned via NLSP.

**NOTE:** Not available for Wellfleet and Cisco software versions under 10.3.

## The NLSP Overview Applet

The **NLSP Overview** applet provides a comprehensive summary of the NLSP protocol running on the router. This Applet provides a quick view of the configuration of NLSP.

**NOTE:** Not available for Wellfleet and Cisco software versions under 10.3.



## Network Performance

---

The NLSP Overview screen has three sections:

- Summary Information
- Timers
- Errors

Summary Information Includes:

Title	Definition
<b>Name</b>	The name of the router.
<b>State</b>	The State of NLSP on the router (possible values are On and Off).
<b>System ID</b>	The system ID of the NLSP process.
<b>LSP Sent</b>	The number of LSPs transmitted.
<b>LSP Received</b>	The number of LSPs received.
<b>Version</b>	The version of NLSP running.

Timers Include:

Title	Definition
<b>Min Broadcast LSP Interval</b>	The minimum interval between LSP transmission on a broadcast circuit.
<b>Min Non-Broadcast LSP Interval</b>	The minimum interval between LSP transmission on a non-broadcast circuit.
<b>Min LSP generation interval</b>	The minimum interval between generating the same LSP.
<b>Max LSP Age</b>	The maximum interval between generating the same LSP.
<b>Broadcast Hello Interval</b>	The interval between successive NLSP Hellos on a broadcast circuit if not the Designated Router.
<b>Non-Broadcast Hello</b>	The interval between successive NLSP

Title	Definition
<b>Interval</b>	Hellos on a non-broadcast circuit.
<b>Designated Router Broadcast Hello Interval</b>	The interval at which the Designated Router sends NLSP Hello messages.
<b>Holding time multiplier</b>	The multiplier used to determine the holding time of NLSP neighbor entries.
<b>Complete SNP Interval</b>	The interval between generation of Complete Sequence Number Packets by a Designated Router of a broadcast circuit.
<b>Partial SNP Interval</b>	The interval between generation of Partial Sequence Number Packets.
<b>WAIT STATE INTERVAL</b>	The delay in the Waiting state before entering the On state.

Errors Include:

Title	Definition
<b>Corrupt LSPs</b>	The number of corrupt LSPs detected.
<b>DataBase OverLoaded</b>	Indicates if the NLSP database is currently overloaded.
<b>Level 1 Database Overload</b>	The number of times the NLSP database has become overloaded.
<b>Maximum Sequence number Exceeds</b>	The number of times the router has tried to exceed the NLSP's maximum sequence number.
<b>Version Errors</b>	The number of rejected NLSPs because of invalid version.
<b>Incorrect Packets</b>	The number of incorrectly formatted NLSPs received.
<b>Resource Failures</b>	The number of times NLSP could not obtain resources.

## Using the NLSP Overview applet

### To start the NLSP Overview applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IPX > NLSP > Overview**. From the application view, right-click the IPX icon in the Boxmap and choose **NLSP > Overview**.
3. Choose the applet parameters and click OK. The applet opens and information will appear in the window.

### Other buttons

The NLSP Overview applet uses the global toolbar buttons.

## The NLSP Area Addresses Applet

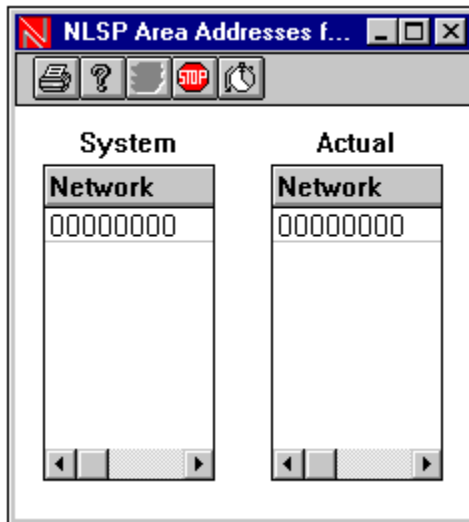
The **NLSP Area Addresses** applet provides information on the NLSP Areas configured and used by the router. The NLSP Area concept provides the functionality to build very large IPX based networks.

Level 1 NLSP routers are only required to keep detailed information on links within the area that they are directly attached to. They rely on Level 2 routers to provide the capability to interconnect to other areas.

### For Novell MPR

By default the MPR is a Level 1 router and does not define NLSP areas (the contents of this applet should be zeros, as illustrated below).

**NOTE:** Not available for Wellfleet and Cisco software versions under 10.3.



The Applet is divided into two parts, the System and Actual tables.

The **System** table displays the configured Areas and associated Masks. The **Actual** table displays the Areas that the router is actually connected to.

## Using the NLSP Area Address applet

To start the NLSP Area Address applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IPX > NLSP > Area Addresses**. From the application view, right-click the IPX icon in the Boxmap and choose **NLSP > Area Addresses**.
3. Choose the applet parameters and click OK. The applet opens and information will appear in the window.

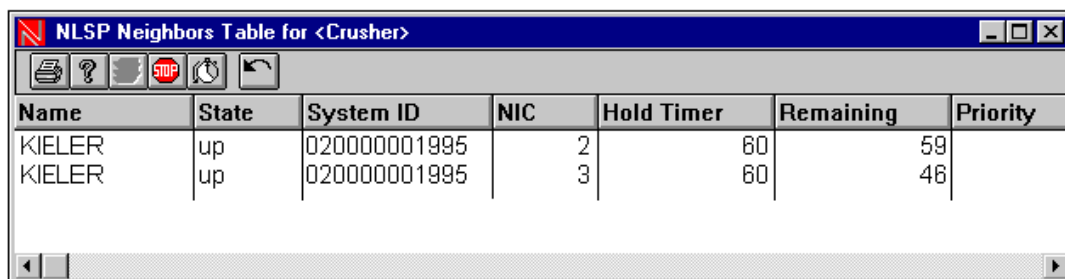
### Other buttons

The NLSP Area Address applet uses the global toolbar buttons.

## The NLSP Neighbors Table Applet

The **NLSP Neighbors Table** applet displays all known NLSP neighbors. The router learns of these neighbors through the transmitting and receiving of NLSP Hello messages.

**NOTE:** Not available for Wellfleet and Cisco software versions under 10.3.



Name	State	System ID	NIC	Hold Timer	Remaining	Priority
KIELER	up	020000001995	2	60	59	48
KIELER	up	020000001995	3	60	48	48

The following information is displayed in the NLSP Neighbors Table window:

Heading	Definition
Name	Name of the router.
State	The State of the connection to neighboring router (Possible values are Initializing, Up, Failed and Down).
System ID	The NLSP system ID of the neighboring router.
NIC	The Node address of the Neighboring router.
Hold Timer	The holding time of this NLSP neighbor.
Remaining	The time-to-live of this entry. This value is reset to Hold Times upon receipt of a Hello.
Priority	The Designated Router priority of the neighbor.


## Using the NLSP Neighbors Table applet

To start the NLSP Neighbors Table applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose IPX > NLSP > Neighbors. From the application view, right-click the IPX icon in the Boxmap and choose NLSP > Neighbors.
3. Choose the applet parameters and click OK. The applet opens and information will appear in the window.

### Other buttons

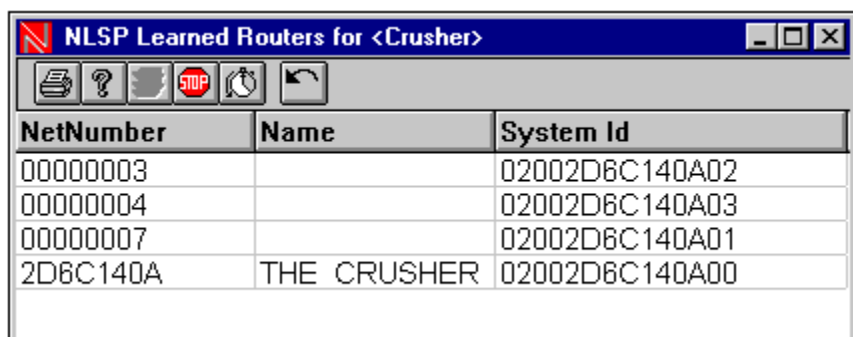
In addition to the global toolbar buttons, the NLSP Neighbors Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The NLSP Learned Routers Applet

The **NLSP Learned Routers** applet correlates the NLSP IDs to the router name.

**NOTE:** Not available for Wellfleet and Cisco software versions under 10.3.



NetNumber	Name	System Id
00000003		02002D6C140A02
00000004		02002D6C140A03
00000007		02002D6C140A01
2D6C140A	THE CRUSHER	02002D6C140A00

The following information is displayed in the NLSP Learned Routers window:

Heading	Definition
Net Number	The IPX network number.
Name	The name of the NLSP router.
System Id	The NLSP system ID number.


### Using the NSLP Learned Routers applet

To start the NLSP Learned Routers applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IPX > NLSP > Learned Routers**. From the application view, right-click the IPX icon in the Boxmap and choose **NLSP > Learned Routers**.
3. Choose the applet parameters and click OK. The applet opens and information will appear in the window.

#### Other buttons

In addition to the global toolbar buttons, the NLSP Learned Routers applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The NLSP Learned Networks Table Applet

The **Learned Networks Table** applet displays all of the IPX networks learned via NLSP. In most cases, the contents of this table do not reflect all of the known IPX networks known to the system. The completed IPX routing table is displayed in the The IPX/SPX Route Table Applet.

**NOTE:** Not available for Wellfleet and Cisco software versions under 10.3.

Network	Delay	Throughput	COST
00000003	200	10000000	20
00000004	200	10000000	20
00000007	200	10000000	20
2D6C140A	0	0	0

The NLSP Learned Networks Table column headings include:

Heading	Definition
<b>Network</b>	The IPX network number.
<b>Delay</b>	The time in microseconds to reach a destination system.
<b>Throughput</b>	The transmit/receive speed of the interface in bits/sec.
<b>COST</b>	The total path to reach the destination. This is used to determine the best route to a destination.


### Using the NLSP Learned Networks Table applet

To start the NLSP Learned Networks Table applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **IPX > NLSP > Learned Networks**. From the application view, right-click the IPX icon in the Boxmap and choose **NLSP > Learned Networks**.
3. Choose the applet parameters and click OK. The applet opens and information will appear in the window.

#### Other buttons

In addition to the global toolbar buttons, the NLSP Learned Networks Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## **AppleTalk tools**

### **AppleTalk Tools: Overview**

The AppleTalk tools provide full information about the AppleTalk protocol on your system.

Available tools are:

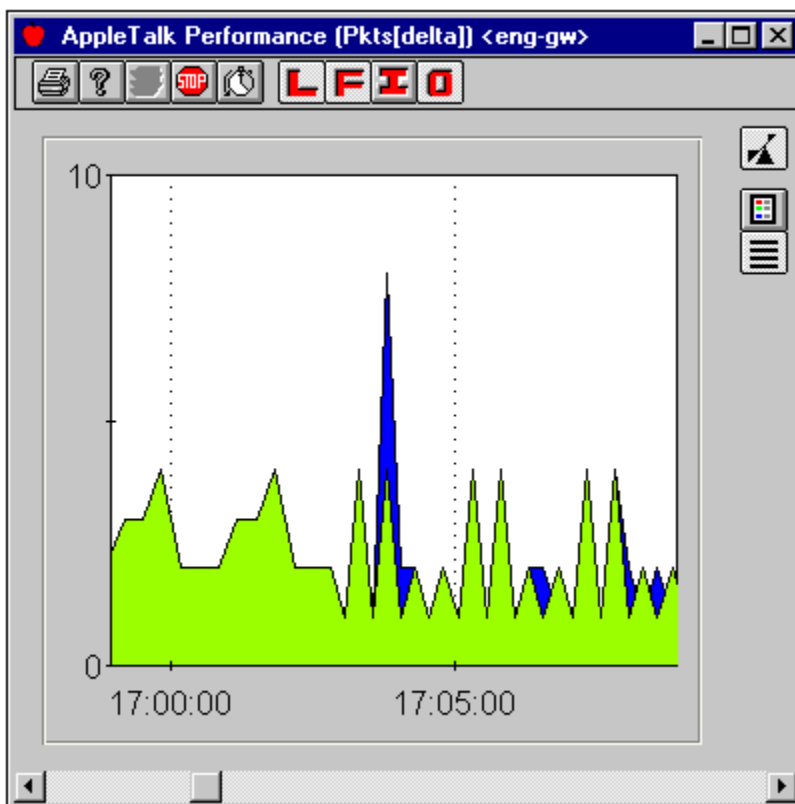
- **The AppleTalk Performance applet**  
Provides performance information for AppleTalk devices.
- **The AppleTalk Route Table applet**  
Provides route table information for AppleTalk devices, such as Next Hop network number and route status.
- **The AppleTalk Translation Table applet**  
Provides a logical-to-physical mapping for all routes.

### The AppleTalk Performance applet

The **AppleTalk Performance** applet monitors Input , Forward , Local , and Output packet statistics for the AppleTalk protocol . Data may be displayed either in Delta , which is the default setting, or Per Second format. Data is updated on the screen based on the polling interval selected.

The graph can be displayed in Line or Mountain style.

**NOTE:** For Wellfleet 7.XX version software and above, the performance is obtained from the Interface menu.



## Using the AppleTalk Performance applet






### To start the AppleTalk Performance applet:




1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **AppleTalk > Performance**. From the logical view, right-click on the Apple Talk icon in the Boxmap and select **Performance**.
3. Choose the applet parameters and click **OK**. The applet opens and Apple Talk performance statistics will begin to appear in the window, based on the polling interval .

Click the mouse on any point in the graph to view the precise statistics at that point.

### Other buttons

In addition to the global toolbar buttons, the AppleTalk Performance applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coded protocols, such as seen below. <div data-bbox="504 1375 749 1497">  </div>
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.
	<b>[Show/Hide Local Graph] button</b> Show and hide the graph for Local packet statistics.

Button	Description
	<b>[Show/Hide Forward Graph] button</b> Show and hide the graph for Forward packet statistics.
	<b>[Show/Hide Input Graph] button</b> Show and hide the graph for Input packet statistics.
	<b>[Show/Hide Output Graph] button</b> Show and hide the graph for Output packet statistics.

### The AppleTalk Route Table applet

The **AppleTalk RouteTable** applet provides a list of known AppleTalk routes for the current router.

**NOTE:** Not available for Cisco Routers

The AppleTalk Route Table Applet includes the following fields:

Route Table Field	Description
<b>Network Start</b>	The beginning AppleTalk network number for this route.
<b>Network End</b>	The ending AppleTalk network number for this route.
<b>State</b>	The current state of the route. See possible values below.
<b>Interface</b>	The interface number of the link to the next router.
<b>Distance</b>	The number of routers a packet must pass through to reach its destination.
<b>Next Hop Net</b>	The network number of the next hop to this route.
<b>Type</b>	The type of network over which this route points. See possible values below.

**State Field**

The State field indicates the current status of this route. The table below lists the possible values for this field:

State	Description
Good	The route to this destination is valid
Suspect	The router is not sure if this route is valid
Going Bad	The route is currently not valid
Bad	The route is currently not valid

**Type Field**

The Type field indicates the type of network to which this route points. The table below lists the possible values for this field.

Type	Description
other	Unknown line type
AppleTalk	Route runs on a standard non serial media
serial-ppp	Route runs on a standard PPP serial media
serial-nonstandard	Route runs on a nonstandard serial media

**Using the AppleTalk Route Table applet****To start the AppleTalk RouteTable applet:**



1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **AppleTalk > Route Table**. From the logical view, right-click on the Apple Talk icon in the Boxmap and select **Route Table**.
3. Choose the applet parameters and click OK. The applet opens and route table information will begin to appear in the window.

Network Performance

Depending on the number of entries, it may take some time to finish building the table.

Other buttons

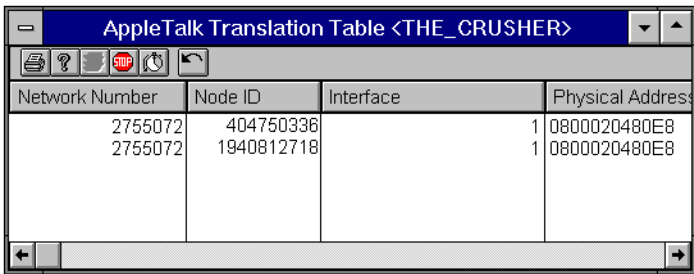
In addition to the global toolbar buttons, the AppleTalk Route Table applet has two specialized buttons on the right hand side of the toolbar:

Button	Description
	<b>[Rescan Table] button</b> When the Stop Default is set in the System Options Configuration dialog box, polling is stopped (the Stop button on the toolbar is grayed out). This button rescans the table.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

The AppleTalk Translation Table applet

The **AppleTalk Translation Table** applet gives a logical-to-physical mapping of all destination routes for the current router for a given (non-serial) media.

**NOTE:** Not available for Cisco Routers



Network Number	Node ID	Interface	Physical Address
2755072	404750336	1	0800020480E8
2755072	1940812718	1	0800020480E8

The following information is displayed in the AppleTalk Translation Table window:

Translation Table Field	Description
Network Number	The AppleTalk network number of this router.
Node ID	The AppleTalk node number of this router.
Interface	The interface where this router is reachable from.
Physical Address	The Media Access Address of this router.


## Using the AppleTalk Translation Table applet

To start the AppleTalk Translation Table applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **AppleTalk > Translation Table**. From the logical view, right-click on the Apple Talk icon in the Boxmap and select **Translation Table**.
3. Choose the applet parameters and click OK. The applet opens and translation table information will appear in the window.

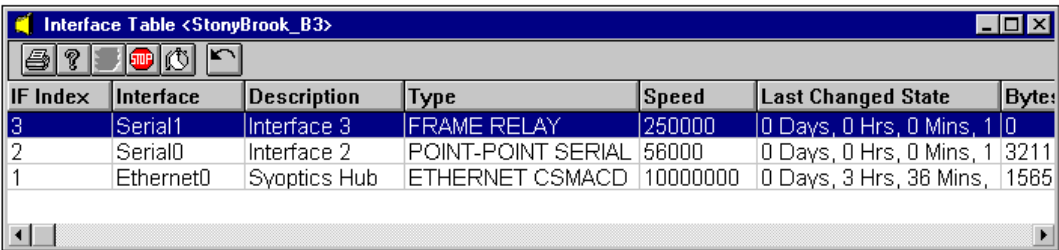
### Other buttons

In addition to the global toolbar buttons the AppleTalk Address Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

# Interface Table applet

The **Interface Table** applet displays a list of all the interfaces available on the device along with related information.



IF Index	Interface	Description	Type	Speed	Last Changed State	Bytes
3	Serial1	Interface 3	FRAME RELAY	250000	0 Days, 0 Hrs, 0 Mins, 1 0	
2	Serial0	Interface 2	POINT-POINT SERIAL	56000	0 Days, 0 Hrs, 0 Mins, 1 3211	
1	Ethernet0	Syoptics Hub	ETHERNET CSMACD	10000000	0 Days, 3 Hrs, 36 Mins,	1565

The Interface Table Applet includes the following fields:

Field	Description
If Index	Interface Index which is usually the Interface Number.
Interface	The interface number for this interface. This number can be used to correlate with other applets (e.g. IP Route Table, IP Address Table, IP Translation Table, etc.).
Description	The name of the interface. This information is configured on the device.
Type	The type of interface (see table of available interface types below).
Speed	The available bandwidth of this interface.
Last Changed State	The amount of time since the interface entered its current state.
Bytes Out	The number of bytes transmitted.
Bytes In	The number of bytes received.
Discards Out	The number of outbound packets discarded due to resource limitations.

Field	Description
<b>Discards In</b>	The number of inbound packets discarded due to resource limitations.
<b>Errors In</b>	The number of inbound packets received with errors that forced them to be ignored.
<b>UNK Prot</b>	The number of packets received containing an unknown protocol field but having a good CRC.
<b>MTU</b>	The size of the largest datagram which can be sent/received on the interface.
<b>MAC Address</b>	The MAC Address of the interface.
<b>Admin</b>	The administrative status of the interface. An interface can be either UP (operational) or DOWN (not operational).
<b>Oper</b>	The operational status of the interface. An interface can be either UP (operational) or DOWN (not operational).

### Type Field

The Type field indicates the type of interfaces, distinguished according to the physical/link protocol, running in the protocol stack. The table below contains a list of the possible values for this field:

Type	Description
<b>Other</b>	Anything not in this list
<b>regular1822</b>	obsolete
<b>hdh1822</b>	obsolete
<b>ddn-x25</b>	department of defense X25
<b>rfe877-x25</b>	RFC approved multi vendor CCITT X25
<b>ethernet-csmacd</b>	DIX consortium Ethernet II
<b>iso88023-csmacd</b>	802.3 Ethernet

## Network Performance

---

Type	Description
<b>iso88024-tokenBus</b>	Arcnet
<b>iso88025-tokenRing</b>	IBM token ring
<b>iso88026-man</b>	Metropolitan Area Network
<b>starLan-ATT 1 MBit ethernet</b>	ATT Ethernet
<b>proteon-10Mbit</b>	Pronet 10 (token ring)
<b>proteon-80Mbit</b>	Pronet 80
<b>hyperchannel</b>	Broadband LAN
<b>fddi</b>	standard fiber distributed data interface
<b>lapb</b>	HDLC with LAPB extensions
<b>sdlc</b>	IBM Synchronous Data Link Control
<b>ds1</b>	T-1
<b>e1</b>	European equivalent of T-1
<b>basicISDN</b>	Basic Rate Interface
<b>primaryISDN</b>	Primary Rate Interface
<b>propPointToPointSerial</b>	proprietary point to point protocol.
<b>Ppp</b>	RFC Point to Point Protocol
<b>softwareLoopback</b>	Software agent loopback
<b>eon</b>	CLNP over IP [11]
<b>ethernet-3Mbit</b>	Proprietary Ethernet
<b>nsip</b>	XNS over IP
<b>slip</b>	IP over serial line protocol
<b>ultra</b>	ULTRA technologies
<b>ds3</b>	T-3

Type	Description
sip	SMDS
frame-relay	Frame Bearer Service

## Using the Interface Table applet

To start the Interface Table applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Interface > Interface Table**. From the application view, right-click on the Interface icon in the Boxmap and select **Interface Table**.
3. Choose the applet parameters and click OK. The applet opens and Interface Table information will begin to appear in the window.

### Frame Relay options

If the device has a Frame Relay interface, you can access the Frame Relay Virtual Circuit Utilization and Frame Relay Virtual Circuit Statistics applets from within the Interface Table.


To do so:

1. Right-click on the table row that contains a Frame Relay device.
2. Select **VC Utilization** or **VC Statistics** to launch the application. Choose the applet parameters and click OK.

The Interface Table applet will remain open after launching the Frame Relay applets.

### Other buttons

In addition to the global toolbar buttons, the Interface Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## **Individual interface tools**

### **Individual Interface tools: Overview**

The Individual Interface tools provide information about particular interfaces on a device. Interfaces are accessed via interface icons, of which there are two types, one for serial interfaces and one for all other types.

#### **Available Interface tools are:**

- **The Description applet**  
Adds a line of descriptive text to the Interface icon.
- **The Utilization applet**  
Shows line utilization for a device as a percentage of bandwidth.
- **The Virtual Circuit Utilization applet**  
Displays CIR information for each DLCI (Data Link Connection Identifier) configured on an interface.
- **The Output Queue Length applet**  
Displays the current, maximum and average values of the output queue in number of packets.
- **The X.25 Circuits applet**  
Displays X.25 information on an existing, established virtual circuit. Displayed information includes status, number of resets, in and out octets, in and out PDUs, etc.
- **The X.25 Statistics applet**  
Displays the values of the monitored X.25 statistics for a particular interface. Displayed statistics include number of calls and call refusals, number of reset requests, number of out call attempts and failures, etc.

#### **Cisco Specific Tools**

There are also Interface tools that work only with Cisco devices. Available tools are:

- **The Utilization applet - Cisco specific**  
Displays line utilization for a device as a percentage of bandwidth.

- **The Utilization Distribution applet - Cisco specific**  
Displays total line utilization divided up by protocol.
- **The Clear Interface applet - Cisco specific**  
Clears all information on the selected Cisco interface.
- **The Mean Packet Size applet - Cisco specific**  
Displays average current Input and Output packet size for the selected interface, as well as the historical average.
- **The Mean Packet Size Distribution applet - Cisco specific**  
Displays the average packet size in terms of specific protocols.

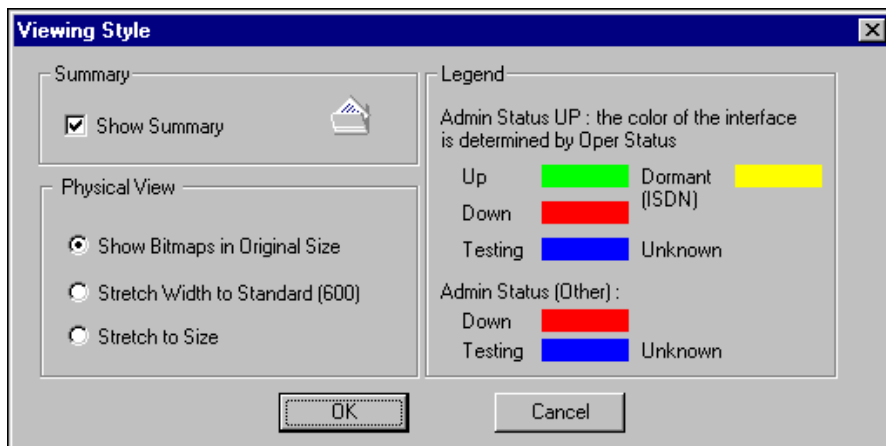
### 3Com Specific Tools

There are also Interface tools that work only with 3Com devices. Available tools are:

- **The Ethernet Statistics applet - 3Com specific**  
Displays, per interface, the number of errors that have occurred in the last polling period. Displayed errors include alignment errors, single, multiple, late and excessive collisions, etc.
- **The TokenRing Statistics applet - 3Com specific**  
Displays, per interface, the number of errors that have occurred in the last polling period. Displayed errors include line errors, burst errors, token errors, number of beacons transmitted, etc.

### Interface icon status colors

The color-coded background of the interface icon displays the interface status. This background allows the user to identify which interfaces are operationally up/down, or administratively down at a glance. Press on the [Style] button in the Boxmap toolbar to view the interface color Legend.



The Up Operational Status is defined as:

Up - **Green**

Down - **Red**

Testing - **Blue**

Dormant - **Yellow**

Unknown - **Gray**

The Administrative Status of the individual Interface Icon can be:

Up - **Green**

Down - **Dark Red**

Testing - **Blue**

Unknown - **Gray**

## The Description applet

The **Description** applet allows you to add a line of descriptive text for each interface. The text is displayed as the third line of each interface.

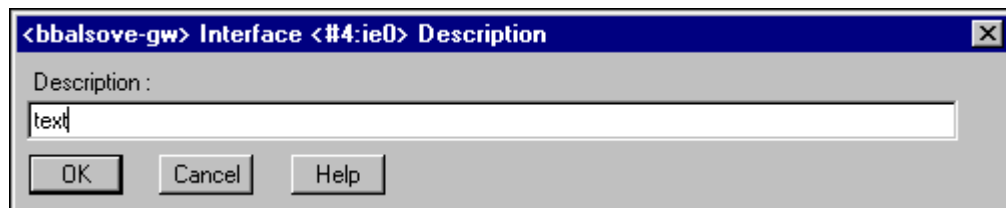
This allows you to more easily identify key interfaces on devices that may have a very large number of interfaces.

---

## Using the Description applet

### To add descriptive text to an interface:

1. In the Boxmap application view, right-click on an individual interface icon and choose Description. In the physical view, right-click on a particular interface and choose Description. The Description window opens.



2. Enter up to 40 characters to describe the interface and click [OK].

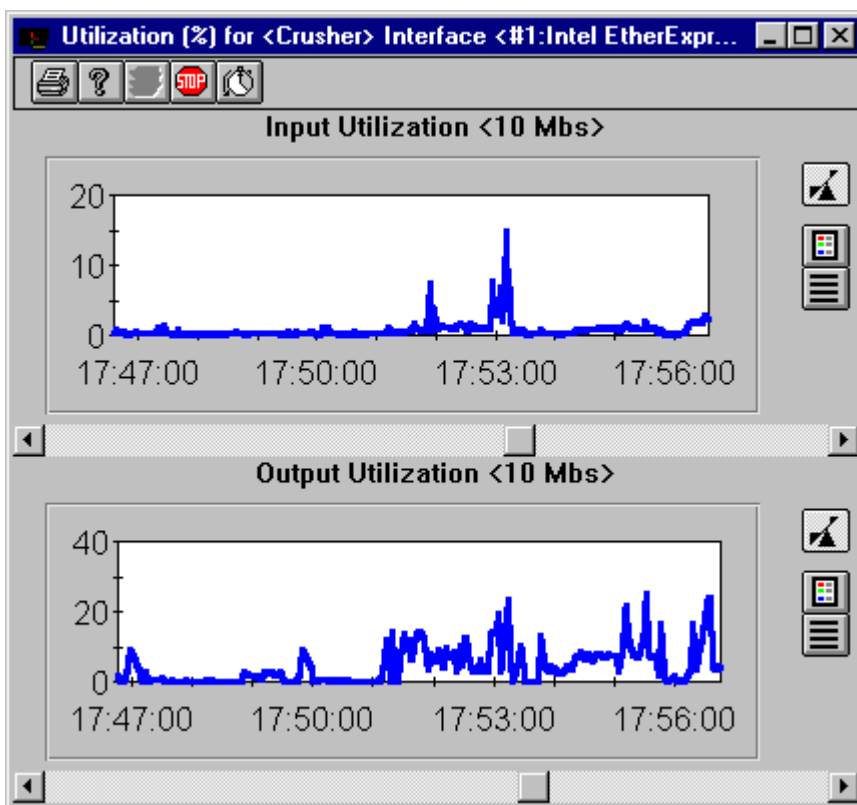
After the operation is completed, the interface will re-display with the descriptive text showing.

## The Utilization applet

The **Utilization** applet shows line utilization for a device as a percentage of bandwidth. The Applet shows Input Utilization in the top graph and Output Utilization in the bottom graph.

The data is updated on screen based on the polling interval entered in the applet parameters dialog box for the applet.

**NOTE:** Cisco has some variations, as described in The Utilization Applet: Cisco Specific.






### Using the Utilization applet

1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click on an individual interface icon and select **Utilization**. From the physical view, right-click on a particular interface and choose **Utilization**.
3. Choose the applet parameters and click OK. The applet opens and utilization statistics will begin to appear in the window, based on the polling interval.

Click the mouse on any point in the graph to view the precise statistics at that point.

### Other buttons

In addition to the global toolbar buttons, the Utilization applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the color-coded key to the graph.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## The Virtual Circuit Utilization applet

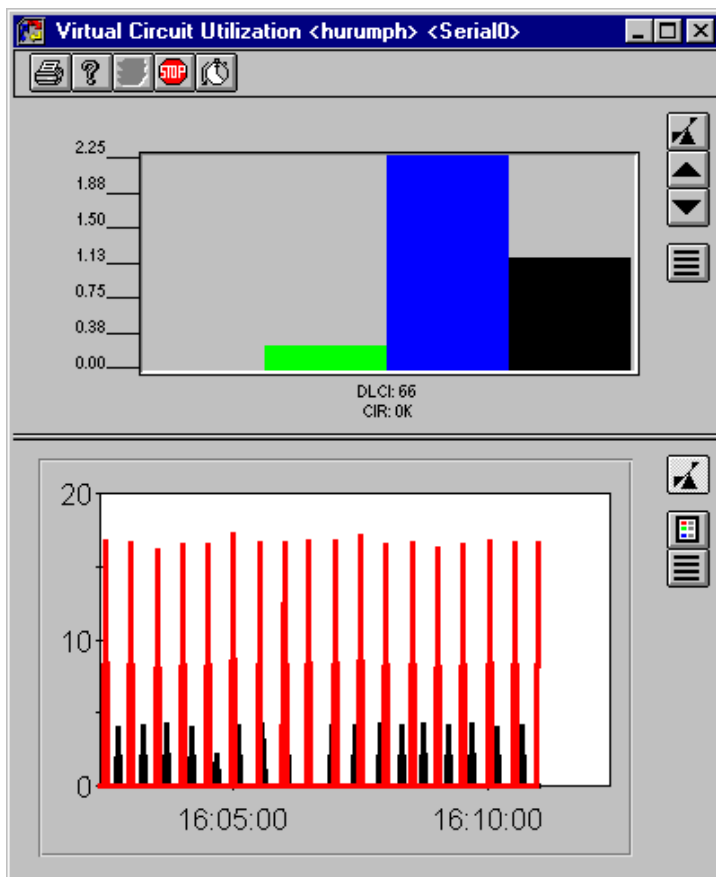
The Virtual Circuit Utilization applet displays CIR information for each DLCI (Data Link Connection Identifier) configured on this interface. Utilization data is displayed as a percentage of CIR.

Each DLCI is displayed in a separate gauge.

Each gauge in the upper pane shows four bar graphs. From left to right, they correspond to:

- **Bar 1** - Input Utilization (as a percentage of CIR). The real-time, on-going input utilization for the DLCI.
- **Bar 2** - Average Input Utilization. The average utilization over the course of the monitoring period.
- **Bar 3** - Output CIR Utilization. The real-time, on-going output utilization for the DLCI.
- **Bar 4** - Average Output Utilization. The average utilization over the course of the monitoring period.

The bottom pane displays the real-time input and output utilization of each configured DLCI as a line graph. This Applet is very useful in determining which DLCIs are generating the most traffic.



### Using the Virtual Circuit Utilization applet

To start the Virtual Circuit Utilization applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click on an individual interface icon and select **VC Utilization**. From the physical view, right-click on a particular interface and choose **VC Utilization**.




**NOTE:** The availability of this applet depends on the protocol running on the device interface.

3. Choose the applet parameters and click OK. The applet opens and Virtual Circuit utilization information will begin to appear in the window, based on the polling interval.

Click the mouse on any point in the graph to view the precise statistics at that point.

### Other buttons

In addition to the global toolbar buttons, the Virtual Circuit Utilization applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the color-coded key to the graph.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

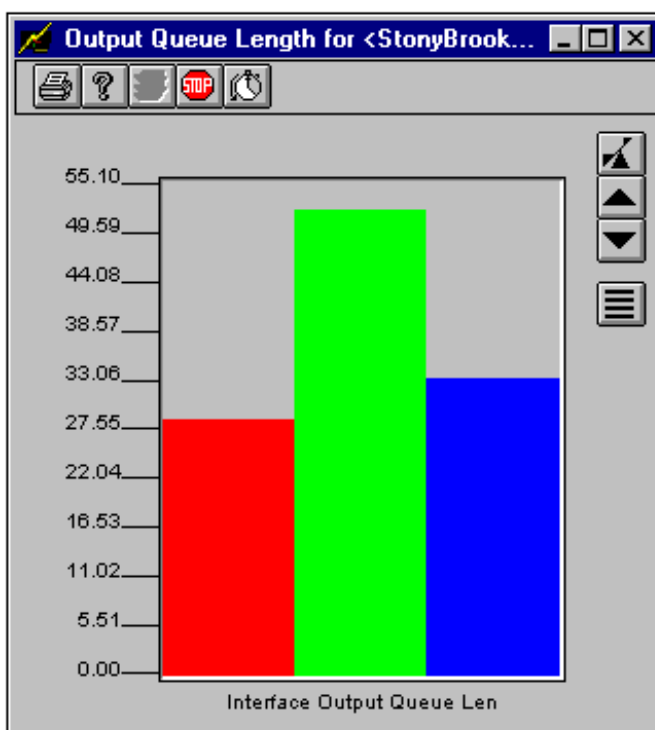
### The Output Queue Length applet

The **Output Queue Length** applet displays the current, maximum and average values of the output queue in number of packets.

The graph contains three bars:

- **Red bar:** Current queue length, in number of packets.
- **Green bar:** Maximum queue length reached during the monitoring period.
- **Blue bar:** Average queue length during the monitoring period.

On serial interfaces with high utilization, the router is forced to buffer packets in memory until they can be sent out by the interface. Most routers buffer between 75-100 packets on an interface. When the maximum value is reached, they begin to drop packets and rely on the higher level protocols to recover. Routers that have high serial line utilization typically experience a queue length of up to 10 packets.



---

## Using the Output Queue Length applet



### To start the Output Queue Length applet:

1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select Output Queue Length. From the physical view, right-click on a particular interface and choose Output Queue Length.
3. Choose the applet parameters and click OK. The applet opens and Output Queue Length information will begin to appear in the window, based on the polling interval.

Hold the mouse pointer on any point in the graph to view the precise statistics.

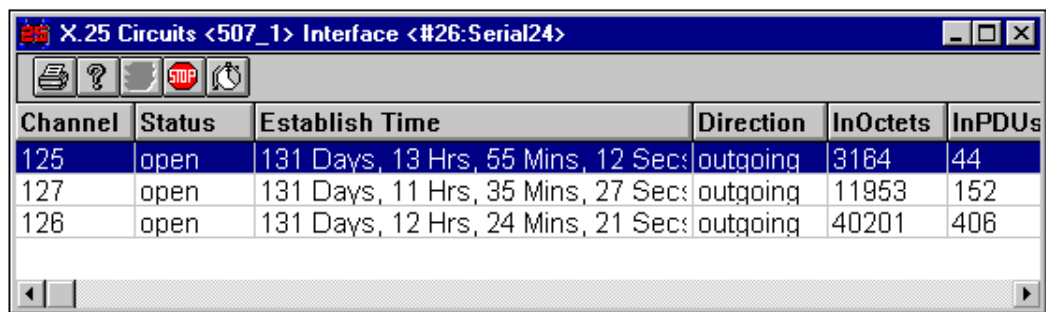
### Other buttons

In addition to the global toolbar buttons, the Virtual Circuit Utilization applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

The X.25 Circuits applet

The **X.25 Circuits** applet displays X.25 information on an existing, established virtual circuit. Virtual circuits that are not established are *not* displayed in this table. The detailed information about the circuit includes the Calling and Called DTE address - the source and destination of the call. This consolidated information is useful in determining where the X.25 connections are being established and what routes they are taking.



The screenshot shows a window titled "X.25 Circuits <507\_1> Interface <#26:Serial24>". It contains a table with the following data:

Channel	Status	Establish Time	Direction	InOctets	InPDUs
125	open	131 Days, 13 Hrs, 55 Mins, 12 Secs	outgoing	3184	44
127	open	131 Days, 11 Hrs, 35 Mins, 27 Secs	outgoing	11953	152
128	open	131 Days, 12 Hrs, 24 Mins, 21 Secs	outgoing	40201	408

The following information is displayed in the X.25 Circuits window:

Heading	Definition
Channel	The channel number for this circuit.
Status	This object reports the current status of the circuit. See Status Table below for possible values.
Establish Time	The amount of time the circuit has been up.
Direction	The direction of the call that established this circuit. [Possible values are incoming (1), outgoing (2), and PVC (3)]
In Octets	The number of octets of user data delivered to the upper layer.
In PDUs	The number of PDUs received for this circuit.
In Remote InitResets	The number of Resets received for this circuit with cause code of DTE initiated.

Heading	Definition
<b>In Provide Init Resets</b>	The number of Resets received for this circuit with cause code other than DTE initiated.
<b>In Interrupts</b>	The number of interrupt packets received for this circuit.
<b>Out Octets</b>	The number of octets of user data sent for this circuit.
<b>Out PDUs</b>	The number of PDUs sent for this circuit.
<b>Out Interrupts</b>	The number of interrupt packets sent on this circuit.
<b>Data Rxmt Time Outs</b>	The number of times the T25 data retransmission times expired for this circuit.
<b>Reset Time Outs</b>	The number of times the T22 reset times expired for this circuit.
<b>Interrupt Time Outs</b>	The number of times the T26 Interrupt timer expired for this circuit.
<b>Call ParamId</b>	This identifies the instance of the X.25CallParmIndex for the circuit.
<b>Called Dte Address</b>	The called X.121 address
<b>Calling Dte Address</b>	The calling address from the call indication packet.
<b>Orig Called Address</b>	The address in the call Redirection or Call Deflection Notification facility.
<b>Circuit Description</b>	A descriptive string associated with this circuit.

Status Values for the X.25 Circuits Applet table:

Possible Status Values
<b>invalid (1)</b>
<b>closed (2)</b>
<b>calling (3)</b>
<b>open (4)</b>

Possible Status Values
clearing (5)
pvc (6)
pvcResetting (7)
startClear (8)
startPvcResetting (9)
other (10)

## Using the X.25 Circuits applet

To start the X.25 Circuits applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the application view, right-click on an individual interface icon and select **X.25 Circuits**. From the physical view, right-click on a particular interface and choose **X.25 Circuits**.
3. The applet opens and X.25 Circuit information will be displayed in the window.

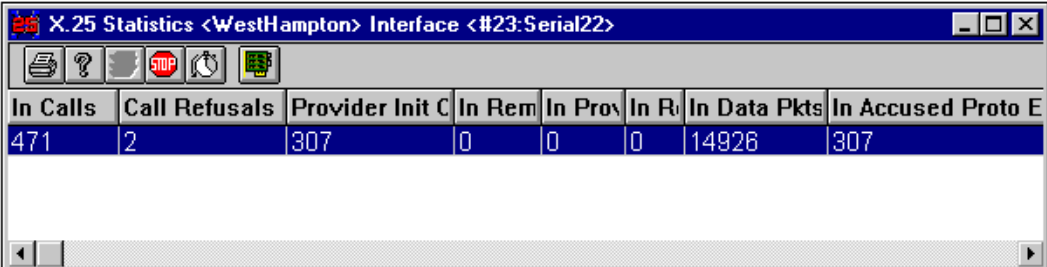
The X.25 Circuits applet uses the global toolbar buttons .

The X.25 Circuits applet can also be accessed from the X.25 Administrative Table applet or the X.25 Operational Table applet.

## The X.25 Statistics applet

The **X.25 Statistics** Applet displays the values of the monitored X.25 statistics for a particular interface. Information presented is the aggregated totals for all virtual circuits configured for the interface.

This information is useful in detecting a problem on a particular interface on the router. More granular information about the individual virtual circuits configured for the interface is available from the X.25 Circuits applet.



In Calls	Call Refusals	Provider Init C	In Rem	In Prov	In R	In Data Pkts	In Accused Proto E
471	2	307	0	0	0	14926	307

The following information is displayed in the X.25 Statistics window:

Heading	Definition
In Calls	The number of incoming calls received.
Call Refusals	The number of incoming calls refused.
Provider Init Clears	The number of clear requests with a cause code other than DTE initiated.
In Remote Init Resets	The number of reset requests received with cause code DTE initiated.
In Provider Init Resets	The number of reset requests received with cause code other than DTE initiated.
In Restarts	The number of remotely initiated (including provider initiated) restarts experienced.
In Data Pkts	The number of data packets received.

## Network Performance

Heading	Definition
<b>In Accused of Proto Errs</b>	The number of packets received containing a procedure error cause code. These include clear, reset, restart or diagnostic packets.
<b>In Interrupts</b>	The number of interrupt packets received.
<b>Out Call Attempts</b>	The number of call attempts.
<b>Out Call Fail</b>	The number of call attempts which failed.
<b>Out Interrupts</b>	The number of interrupt packets sent.
<b>Out Data Pkts</b>	The number of data packets sent.
<b>Outgoing Circ</b>	The number of active outgoing circuits.
<b>Incoming Circ</b>	The number of active incoming circuits.
<b>Two Way Circ</b>	The number of active two-way circuits.
<b>Restart TimeOuts</b>	The number of times the T20 restart timer expired.
<b>Call TimeOuts</b>	The number of times the T21 call times expired.
<b>Reset TimeOuts</b>	The number of times the T22 reset timer expired.
<b>Clear TimeOuts</b>	The number of times the T23 clear timer expired.
<b>Data Rxmt TimeOuts</b>	The number of times the T25 data timer expired.
<b>Interrupt TimeOuts</b>	The number of times the T26 interrupt timer expired.
<b>Retry Cnt Exceededs</b>	The number of times a retry counter was exhausted.
<b>Clear Cnt Exceededs</b>	The number of times the R23 clear count was exceeded.

## Using the X.25 Statistics applet

To start the X.25 Statistics applet:

1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select X.25 Statistics. From the physical view, right-click on a particular

interface and choose X.25 Statistics.

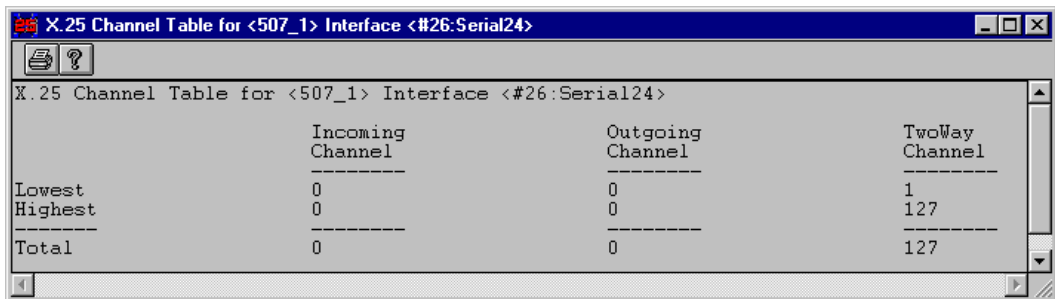
3. The applet opens and X.25 Statistics information will be displayed in the window.

The X.25 Statistics applet can also be accessed from the X.25 Administrative Table applet or the X.25 Operational Table applet.

### The Channel Table

You can also launch the Channel Table. The Channel Table displays the percent utilization of the virtual circuits defined for each category (Incoming, Outgoing and Two Way). The lowest, highest and total values are displayed in the text.

To launch the table, click the [Channel Table] button .



	Incoming Channel	Outgoing Channel	TwoWay Channel
Lowest	0	0	1
Highest	0	0	127
Total	0	0	127

The X.25 Statistics applet uses the global toolbar buttons.

## **Tools for Cisco devices**

### **Cisco Specific Interface tools: Overview**

There are Interface tools that work only with Cisco devices. Available tools are:

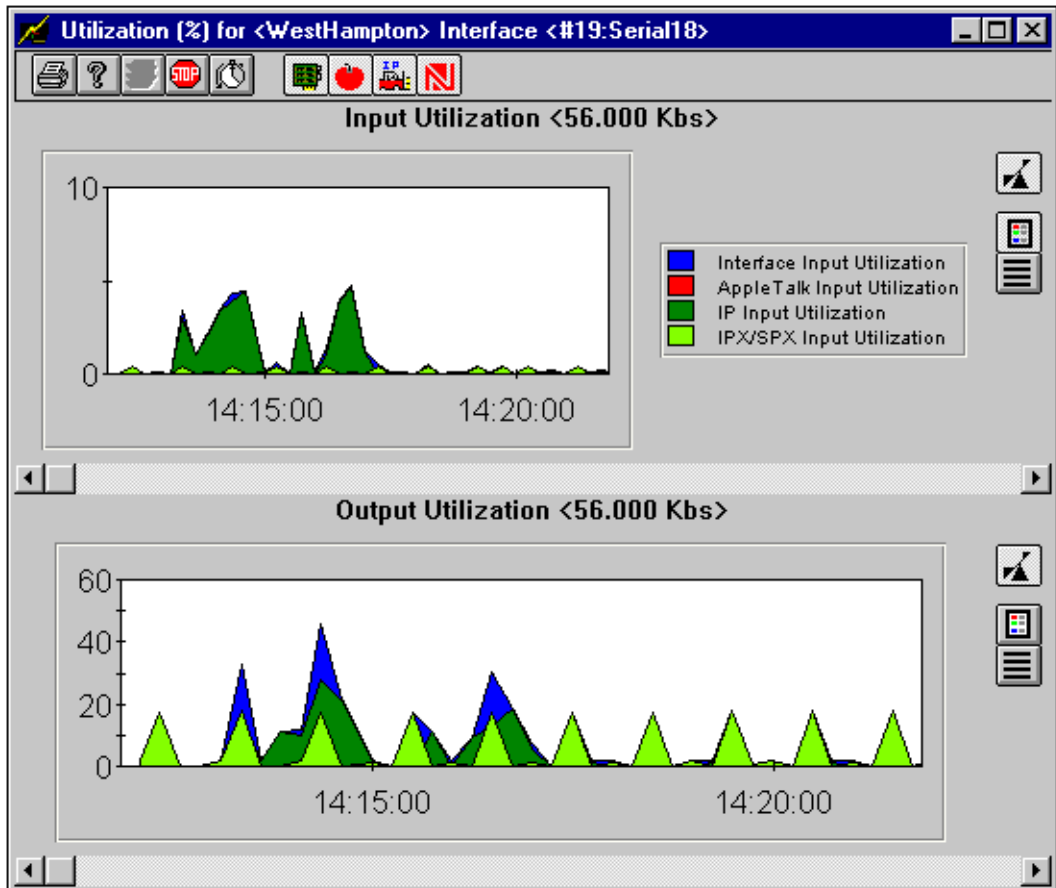
- **The Utilization applet - Cisco specific**  
Displays line utilization for a device as a percentage of bandwidth.
- **The Utilization Distribution applet - Cisco specific**  
Displays total line utilization divided up by protocol.
- **The Clear Interface applet - Cisco specific**  
Clears all information on the selected Cisco interface.
- **The Mean Packet Size applet - Cisco specific**  
Displays average current Input and Output packet size for the selected interface, as well as the historical average.
- **The Mean Packet Size Distribution applet - Cisco specific**  
Displays the average packet size in terms of specific protocols.

### **The Utilization Applet- Cisco Specific**

The **Utilization** applet shows line utilization for a device as a percentage of bandwidth. The applet shows Input Utilization in the top graph and Output Utilization in the bottom graph. Each Graph shows up to four lines, depending on the available protocols:

- AppleTalk Utilization
- IP Utilization
- Novell Utilization (IPX/SPX)
- Total Interface Utilization

The data is updated on screen based on the polling interval.



### Reading the chart

Consider the bottom graph, Output Utilization. Total line bandwidth is listed at 56.000 Kbs. The blue mountain peaks show the total interface utilization as a *percentage* of total bandwidth. At its highest point, the line is at about 50% utilization (i.e., 50% of the 56 Kbs).

This is broken down by color-coded protocol lines. The dark green, for IP, is about 30% of total utilization, with IPX at about 20% (at the highest peak). AppleTalk, while configured on this device (as shown by the AppleTalk icon), is not being used.

To more clearly view a particular protocol graph, you can turn protocols on and off using the [Show/Hide] protocol buttons.

**NOTE:** For Cisco Routers with Version 9.0 or less, it is not possible to display individual protocol utilization statistics. Only total Input and Output Utilization are monitored.

### Using the Cisco Specific Utilization applet





#### To start the Utilization applet:




1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select Utilization. From the physical view, right-click on a particular interface and choose Utilization.
3. Choose the applet parameters and click OK. The applet opens and utilization statistics will begin to appear in the window, based on the polling interval.

Click the mouse on any point in the graph to view the precise statistics at that point.

#### Other buttons

In addition to the global toolbar buttons , the Utilization applet has the following specialized buttons:

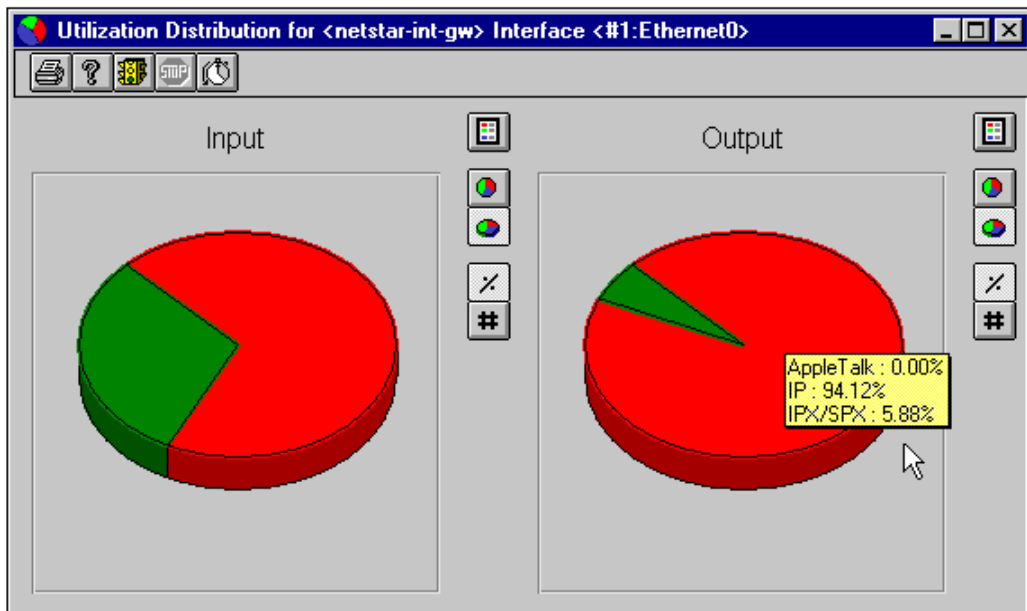
Button	Description
	<b>[Show/Hide Interface Graph] button</b> Toggles the Interface graph line on and off.
	<b>[Show/Hide AppleTalk Graph] button</b> Toggles the AppleTalk graph line on and off.
	<b>[Show/Hide IP Graph] button</b> Toggles the IP graph line on and off.
	<b>[Show/Hide IPX/SPX Graph] button</b> Toggles the IPS/SPX graph line on and off.

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the color-coded key to the graphs.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the graph for easier reading.

### The Utilization Distribution Applet - Cisco Specific

The **Utilization Distribution** applet displays total line utilization divided up by protocol. Each protocol on the device is displayed as part of a pie chart. Input and output utilization are displayed separately.

**NOTE:** Applet only available for Cisco routers using software v 9.1 and above.



Click the left mouse button on the pie chart to see the current values for each protocol, as shown above.

### Reading the chart

Two different sets of numbers are available from each Utilization Distribution pie chart: percentages and integer values (toggled by clicking the [Show Values/Show Percent] button.

Viewing **percentages** will show you the breakdown of current utilization by protocol. For example, in the Output chart above, utilization shows IP at 94.12% and IPX at 5.88%. This means that of the *current* utilization, 94.12% is IP and 5.88% is IPX. *This does not mean that total line utilization is at 100%*. (For total line utilization, see the Utilization applet.)

Viewing **values** will show the numbers that are used in calculating the percentages. For the Output chart, viewing values in this case showed IP at 15.0 and IPX at 0.9. These values are portions of maximum possible utilization (equal to 100). Therefore, the IP utilization is 15 out of a total *current* utilization of 15.9 (IP + IPX) and a maximum utilization of 100. These figures are easily converted to utilization percentage. In this case, IP is 15% of total maximum bandwidth, IPX .9 %, and the total utilization is 15.9%.

(If you calculate the numbers yourself, there will be a slight discrepancy due to rounding of the displayed numbers.)

## Using the Utilization Distribution applet - Cisco Specific





### To start the Utilization Distribution applet:

1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select Utilization Distribution. From the physical view, right-click on a particular interface and choose Utilization Distribution.
3. Choose the applet parameters and click OK. The applet opens and utilization pie charts will appear in the window, based on the polling interval. The pie charts will update for each polling interval.

Click the mouse on any point in the graph to view the precise statistics.

### Other buttons

There are three other button functions available for the pie charts.

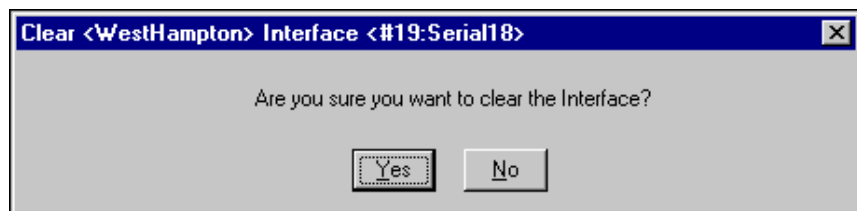
Button	Description
	<b>[Show/Hide Pie Legend] button</b> Displays the key to the color-coded protocols, such as seen below: 
	<b>[Show/Hide 3D Effect] buttons</b> Toggles the pie chart between a 2D and 3D image.
	<b>The [Show Values/Show Percent] buttons</b> Toggle the pie charts between displaying information as a integer value (e.g., 10 alerts sent) or as a percentage (e.g. 10% of all alerts sent).

## The Clear Interface Applet - Cisco Specific

The Clear Interface applet will clear all information on the selected Cisco interface.

### To clear an interface:

1. Select the **Clear Interface** applet from the pull-down menu. The following sample message is received:



2. Click the [Yes] button to clear the current counters. The counters will then be refreshed.

### The Mean Packet Size Applet - Cisco Specific

The Mean Packet Size applet displays average current Input and Output packet size for the selected interface, as well as the historical average. Data is displayed as Octets per packet.

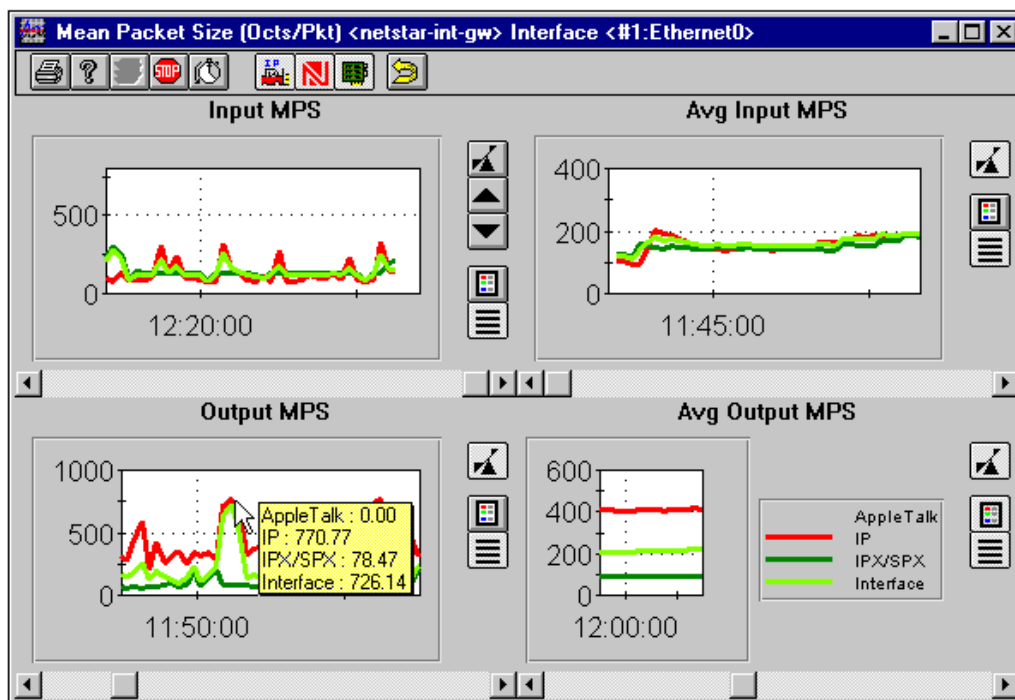
The graphs on the left display current information based on the most recent polling interval. The graphs on the right display average packet size for the entire monitoring period.

Each Graph shows up to four lines, depending on available protocols. They are:

- AppleTalk packet size
- IP packet size
- Novell packet size (IPX/SPX)
- Total Interface packet size

The data is updated on screen based on the polling interval.

**NOTE:** This applet is only available for Cisco routers using software version 9.1 and above.



Click the mouse on any point in the graph, as shown above, to view the values for the packet statistics at that point.

### Reading the graph

The graph displays packet information as Octets per second. For example, in the Output graph (lower left), clicking on the high-point in the graph shows IP at 770.77, which is equal to an average of 770.77 Octets in each packet. IPX is 78.47 Octets per packet. The Interface reading is the average Octets per packet for the entire interface. This does not necessarily equal the average of the two protocols ( $IP + IPX / 2$ ) because, for example, there may be far more packets flowing via IP than IPX during a burst of data (as is the case here). Therefore, the average packet size for the interface may be closer to one protocol than to the other.

As would be expected, when you look at the historical averages on the right side, the Interface figure is very close to midway between IP and IPX, because over time the effects of data bursts are lessened.

## Using the Mean Packet Size applet









### To start the Mean Packet Size applet:

1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select Mean Packet Size. From the physical view, right-click on a particular interface and choose Mean Packet Size.
3. Choose the applet parameters and click OK. The applet opens and packet size information will begin to be graphed in the window, based on the polling interval.

Click the mouse on any point in the graph to view the precise statistics at that point.

### Other buttons

In addition to the global toolbar buttons, the Mean Packet Size applet has the following specialized buttons:

Button	Description
	<b>[Show/Hide Interface Graph] button</b> Toggles the Interface graph line on and off.
	<b>[Show/Hide AppleTalk Graph] button</b> Toggles the AppleTalk graph line on and off.
	<b>[Show/Hide IP Graph] button</b> Toggles the IP graph line on and off.
	<b>[Show/Hide IPX/SPX Graph] button</b> Toggles the IPS/SPX graph line on and off.
	<b>[Reset Average Mean Packet Size] button</b> Resets the historical average mean packet size to zero, allowing you to gather new data from that point forward. After clicking, a message will prompt you to confirm your selection.
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the color-coded key to the graphs.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the graph for easier reading.

## The Mean Packet Size Distribution applet - Cisco Specific

The **Mean Packet Size Distribution** applet displays the average packet size in terms of specific protocols. Each pie chart takes the average packet size information and divides it up based on what percentage of the packets are moving via each protocol.

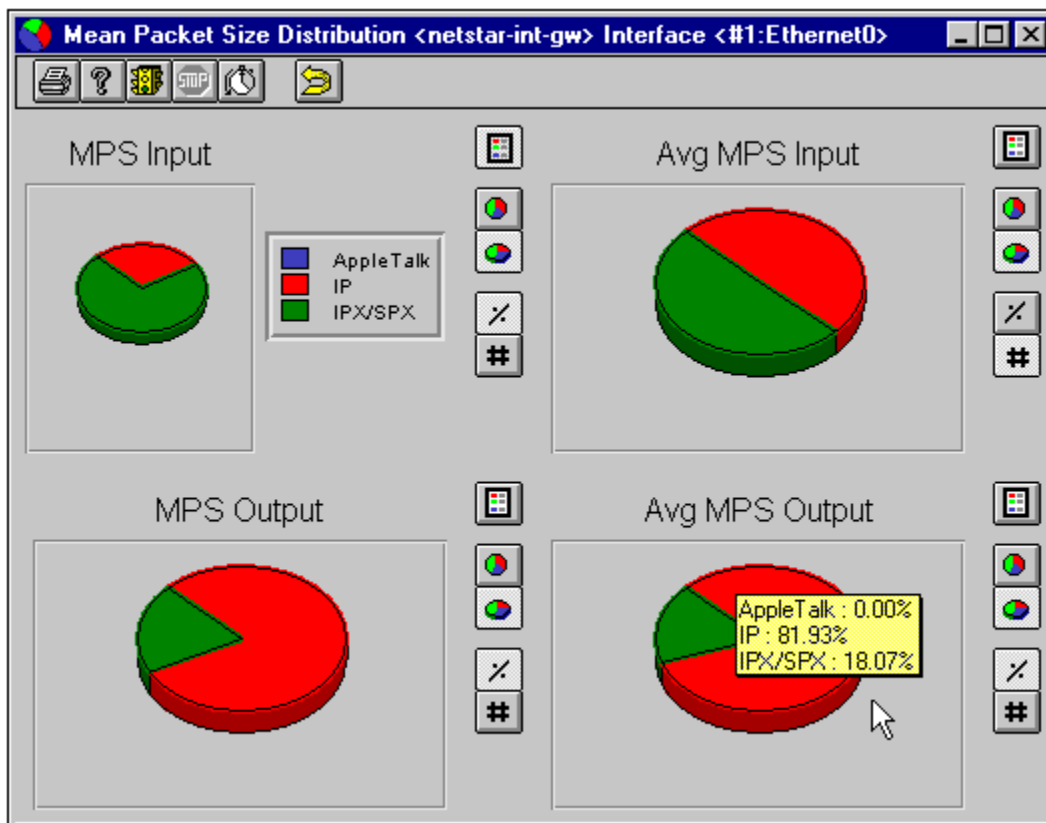
The graphs on the left display current information. The graphs on the right display information based on the entire monitoring period. Both Input and Output packets are shown.

Each pie chart shows up to three sections, depending on the available protocols. They are:

- AppleTalk
- IP
- Novell (IPX/SPX)

The data is updated on screen based on the polling interval.

**NOTE:** This applet is only available for Cisco routers running software version 9.1 and above.



Click the left mouse button on the pie chart to see the current values for each protocol, as shown above.

### Reading the chart

Two different sets of numbers are available from each Mean Packet Size Distribution pie chart: percentages and integer values (toggled by clicking the [Show Values/Show Percent] button).

Viewing **percentages** will show you the breakdown of packet information based on protocol. For example, in the Average Output chart above (bottom right), 81.93% of the packets moving over the interface are using IP, and 18.07% are using IPX. AppleTalk is not being used.

Viewing **values** will show the numbers that are used in calculating the percentages. For example, in this case, switching to values would show an IP mean packet size of 420.23 (Octets per packet) and an IPX mean packet size of 92.96. (If you calculate the numbers yourself, there will be a slight discrepancy due to rounding of the displayed numbers.)

Because we were looking at the Average Output chart, these figures represent the average packet size over the course of the monitoring period. The charts of the left side show current information, based on the most recent polling interval.

## Using the Mean Packet Size Distribution applet


**To start the Mean Packet Size Distribution applet:**

1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select Mean Packet Size Distribution. From the physical view, right-click on a particular interface and choose Mean Packet Size Distribution.
3. Choose the applet parameters and click OK. The applet opens and distribution pie charts will appear in the window, based on the polling interval. The pie charts will update for each polling interval.

Click the mouse on any point in the chart to view the precise statistics.





### Other buttons

There are three other button functions available for the pie charts.

Button	Description
	<b>[Reset Average Mean Packet Size] button</b> Resets the historical average mean packet size to zero, allowing you to gather new data from that point forward. After clicking, a message will prompt you to confirm your selection.

## Network Performance

---

Button	Description
	<b>[Show/Hide Pie Legend] button</b> Displays the key to the color-coded protocols, such as seen below: 
	<b>[Show/Hide 3D Effect] buttons</b> Toggles the pie chart between a 2D and 3D image.
	<b>[Show Values/Show Percent] buttons</b> Toggle the pie charts between displaying information as a integer value (e.g., 10 alerts sent) or as a percentage (e.g. 10% of all alerts sent).

## **Tools for 3Com devices**

### **3Com Specific Interface Tools: Overview**

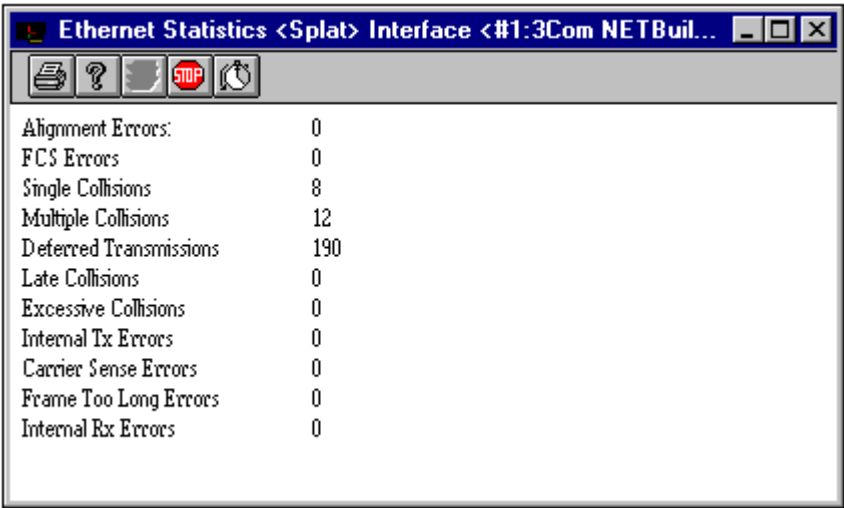
There are Interface tools that work only with 3Com devices. Available tools are:

- **The Ethernet Statistics Applet:3Com Specific**  
Displays, per interface, the number of errors that have occurred in the last polling period. Displayed errors include alignment errors, single, multiple, late and excessive collisions, etc.
- **The TokenRing Statistics applet - 3Com Specific**  
Displays, per interface, the number of errors that have occurred in the last polling period. Displayed errors include line errors, burst errors, token errors, number of beacons transmitted, etc.

### The Ethernet Statistics Applet:3Com Specific

The **Ethernet Statistics** applet displays, per interface, the number of errors that have occurred in the last polling period.

**NOTE:** This applet is only available from an Ethernet interface icon on a 3Com device.



The Status Number will turn red if it has changed from the last polling interval. If another polling interval passes without another change, the red status number will clear.

The following information is displayed in the Ethernet Statistics window:

Field Name	Description
Alignment Errors	The number of frames received that are not an integral number of bytes in length and do not pass the FCS check.
FCS Errors	The number of frames received that are an integral number of bytes and do not pass the Checksum check.

Field Name	Description
<b>Single Collisions</b>	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
<b>Multiple Collisions</b>	The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
<b>Deferred Transmissions</b>	The number of frame transmissions delayed because the medium was busy.
<b>Late Collisions</b>	The number of frames for which a collision was detected later than 512 bit-times into transmission.
<b>Excessive Collisions</b>	The number of frames which failed transmission because of excessive collisions.
<b>Internal Tx Errors</b>	The number of frames which failed transmission that are not counted in other frame transmit errors.
<b>Carrier Sense Errors</b>	The number of times that carrier sense was lost or never detected during transmission of a frame.
<b>Frame Too Long Errors</b>	The number of frames received which exceeded the maximum permitted frame size.
<b>Internal Rx Errors</b>	The number of frames received which are not counted by other errors.

## Using the Ethernet Statistics applet

To start the Ethernet Statistics applet:

1. Right-click on a device icon and select Boxmap.
2. From the application view, right-click on an individual interface icon and select Ethernet Statistics. From the physical view, right-click on a particular interface and choose Ethernet Statistics.

## Network Performance

---

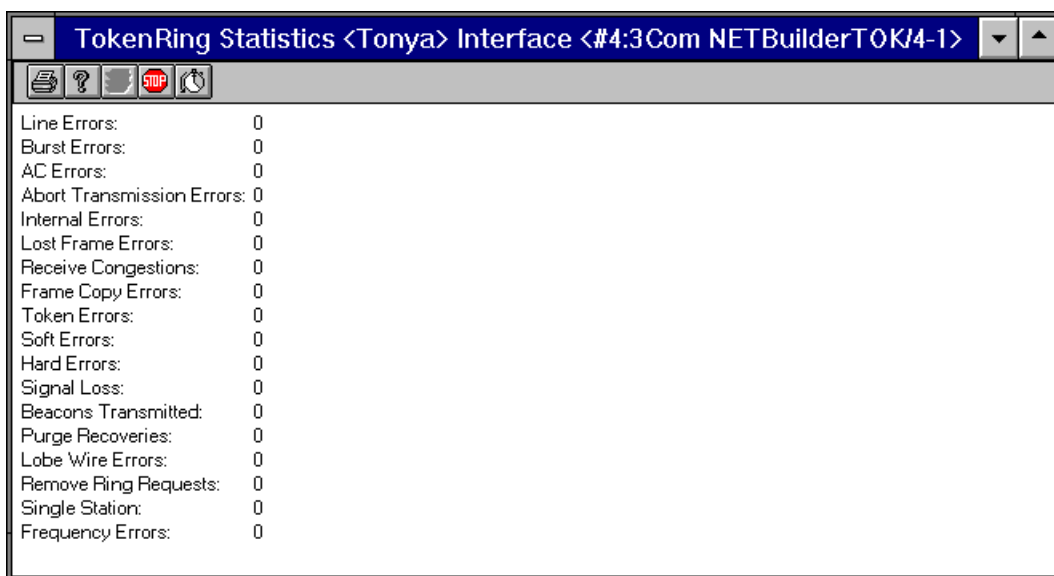
3. Choose the applet parameters and click OK. The applet opens and Ethernet statistics will be displayed in the window, based on the polling interval.

The Ethernet Statistics applet also uses the global [toolbar buttons](#)

### The TokenRing Statistics applet - 3Com Specific

The **TokenRing Statistics** applet displays, per interface, the number of errors that have occurred in the last polling period.

**NOTE:** This applet is only available from an TokenRing interface icon on a 3Com device.



The Status Number will turn red, if it has changed from the last polling interval. If another polling interval passes without another change, the red status number will clear.

The following information is displayed in the TokenRing Statistics window:

Field Name	Description
<b>Line Errors</b>	The number of frames received where there was a Checksum error or framing error.
<b>Burst Errors</b>	The number of times the interface detects the absence of transmissions for five half-bit times.
<b>AC Errors</b>	The number of times the interface detects an error in two successive AMP or SMP frames.
<b>Abort Transmission Errors</b>	The number of aborts transmitted while the interface was transmitting a frame.
<b>Internal Errors</b>	The number of internal errors detected.
<b>Lost Frame Errors</b>	The number of frames which could not be transmitted on an interface because the TRR timer expired during transmission.
<b>Receive Congestions</b>	The number of frames lost due to lack of buffer space.
<b>Frame Copy Errors</b>	The number of frames addressed to this interface where there might be a duplicate address or a possible line hit.
<b>Token Errors</b>	The number of times the interface detected an error condition that needs a token transmitted.
<b>Soft Errors</b>	The number of errors that are recoverable by the MAC layer protocols.
<b>Hard Errors</b>	The number of times an interface is either receiving or transmitting beacon MAC frames.
<b>Signal Loss</b>	The number of times this interface has detected the loss of signal condition from the ring.
<b>Beacons transmitted</b>	The number of times this interface has transmitted a beacon frame.
<b>Purge Recoveries</b>	The number of times the ring has been purged and is being recovered back into a normal operating state.
<b>Lobe Wire Errors</b>	The number of times the interface has detected an open or short circuit.

## Network Performance

---

Field Name	Description
<b>Remove Ring Requests</b>	The number of times this interface receives a remove ring MAC frame.
<b>Single Station</b>	The number of times this interface has sensed that it is the only station on the ring.
<b>Frequency Errors</b>	The number of times this interface has detected that the frequency of an incoming signal does not match what is expected.

## **CPU Utilization tools**

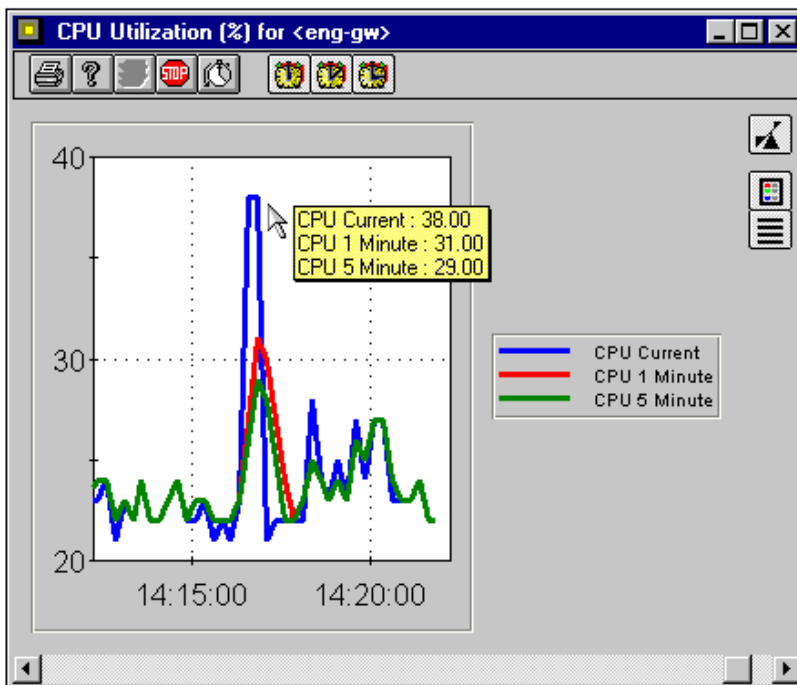
The CPU Utilization tools let you check what percentage of a device's CPU is being utilized.

Available tools are:

- **The CPU Utilization applet - Cisco specific**  
Displays CPU utilization data for Cisco devices. Provides current statistics, plus 1 minute and 5 minute moving averages.
- **The CPU Utilization applet - 3Com specific**  
Displays CPU utilization data for 3Com devices.

### **The CPU Utilization applet - Cisco specific**

The **CPU Utilization** applet shows the current, one and five minute CPU utilization statistics (exponentially decayed) calculated by the router. The 1 and 5 minute statistics are moving averages. Data is updated on the screen based on the polling interval.



Click the mouse on any point in the graph to view the CPU utilization information at that point.

### Reading the chart

The chart above shows CPU Utilization statistics. At the peak of the graph, a mouse click shows that current CPU utilization is 38 percent. The 1 minute (red line) and 5 minute (green line) averages are also displayed.

## Using the CPU Utilization applet - Cisco specific

### To start the CPU Utilization applet:



1. Right-click on a Cisco router device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose CPU Utilization. From the application view, right-click the CPU Utilization icon and select **Utilization**.
3. Choose the applet parameters and click OK. The applet opens and CPU utilization information will begin to be graphed in the window, based on the polling interval.






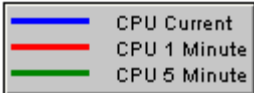

Click the mouse on any point in the graph to view the precise statistics at that point.

4. Click the [Show/Hide CPU] buttons (see below) to view the current utilization information, or to see 1 minute and/or 5 minute moving averages.

### Other buttons

In addition to the global toolbar buttons, the CPU Utilization applet has the following specialized buttons:

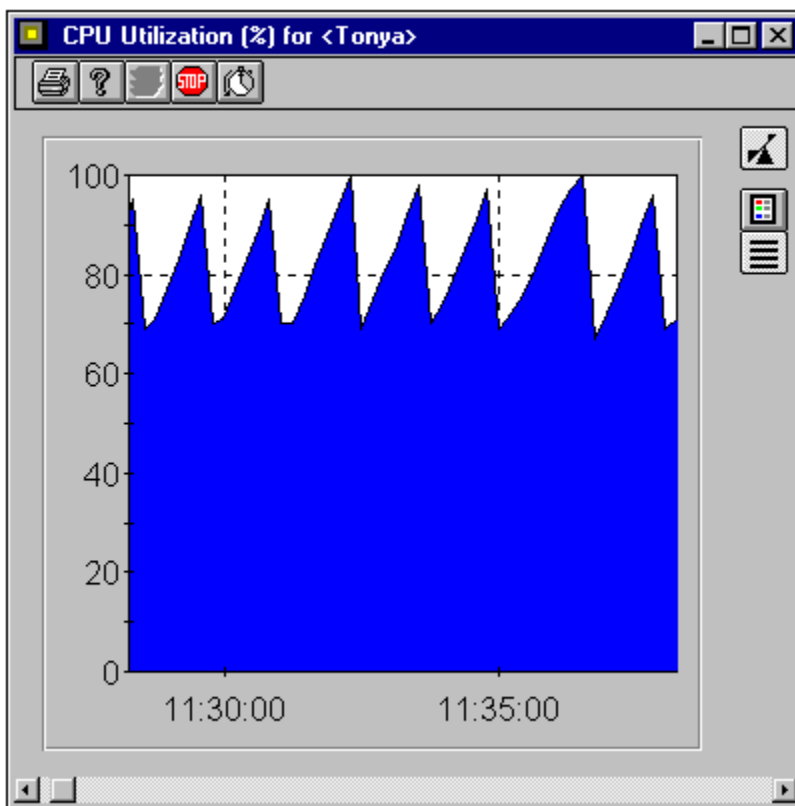
Button	Description
	<b>[Show/Hide CPU Current Graph] button</b> Toggles the current CPU utilization graph line on and off.
	<b>[Show/Hide CPU 1 Minute Graph] button</b> Toggles the 1 minute moving average CPU utilization graph line on and off.

Button	Description
	<b>[Show/Hide CPU 5 Minute Graph] button</b> Toggles the 5 minute moving average CPU utilization graph line on and off.
  	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coded CPU utilization information, such as seen below. <div data-bbox="498 875 751 967">  </div>
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## The CPU Utilization applet - 3Com specific

The **CPU Utilization** applet shows the current CPU utilization statistics calculated by the router.

Data is updated on the screen based on the polling interval.



### Reading the chart

The chart above shows CPU Utilization statistics. This graph shows a router that is continually peaking near or at 100% of capacity.

---

## Using the CPU Utilization applet - 3Com specific



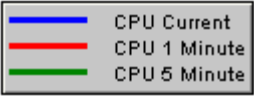

### To start the CPU Utilization applet:

1. Right-click on a 3Com router device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **CPU Utilization**. From the application view, right-click the CPU Utilization icon and select Utilization.
3. Choose the applet parameters and click OK. The applet opens and CPU utilization information will begin to be graphed in the window, based on the polling interval.

Click the mouse on any point in the graph to view the precise statistics at that point.

### Other buttons

In addition to the global toolbar buttons, the CPU Utilization applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the key to the color-coded CPU utilization information, such as seen below. 
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## **ISDN tools**

The ISDN tools provide ISDN usage statistics.

Available tools are:

- **The ISDN Neighbor Table applet - Cisco specific**  
Provides ISDN usage statistics for Cisco devices. Information displayed includes interface name and number, maximum call time, duration of last call, number of calls completed/failed/accepted, etc.

### **The ISDN Neighbor Table applet - Cisco specific**

The **ISDN Neighbor Table** applet shows ISDN usage statistics. Data is updated on the screen based on the polling interval.

The following information is displayed in the ISDN Neighbor Table window:

Field	Description
<b>IF Index</b>	The system defined interface number.
<b>IF Name</b>	The system defined name of the device.
<b>NbrLogIf</b>	The interface number of the B-channel associated with the neighbor.
<b>NbrName</b>	The ASCII name of the neighbor.
<b>NbrAddress</b>	Call Address at which the neighbor should be called. Think of this as the set of characters following 'ATDT' or the 'phone number' included in a D channel call request.
<b>NbrPermission</b>	Applicable permissions of which interfaces can call each other.
<b>NbrMaxDuration</b>	Maximum call duration in seconds.
<b>NbrLastDuration</b>	Duration of last call in seconds.

Field	Description
NbrClearReason	ASCII reason that the last call terminated.
NbrClearCode	Encoded reason for the last call tear down.
NbrSuccessCalls	Number of completed calls to neighbor since system reset.
NbrFailCalls	Number of call attempts that have failed.
NbrAcceptCalls	Number of calls accepted from the neighbor.
NbrRefuseCalls	Number of calls from neighbor that have been refused.
NbrLastAttemptTime	SysUpTime of last call attempt.
NbrStatus	Status of this entry.
NbrCallOrigin	Indication of an outgoing or incoming call.


## Using the ISDN Neighbor Table applet

To start the ISDN Neighbor Table applet:

1. Right-click on a Cisco router icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose ISDN Neighbor Table. From the application view, right-click the ISDN icon in the Boxmap and choose Neighbor Table Applet.
3. Choose the applet parameters and click OK. The applet opens and neighbor table information will appear in the window.

### Other buttons

In addition to the global toolbar buttons the ISDN Neighbor Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## **Frame Relay tools**

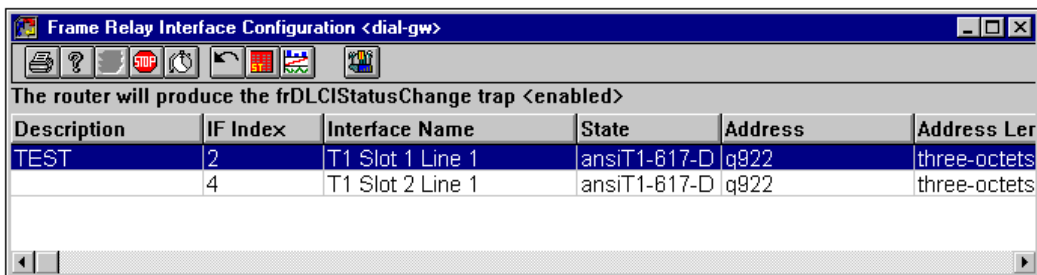
The Frame Relay tools provide information about Frame Relay on your system.

Available tools are:

- **Frame Relay Interface Configuration applet**  
Displays information about all configured Frame Relay interfaces on a device. Information includes interface name and index, address, address length, polling interval, etc.
- **Frame Relay Virtual Circuit Utilization applet**  
Displays performance information for DLCIs on a virtual circuit. Utilization is shown as a percentage of CIR.
- **Frame Relay Virtual Circuit Statistics applet**  
Displays information for all DLCIs configured on the device. Information includes Interface name and number, DLCI number, forward and backward congestion, sent/received frames and bytes, etc.
- **Frame Relay Virtual Circuit Link Utilization applet**  
Displays statistical performance information for virtual circuit links. Input and output utilization is shown as a percentage of CIR for both ends of the virtual circuit link.
- **Frame Relay Virtual Circuit Link Statistics applet**  
Displays information for virtual circuit links. Information includes device and interface name, link status (good, degraded, poor), bytes/frames in and out, FECN, BECN, percentage of CIR throughput, etc.
- **DLCI Configuration applet**  
Provides a means to modify selected DLCIs. Factors that can be modified are Stored CIR, Stored Maximum Transmission and the Percentage of CIR Utilization Threshold.

## The Frame Relay Interface Configuration applet

The **Frame Relay Interface Configuration** applet displays information about all of the configured Frame Relay Interfaces on the device. The applet also displays whether or not the router is able to send DLCI status change Traps.



The following information is displayed in the Frame Relay Interface Configuration window:

Heading	Definition
<b>Description</b>	The user-defined description set in the Description Applet (under the specific Interface Icon on the router).
<b>IF Index</b>	The system defined interface number.
<b>Interface Name</b>	The system defined interface name.
<b>State</b>	Displays which Data Link Connection Management scheme is active. Possible values are:  <b>noLmiConfigured</b>  <b>ImiRev1</b>  <b>ansiT1-617-D (ANSI T1.617 Annex D)</b>  <b>ansiT1-617-B (ANSI T1.617 Annex B)</b>

Heading	Definition
<b>Address</b>	The type of addressing format. Possible values are: <b>q921 (13 bit DLCI)</b> <b>q922March90 (11 bit DLCI)</b> <b>q922November (10 bit DLCI)</b> <b>q922 (Final Standard)</b>
<b>Address Length</b>	The length of the address field. Possible values are Two Octets, Three Octets or Four Octets.
<b>Polling Interval</b>	The number of seconds between successive Status Inquiry Messages.
<b>Enquiry Interval</b>	The number of Status Inquiry intervals that pass before a Full Status Inquiry Message is issued.
<b>Error Threshold</b>	The number of unanswered Status Inquiry Messages before declaring the link down.
<b>Monitored Events</b>	The number of intervals making up the period for counting the number of unanswered status messages.
<b>Max Supported VCs</b>	The maximum number of VCs supported on this interface.
<b>Multi Cast</b>	Indicates if the interface uses a multi-cast service.

## Using the Frame Relay Interface Configuration applet





To start the Frame Relay Interface Configuration applet:

1. Use one of the following:
  - a. Right-click on a device icon or backpanel and select **Frame Relay > Interface Configuration**.
  - b. Right-click on the Frame Relay icon in the Boxmap and select **Interface Configuration**.
2. Choose the applet parameters and click OK. The applet opens and Frame

Relay configuration information will appear in the window, based on the polling interval.

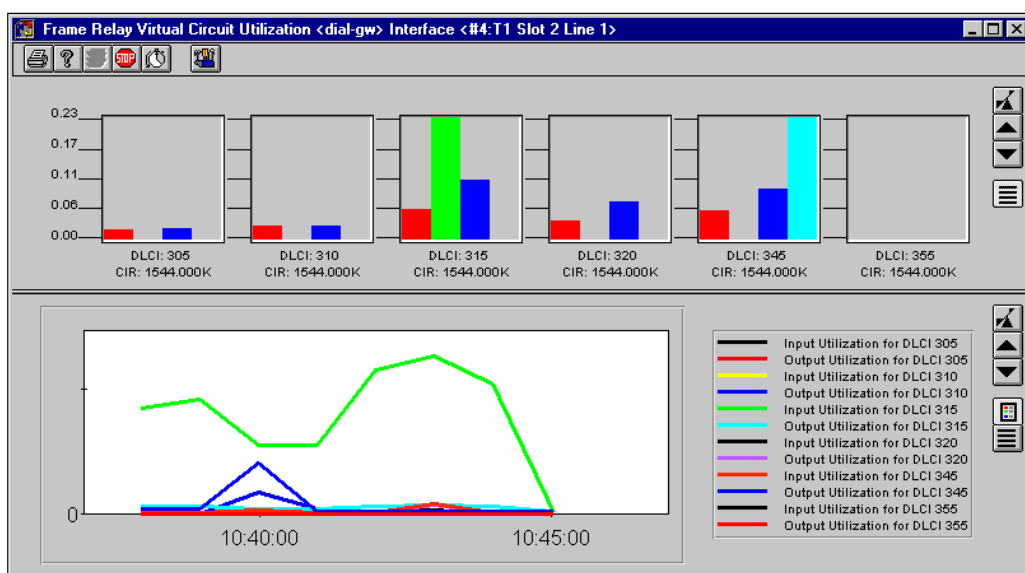
### Other buttons

In addition to the global toolbar buttons, the Frame Relay Interface Configuration applet has the following specialized buttons:

Button	Description
	<b>[Virtual Circuit Statistics] button</b> Launches the Frame Relay Virtual Circuit Statistics applet for the selected row. This applet displays statistics for all DLCIs on the selected interface. Statistics include forward and backward congestion, sent/received frames and bytes, committed burst, etc.
	<b>[Virtual Circuit Utilization] button</b> Launches the Frame Relay Virtual Circuit Utilization applet for the selected row. This applet displays performance information for DLCIs on a virtual circuit.
	<b>[DLCI Configuration] button</b> Launches the DLCI Configuration applet for the selected row. This applet allows you to modify the configuration of a selected DLCI.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

### The Frame Relay Virtual Circuit Utilization applet

The **Frame Relay Virtual Circuit Utilization** applet displays performance information for DLCIs on a virtual circuit. Utilization is shown as a percentage of CIR.



#### Reading the chart

The applet is divided into two panes.

The top pane displays each DLCI configured on this interface in a separate gauge, with a maximum of 10 DLCIs displayed at one time. Utilization information is displayed as a percentage of CIR. This applet is very useful in determining which DLCIs are generating the most traffic, and how much CIR is actually being utilized.

Each gauge in the upper pane shows four bar graphs. From left to right, they are:

**Bar 1** - Input Utilization (as a percentage of CIR). The real-time, on-going input utilization for the DLCI.

**Bar 2** - Average Input Utilization. The average utilization over the course of

the monitoring period.

**Bar 3** - Output CIR Utilization. The real-time, on-going output utilization for the DLCI.

**Bar 4** - Average Output Utilization. The average utilization over the course of the monitoring period.

If there are more than 10 DLCIs on the interface, use the [Next Page] button to advance to the next page, and the [Previous Page] button to return to an earlier page.

The bottom pane displays the real-time input and output utilization of each configured DLCI as a line graph.

## Using the Frame Relay Virtual Circuit Utilization applet


The **Frame Relay Virtual Circuit Utilization** applet is launched from within the Frame Relay Interface Configuration applet.

### To open the Utilization applet:




1. Start the Frame Relay Interface Configuration applet.
2. Highlight a particular interface within this applet and click the [Virtual Circuit Utilization] button. You can also right-click on the selected interface and choose **VC Utilization**.
3. Choose the applet parameters and click OK. The Frame Relay Virtual Circuit utilization window will open and utilization statistics will appear, based on the polling interval.

### Other buttons

In addition to the global toolbar buttons, the Frame Relay Virtual Circuit Utilization applet has the following specialized buttons:

Button	Description
	<b>[DLCI Configuration] button</b> Launches the DLCI Configuration applet for the selected row. This applet allows you to modify the configuration of a selected DLCI.

## Network Performance

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph reading are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the color-coded key to the graph.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## The Frame Relay Virtual Circuit Statistics applet

The **Frame Relay Virtual Circuit Statistics** applet displays information for all of the DLCIs configured on the device, sorted by interface. Statistics for each DLCI are listed in the columns.

Frame Relay Virtual Circuit Statistics <RussNetCentral>									
IF Index	Interface	VC Name	DLCI#	State	Forward	Backward	Sent Frames	Sent Bytes	Re
3	Serial0		100	active	0	0	242803	112425316	11
3	Serial0	Virtual Circuit 1	101	active	0	0	257230	110416278	61
3	Serial0	Virtual Circuit 2	102	active	0	0	232515	107617294	32
3	Serial0	Virtual Circuit 3	103	active	0	0	310044	118457395	18
3	Serial0		104	active	0	0	255766	101626276	11

The following information is displayed in the Frame Relay Virtual Circuit Statistics window:

Heading	Definition
<b>IF Index</b>	The system defined interface number.

Heading	Definition
<b>Interface</b>	The interface the DLCI exists on.
<b>VC Name</b>	The user-configured name for the virtual circuit. This field must be configured using the VC Link Configuration applet.
<b>DLCI#</b>	The Data Link Connection Identifier for the circuit.
<b>State</b>	Indicates whether the particular virtual circuit is operational.
<b>Forward Congestion</b>	The number of frames received from the network indicating forward congestion.
<b>Backward Congestion</b>	The number of frames received from the network indicating backward congestion.
<b>Sent Frames</b>	The number of frames sent from this virtual circuit.
<b>Sent Bytes</b>	The number of bytes sent from this virtual circuit.
<b>Received Frames</b>	The number of frames received over this virtual circuit.
<b>Received Bytes</b>	The number of bytes received over this virtual circuit.
<b>Committed Burst</b>	The maximum amount of committed data bits that the network will attempt to deliver.
<b>Excess Bursts</b>	The maximum amount of uncommitted data bits that the network will attempt to deliver.
<b>Agent CIR</b>	The CIR MIB variable supplied by the manufacturer of the device.

### Using the Frame Relay Virtual Circuit Statistics applet





The **Frame Relay Virtual Circuit Statistics** applet is launched from within the Frame Relay Interface Configuration applet.

#### To open the Statistics applet:

1. Start the Frame Relay Interface Configuration applet.
2. Highlight a particular interface within this applet and click the [Virtual Circuit Statistics] button. You can also right-click on the selected interface and choose **VC Statistics**.
3. Choose the applet parameters and click OK. The Frame Relay Virtual Circuit Statistics window will open and utilization statistics will appear, based on the polling interval.

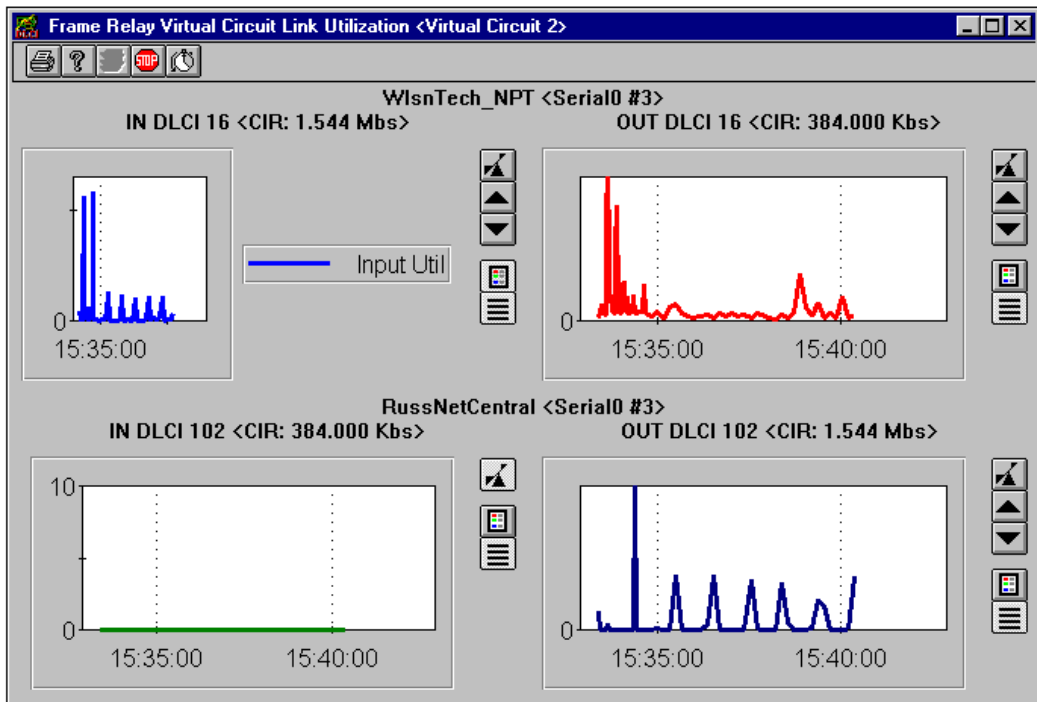
#### Other buttons

In addition to the global toolbar buttons, the Frame Relay Virtual Circuits Statistics applet has the following specialized buttons:

Button	Description
	<b>[VC Link Utilization] button</b> Launches the Frame Relay Virtual Circuit Link Utilization applet for the selected row. This applet provides performance information for virtual circuit links (if any are configured).
	<b>[VC Link Statistics]</b> Launches the Frame Relay Virtual Circuit Link Statistics applet for the selected row. This applet provides statistical information for virtual circuit links (if any are configured).
	<b>[DLCI Configuration] button</b> Launches the DLCI Configuration applet for the selected row. This applet allows you to modify the configuration of a selected DLCI.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The Frame Relay Virtual Circuit Link Utilization applet

The **Frame Relay Virtual Circuit Link Utilization** applet displays statistical performance information for virtual circuit links. Input and output utilization are shown as a percentage of CIR for both ends of the virtual circuit link.



### Reading the chart

The VC Link chart shows real-time utilization for both sides of a virtual circuit. In the sample above, we see the link between two devices, WlsnTech\_NPT (using Serial0) and RussNetCentral (using Serial0). The top window pane shows the Input (left side) and Output (right side) utilization for WlsnTechNPT. Utilization statistics are shown as a percentage of CIR, which in this case is 1.544 Mbs input and 384 Kbs output.

The bottom window pane shows Input and Output for RussNetCentral. Together, this applet gives a complete picture of the traffic on the given virtual circuit and the degree to which the CIR is being used.

## Using the Frame Relay Virtual Circuit Link Utilization applet




The **Frame Relay Virtual Circuit Link Utilization** applet is launched from within the Frame Relay Virtual Circuit Statistics applet. *This applet is only available if there are virtual circuit links configured for the device.*

### To open the Link Utilization applet:

1. Start the Frame Relay Virtual Circuit Statistics applet.
2. Highlight a particular interface within this applet and click the [VC Link Utilization] button. You can also right-click on the selected interface and choose VC Link Utilization.
3. Choose the applet parameters and click OK. The Frame Relay Virtual Circuit Link Utilization window will open and utilization statistics will begin to appear, based on the polling interval.

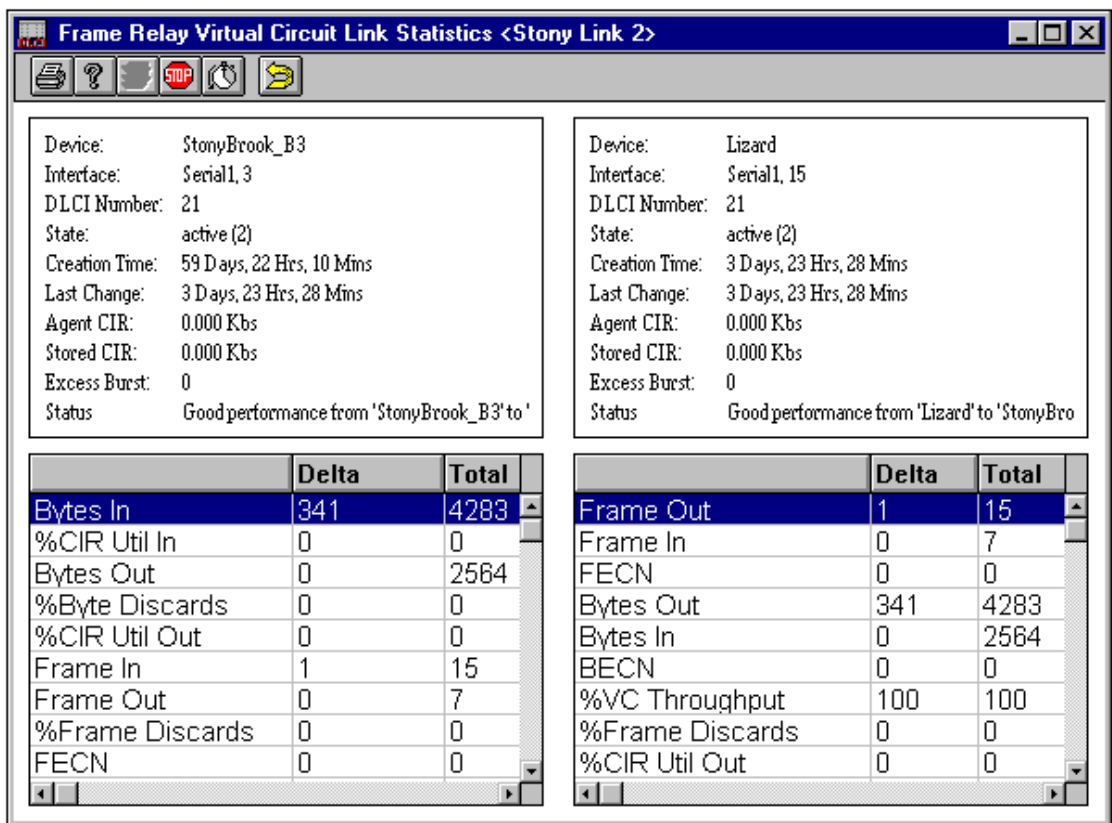
### Other Buttons

In addition to the global toolbar buttons, the Frame Relay Virtual Circuit Link Utilization applet has the following specialized buttons:

Button	Description
	<b>[Autoscale Graph] buttons</b> Adjusts the graph scale up or down. This is useful if the graph readings are going higher than the top of the gauge, or are very low and hard to see at the bottom of the gauge.
	<b>[Show/Hide Graph Legend] button</b> Displays the color-coded key to the graph.
	<b>[Show/Hide Graph Grid] button</b> Places a grid on the gauges for easier reading.

## The Frame Relay Virtual Circuit Link Statistics applet

The **Frame Relay Virtual Circuit Link Statistics** applet displays information for virtual circuit links. Information includes device and interface name, link status (good, degraded, poor), bytes/frames in and out, FECN, BECN, percentage of CIR throughput, etc.



The following information is displayed in the upper pane of the Virtual Circuit Link Statistics window:

Heading	Definition
Device	The name of the device.
Interface	The interface the DLCI exists on.

## Network Performance

---

Heading	Definition
<b>DLCI Number</b>	The Data Link Connection Identifier for this virtual circuit.
<b>State</b>	Indicates whether the particular virtual circuit is operational. Possible values are: Active, inactive, invalid.
<b>Creation Time</b>	How long the virtual circuit has been operating.
<b>Last Change</b>	How long since the last time the virtual circuit was changed.
<b>Agent CIR</b>	The CIR MIB variable supplied by the manufacturer of the device.
<b>Stored CIR</b>	The manually set value for the CIR MIB variable.
<b>Excess Burst</b>	The maximum amount of uncommitted data bits that the network will attempt to deliver.
<b>Status</b>	Rates the performance of the virtual circuit. The status levels are: Good (throughput is above the CIR threshold value), Degraded (throughput is below the CIR threshold, but not below the ratio of CIR/MAX), Poor (throughput is less than CIR/MAX). (MAX = the maximum amount of data the switch will attempt to deliver.)

The following information is displayed in the lower pane of the Virtual Circuit Link Statistics window:

Heading	Definition
<b>Bytes In</b>	The number of bytes received over this virtual circuit.
<b>% CIR Util In</b>	The percentage of the incoming CIR that is being utilized.
<b>Bytes Out</b>	The number of bytes sent from this virtual circuit.
<b>% Byte Discards</b>	The percentage of bytes which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
<b>% CIR Util Out</b>	The percentage of the outgoing CIR that is being utilized.

Heading	Definition
<b>Frame In</b>	The number of frames received over this virtual circuit.
<b>Frame Out</b>	The number of frames sent from this virtual circuit.
<b>% Frame Discards</b>	The percentage of frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
<b>FECN (Forward Explicit Congestion Notification)</b>	The number of frames received from the network indicating forward congestion.
<b>BECN (Backward Explicit Congestion Notification)</b>	The number of frames received from the network indicating backward congestion.
<b>% CIR Throughput</b>	The percentage of the CIR that is being used across the circuit.
<b>% VC Throughput</b>	The percentage of transmitted data that is delivered on the other side of the virtual circuit.

#### Reading the chart

When reading the VC Link Statistics window, the Bytes In on one side of the Virtual Circuit should match the Bytes Out on the other side, and the Frame In on one side should match the Frame Out on the other side. The % Byte Discards and % Frame Discards inform you of the percent of data that your carrier is dropping. A high percentage of discards can indicate the need to increase the bandwidth for this circuit.

### Using the Frame Relay Virtual Circuit Link Statistics applet


The Frame Relay Virtual Circuit Link Statistics applet is launched from within the Frame Relay Virtual Circuit Statistics applet. *This applet is only available if there are virtual circuit links configured for the device.*

#### To open the Link Statistics applet:

1. Start the Frame Relay Virtual Circuit Statistics applet.
2. Highlight a particular interface within this applet and click the [VC Link Statistics] button. You can also right-click on the selected interface and choose **VC Link Statistics**.
3. Choose the applet parameters and click OK. The Frame Relay Virtual Circuit Link Statistics window will open and statistics will begin to appear, based on the polling interval.

#### Other Buttons

In addition to the global toolbar buttons, the Frame Relay Virtual Link Statistics applet has the following specialized button:

Button	Description
	<b>[Reset Statistics] button</b> Resets field information to zero, allowing you to gather new data from that point forward. After clicking, a message will prompt you to confirm your selection.

## The DLCI Configuration applet

The **DLCI Configuration** applet lets you modify the configuration of any selected DLCI. It is important to keep CIR information up to date, because performance calculations are based on these values. Incorrect or out-of-date information can lead to misleading performance results.

The screenshot shows the 'DLCI Configuration' window. At the top, there is a 'DLCI List:' label. Below it is a table with the following data:

Device	Interface	DLCI	Agent CIR	Stored CIR	Agent Max Tx	Stored Max Tx	%CIR Util Thr
StonyBrook B3	Serial1 <3>	21	0	20000	0	20000	75
StonyBrook B3	Serial1 <3>	30	0	0	0	0	0
StonyBrook B3	Serial1 <3>	31	0	0	0	0	0
StonyBrook B3	Serial1 <3>	32	0	0	0	0	0
StonyBrook B3	Serial1 <3>	33	0	0	0	0	0
StonyBrook B3	Serial1 <3>	34	0	0	0	0	0
StonyBrook B3	Serial1 <3>	35	0	0	0	0	60
StonyBrook B3	Serial1 <3>	36	0	0	0	0	0
StonyBrook B3	Serial1 <3>	37	0	0	0	0	0
StonyBrook B3	Serial1 <3>	38	0	0	0	0	0

Below the table, there are three input fields with spinners:

- Stored CIR: (Kbps) with a value of 20.
- Stored Max Tx: (Kbps) with a value of 20.
- %CIR Util Threshold: with a value of 75.

At the bottom, there are five buttons: Ok, Apply, Delete, Cancel, and Help.

The following information is displayed in the DLCI Configuration window:

Heading	Definition
Device	The name of the device the DLCI is on.
Interface	The system defined interface name.
DLCI	The Data Link Connection Identifier for this virtual circuit.
Agent CIR	The CIR MIB variable configured on the device.
Stored CIR	The manually set value for the CIR MIB variable. This overrides the Agent CIR value. Some devices do not support the Agent CIR variable.

Heading	Definition
<b>Agent MaxTx (Tx = transmission)</b>	The amount of data that the switch will attempt to deliver in a measurement interval. This is usually available from the device by default. However, some devices do not support this value. In that case, you can manually enter a value in the Stored MaxTx field.
<b>Stored MaxTx (Tx = transmission)</b>	The manually entered value for the maximum amount of data the switch will attempt to deliver. The default value is the same as the value for Agent MaxTx if not set to zero.
<b>%CIR Util Threshold</b>	The manually entered value that specifies the DLCI transmission utilization threshold. The default value is 60%. Utilization threshold events can be turned off by setting this value to 0%. The range for this value is 0 - 2000%. An event is generated if this value is exceeded.

### Using the DLCI Configuration applet

#### To start the DLCI Configuration applet:

1. Use one of the following:
  - a. Right-click on a device icon or backpanel and select **Frame Relay > DLCI Configuration**.
  - b. Right-click on the Frame Relay icon in the Boxmap and select **DLCI Configuration**.
2. The applet opens and DLCI information is displayed.
3. To set values for Stored CIR, Stored Maximum Transmission and/or Percentage of CIR Utilization Threshold, highlight a specific DLCI, enter a value in the respective spin box and click [Apply]. Set as many DLCI's as needed.
4. Click [OK] when all settings are complete.
5. To restore settings to zero, highlight the DLCI and click [Delete].

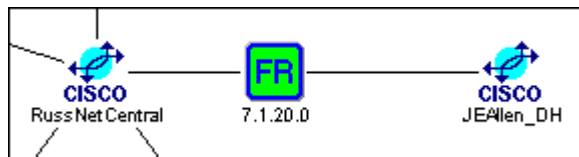
---

## Configuring Virtual Circuit Links

Virtual Circuits represent logical connections between interfaces on devices connected through a Frame Relay Cloud.

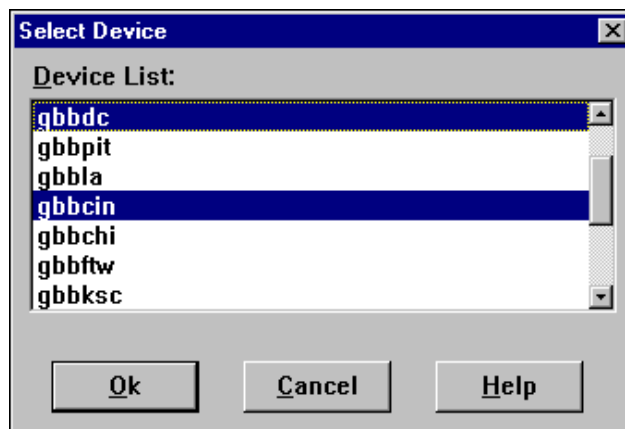
### To configure a Virtual Circuit in a Frame Relay Cloud:

1. Right-click the Frame Relay Cloud icon in either the Internet map or the Group Wizard and select **Circuit Map**. The Circuit Map can also be displayed by double-clicking the Frame Relay Cloud icon in the Group Wizard screen.
2. From within the Circuit Map, select a Frame Relay circuit icon that is between two devices, such as shown below. You cannot configure a Frame Relay circuit if it is not connecting two devices.



Right-click the Frame Relay Circuit icon and select **Configuration**.

If the Frame Relay Circuit is connecting more than two devices, the Select Device dialog box will appear.



Choose two devices from the list, and click [OK].

More than two devices may be connected to a Frame Relay Circuit icon

only if subinterfacing is not implemented on your network.

3. The Virtual Circuit Link Configuration dialog box displays:

DLCI	State	Agent CIR	Stored CIR	Agent MaxTx	Stored MaxTx	%CIR Util Thresh	%VC Throughput
100	active	0	0	0	0	50	50
104	active	0	0	0	0	0	0

The top of the dialog displays the device name, the parent interface (Poll IF), the logical interface you are configuring (Config IF), the IP address and the Current DLCI.

The Virtual Circuit dialog box contains the following fields:

Heading	Definition
DLCI	The Data Link Connection Identifier for this virtual circuit.
State	Indicates if the DLCI is active or inactive.
Agent CIR	The CIR MIB variable configured on the device.
Stored CIR	The manually set value for the CIR MIB variable. This overrides the Agent CIR value. Some devices do not support the Agent CIR variable.
Agent MaxTx (Tx = transmission)	The amount of data that the switch will attempt to deliver in a measurement interval.

Heading	Definition
<b>Stored MaxTx (Tx = transmission)</b>	The manually entered value for the maximum amount of data the switch will attempt to deliver. The default value is the same as the value for Agent MaxTx if not set to zero.
<b>%CIR Util Thresh</b>	The manually entered value that specifies the DLCI transmission utilization threshold. The default value is 60%. Utilization threshold events can be turned off by setting this value to 0%. The range for this value is 0 - 2000%. An event is generated if this value is exceeded.
<b>%VC Throughput Thresh</b>	Specifies a threshold value for virtual circuit throughput. The default value is 50%. An event is generated if throughput falls below the specified value.

- For each device, select a DLCI that you want associated with the Virtual Circuit. To function properly, all DLCIs *must* have been configured using the DLCI Configuration applet.

To associate a DLCI with a Virtual Circuit, highlight it from the DLCI list and click [Apply]. The DLCI you select appears in the “Cur DLCI” field.

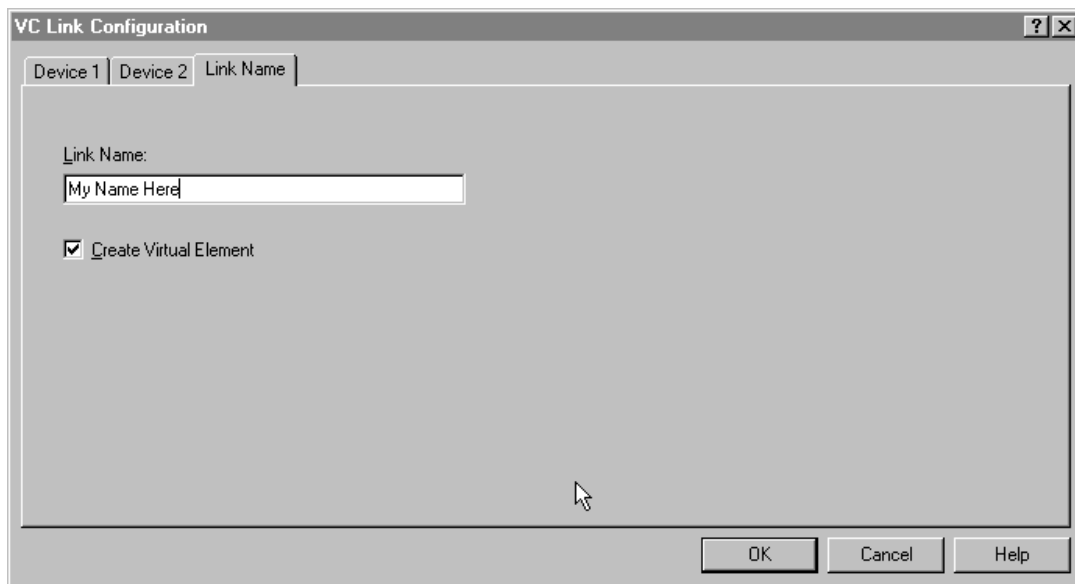
**NOTE for Ascend Devices:** Ascend devices may not automatically display the interface containing the DLCI. To find the correct interface, open the Frame Relay Interface Configuration applet for the device. The IF Index numbers for any DLCI's will be listed there. Then, in the Link Configuration window, select the proper interface using the Poll IF drop-down list. The DLCI information will then appear in the table.

Use the Device tabs to change the device for which you are selecting a DLCI.

**NOTE:** If you are using subinterfacing or virtual ports, you must verify that the Poll IF field contains the correct information. The Poll IF Field should contain the physical interface connected to the Frame Relay network.

- Click the Link Name tab to give the Virtual Circuit link a descriptive name.

## Network Performance



To give the link a descriptive name, enter a name in the Link Name dialog box.

Select **Create Virtual Element** to create an icon for the Virtual Circuit in the Group Wizard screen. This allows you to check the Virtual Circuit Link Utilization graphs and the Virtual Circuit Link Statistics directly from the Group Wizard screen. Right-click on the icon to access the applications.



## **X.25 Tools**

The X.25 tools provide information about X.25 communications on your system.

**NOTE:** X.25 tools are not available for Wellfleet/Bay routers.

There are two categories of X.25 tools: Administrative and Operational.

- **Administrative tools** display information about the X.25 configuration as defined by the administrator.
- **Operational tools** display information about the current X.25 operating parameters. These values reflect changes in the X.25 configuration made after the system was started.

Available administrative tools are:

- **X.25 Administrative Table applet**  
Displays the X.25 configuration for a device as defined by the administrator. Displayed information includes interface name and index, maximum active circuits, number of PVCs, etc.
- **X.25 Administrative Table Overview applet**  
Displays consolidated interface information, including the timer and counter information (such as restart, reset, clear, reject) and call parameters.
- **X.25 Administrative Table Timer Variables applet**  
Displays X.25 timer variable information, including restart timer, reset timer, call timer, clear timer, etc.
- **X.25 Administrative Table Counter Variables applet**  
Displays X.25 counter variable information, including restart count, reset count, reject count, clear count, etc.

Available operational tools are:

- **X.25 Operational Table applet**  
Displays the current X.25 operating parameters, reflecting changes made after the system was started.

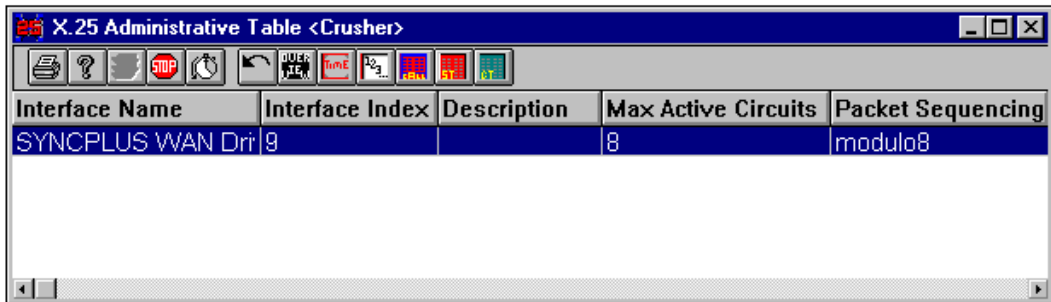
- **X.25 Operational Table OverView applet**  
Displays consolidated interface information, including the timer and counter information (such as restart, reset, clear, reject) and call parameters.
- **X.25 Operational Table Timer Variables applet**  
Displays X.25 timer variable information, including restart timer, reset timer, call timer, clear timer, etc.
- **X.25 Operational Table Counter Variables applet**  
Displays X.25 counter variable information, including restart count, reset count, reject count, clear count, etc.

One additional tool is accessed from both the administrative and operational tools:

- **X.25 Call Parameters Table applet**  
Displays X.25 call parameters information, only for parameters manually defined to the router. Otherwise, this table is empty

## X.25 Administrative Table applet

The **X.25 Administrative Table** applet contains the X.25 configuration defined by the administrator. The Administrative Table displays the basic X.25 configuration data. It provides toolbar access to detailed configuration information. The information presented reflects the X.25 configuration that will be utilized upon the next reinitialization.



The following Information is displayed in the X.25 Administrative Table.






Heading	Definition
Interface Name	The name of the interface.
Interface Index	The interface number.
Description	The interface description defined in the Description applet for the interface.
Max Active Circuits	The number of active circuits supported.
Packet Sequencing	The type of packet sequencing in use (possible values are Modulo 8 or Modulo 128).
Number of PVCs	The number of Permanent Virtual Circuits configured.
X.121 Address	The X.121 address assigned to this interface.
CCITT Version (Also referred to as ITU-T version.)	The version of X.25 supported.



## Using the X.25 Administrative Table applet

**To start the X.25 Administrative Table applet:**

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose **X.25 > Administrative Table**. From the application view, right-click the X.25 icon and choose **Administrative Table**.
3. Choose the Applet Parameters and click OK. The applet opens and X.25 configuration information appears.

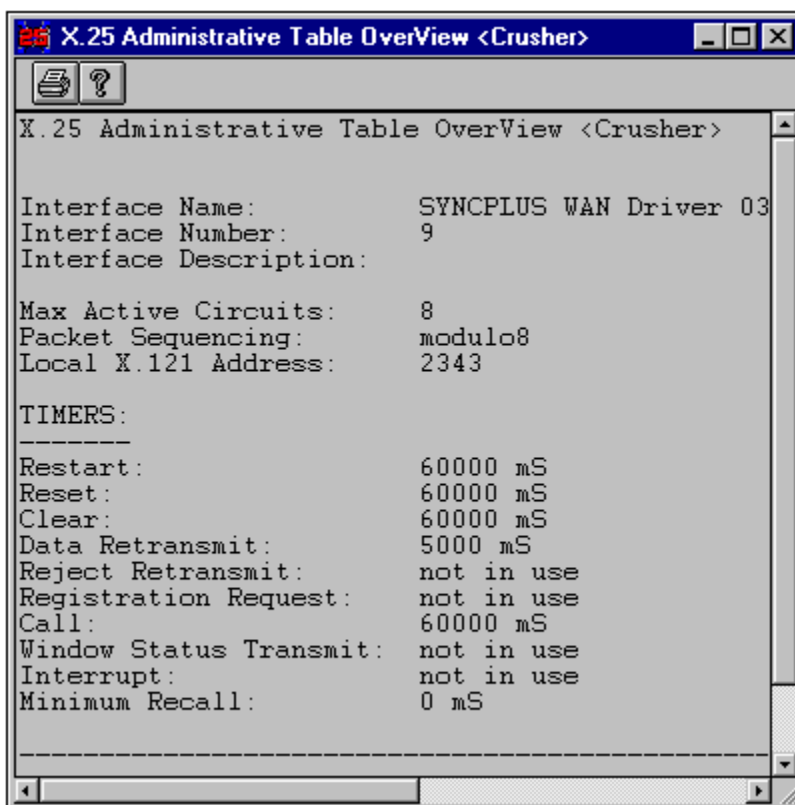
In addition to the global Toolbars, there are seven specialized buttons on the right-hand side of the X.25 Administrative applet toolbar.

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.
	<b>[X.25 Overview] button</b> Opens the X.25 Administrative Table Overview applet for a selected row. Displays consolidated interface information.
	<b>[Show the Timer Variables] button</b> Opens the X.25 Administrative Table Timer Variables applet for a selected row. Displays timer information, such as restart, reset and clear times.
	<b>[Show the Counter Variables] button</b> Opens the X.25 Administrative Table Counter Variables applet for the selected row. Displays counter information, such as restart count, reset count, etc.
	<b>[Show the Call Parameters Table] button</b> Opens the X.25 Call Parameters Table applet which for the selected row. Displays call parameter information, such as status, in and out packet size, etc.

Button	Description
	<p><b>[Show the X.25 Statistics] button</b></p> <p>Opens the X.25 Statistics applet which displays the values of the monitored X.25 statistics for a particular interface. Information presented is the aggregated totals for all virtual circuits configured for the interface.</p>
	<p><b>[Show the X.25 Circuits] button</b></p> <p>Opens the X.25 Circuits applet which displays information on an existing, established virtual circuit. Virtual circuits that are not established are not displayed in this table. The detailed information about the circuit includes the Calling and Called DTE address - the source and destination of the call.</p>

## X.25 Administrative Table Overview applet

The **X.25 Administrative Table Overview** provides consolidated interface information including the timers, counters and call parameters. The device name and interface that is the source of the information is displayed in the top of the screen.



There are three sections to the X.25 Administrative Table OverView screen:

- General Information
- Timers
- Counters

The following general information is displayed at the top of the X.25 Administrative Table Overview screen:

Title	Definition
Interface Name	The name of the interface.
Interface Number	The interface number.
Description	The interface description defined in the Description applet for the interface.
Max Active Circuits	The number of active circuits supported.
Packet Sequencing	The type of packet sequencing in use (possible values are Modulo 8 or Modulo 128).
Local X.121 Address	The X.121 address assigned to this interface.
Number of PVCs	The number of Permanent Virtual Circuits configured. The PVCs use channel numbers from 1 to this number.
Interface Mode	Defines the mode of operation. Possible values are: <b>DTE: Data Terminal Equipment</b> <b>DCE: Data Circuit-terminating Equipment</b> <b>DXE: Indicates the mode will be determined by exchange identification.</b>
CCITT Version (Also referred to as ITU-T version.)	The version of X.25 supported.

The following information is displayed in the Timers section of the window.

Title	Definition
Restart timer (T20)	The time-out period in milliseconds for receiving a Restart confirmation.
Reset timer (T22)	The time-out period in milliseconds for receiving a Reset confirmation.

## Network Performance

Title	Definition
<b>Clear timer (T23)</b>	The time-out period in milliseconds for receiving a Clear confirmation.
<b>Data Retransmit timer (T25)</b>	<p>The time-out period in milliseconds that a transmitted frame can remain unacknowledged before the protocol translator polls for an acknowledgment.</p> <p>The retransmit timer setting should match that of the network.</p> <p>On leased-lines, this setting is very important. The timer setting must be long enough that a maximum-sized frame can complete a round-trip on the circuit. If the setting is too brief, acknowledgment polling will occur before the round-trip is completed, which will waste bandwidth. If the setting is too long, too much time will pass before the translator requests acknowledgment, which also reduced bandwidth.</p>
<b>Reject Retransmit timer (T27)</b>	The time-out period in milliseconds for receiving information after using a Reject.
<b>Registration Request timer (T28)</b>	The registration time-out period in milliseconds.
<b>Call timer (T21)</b>	The time-out period in milliseconds for receiving a Call Accepted packet.
<b>Window Status Transmit timer (T24)</b>	The windows status transmission timer in milliseconds.
<b>Interrupt time (T26)</b>	The interrupt time in milliseconds.
<b>Minimum Recall timer (T29)</b>	The minimum time between unsuccessful call attempts in milliseconds.

The following information is displayed in the Counters section of the window.

Title	Definition
<b>Restart Count (R20)</b>	The Restart retransmission count

---

Title	Definition
<b>Reset Count (R22)</b>	The Reset retransmission count
<b>Clear Count (R23)</b>	The Clear retransmission count
<b>Reject Count (R27)</b>	The Reject retransmission count
<b>Data Retransmit Count (R25)</b>	The Data retransmission count
<b>Register Request Count (R28)</b>	The Registration retransmission count

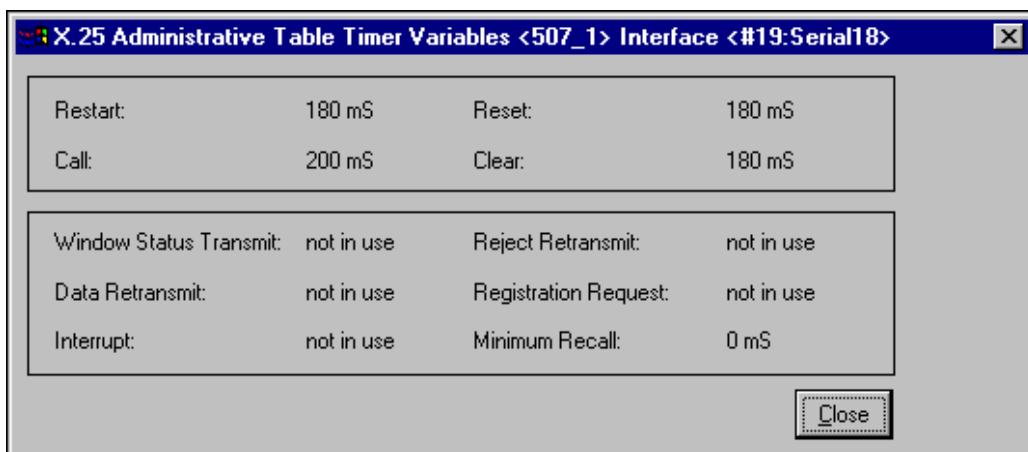
## Using the X.25 Administrative Table Overview applet

To start the X.25 Administrative Table Overview applet:

1. Open the X.25 Administrative Table applet.
2. Highlight an interface and click the [X.25 Overview] button. The applet opens and X.25 information appears.

## X.25 Administrative Table Timer Variables applet

The **X.25 Administrative Table Timer Variables** applet is launched from within the X.25 Administrative Table applet by selecting a row in the table and clicking on the [Timer Variables] button. It shows information specific to the timer variables.



The following information is displayed in the Timer Variables window.

Title	Definition
<b>Restart timer (T20)</b>	The time-out period in milliseconds for receiving a Restart confirmation.
<b>Reset timer (T22)</b>	The time-out period in milliseconds for receiving a Reset confirmation.
<b>Call timer (T21)</b>	The time-out period in milliseconds for receiving a Call Accepted packet.
<b>Clear timer (T23)</b>	The time-out period in milliseconds for receiving a Clear confirmation.
<b>Window Status Transmit timer (T24)</b>	The windows status transmission timer in milliseconds.

Title	Definition
<b>Data Retransmit timer (T25)</b>	<p>The time-out period in milliseconds that a transmitted frame can remain unacknowledged before the protocol translator polls for an acknowledgment.</p> <p>The retransmit timer setting should match that of the network.</p> <p>On leased-lines, this setting is very important. The timer setting must be long enough that a maximum-sized frame can complete a round-trip on the circuit. If the setting is too brief, acknowledgment polling will occur before the round-trip is completed, which will waste bandwidth. If the setting is too long, too much time will pass before the translator requests acknowledgment, which also reduced bandwidth.</p>
<b>Interrupt time (T26)</b>	The interrupt time in milliseconds.
<b>Reject Retransmit timer (T27)</b>	The time-out period in milliseconds for receiving information after using a Reject.
<b>Registration Request timer (T28)</b>	The registration time-out period in milliseconds.
<b>Minimum Recall timer (T29)</b>	The minimum time between unsuccessful call attempts in milliseconds.

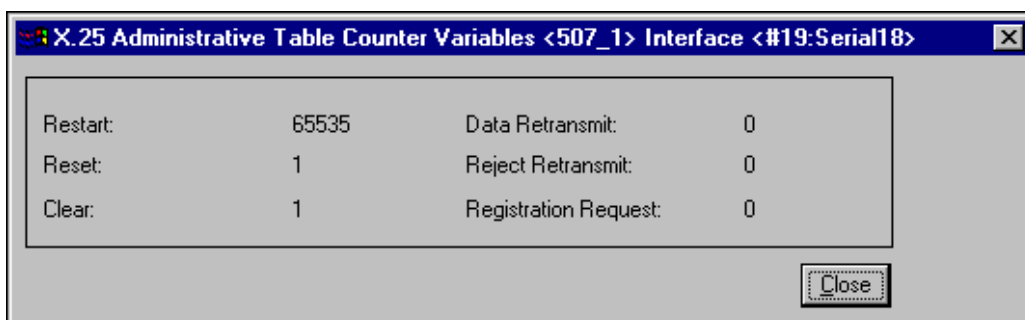
## Using the X.25 Administrative Table Timer Variables applet

**To start the X.25 Administrative Table Timer Variables applet:**

1. Open the X.25 Administrative Table applet.
2. Highlight an interface and click the [Timer Variables] button. The applet opens and X.25 timer variable information appears.

## X.25 Administrative Table Counter Variables applet

The **X.25 Administrative Table Counter Variables** applet is launched from within the X.25 Administrative Table applet by selecting a row in the table and clicking on the [Counter Variables] button. It shows information specific to the counter variables.



The following information is displayed in the Counter Variables window.

Title	Definition
<b>Restart Count (R20)</b>	The Restart retransmission count
<b>Reset Count (R22)</b>	The Reset retransmission count
<b>Clear Count (R23)</b>	The Clear retransmission count
<b>Data Retransmit Count (R25)</b>	The Data retransmission count
<b>Reject Count (R27)</b>	The Reject retransmission count
<b>Register Request Count (R28)</b>	The Registration retransmission count

## Using the X.25 Administrative Table Counter Variables applet

To start the **X.25 Administrative Table Counter Variables** applet:

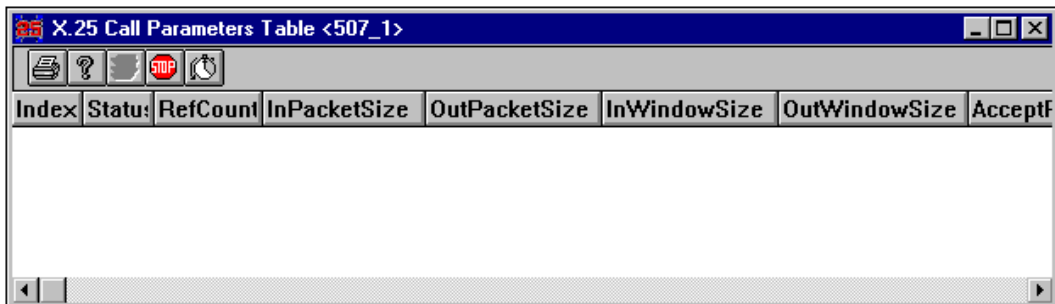
1. Open the X.25 Administrative Table applet.
2. Highlight an interface and click the [Counter Variables] button. The applet opens and X.25 timer counter information appears.

## X.25 Call Parameters Table applet

The **X.25 Call Parameters Table** applet is launched from within the X.25 Administrative Table applet or X.25 Operational Table applet by selecting a row in the table and clicking on the [Call Parameters] button. It shows information specific to Call Parameters.

Call Parameters are parameters which can be varied between X.25 calls. The table shows values for the call parameters only if they were manually defined to the router. Otherwise, this table is empty.

For Novell MPR Users: Please refer to the Novell MultiProtocol Router Administrators Guide for more details on configuring call parameters and for defining the call parameters headings.



The following information is displayed in the Call Parameters table.

Title	Definition
<b>Index</b>	A value that distinguishes one value from another in the Call Parameters table. Entries in this table are referenced by other objects.
<b>Status</b>	<p>The status of the Call Parameter entry. Possible values are:</p> <p><b>Valid</b> - the entry is configured.</p> <p><b>CreateRequest</b> - a request has been received to create an entry. Immediately upon completing the createRequest, the status switches to UnderCreation.</p> <p><b>UnderCreation</b> - entries remain in this state until the entry configuration is complete, at which time the entry becomes valid,</p>

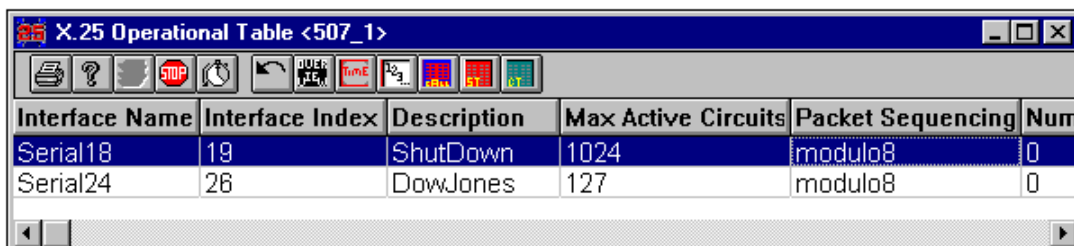
## Network Performance

Title	Definition
	or until the creation process aborts, and the entry becomes invalid. <b>Invalid</b> - indicates the entire entry is invalid, that is, it disassociates the mapping associated with the entry.
RefCount	The number of references know to exist to this set of call parameters. This is the number of other objects that have returned a value of, and will return a value of, the Index for this set of call parameters.
InPacketSize	The maximum receive packet size in octets for a circuit.
OutPacketSize	The maximum transmit packet size in octets for a circuit.
InWindowSize	The receive window size for a circuit.
OutWindowSize	The transmit window size for a circuit.
AcceptReverse Charging	Indicates if reverse charges are refused or accepted. Possible values are Default, Accept, Refuse and NeverAccept.

## X.25 Operational Table applet

The **X.25 Operational Table** applet displays the current X.25 operating parameters. These values reflect changes in the X.25 configuration made after the system was started.

The Operational Table displays the basic X.25 configuration data. It provides toolbar access to detailed configuration information.



Interface Name	Interface Index	Description	Max Active Circuits	Packet Sequencing	Num
Serial18	19	ShutDown	1024	modulo8	0
Serial24	26	DowJones	127	modulo8	0

---

The X.25 Operational Table headings include:

Heading	Definition
Interface Name	The name of the interface.
Interface Index	The interface number.
Description	The interface description defined in the Description applet for the interface.
Max Active Circuits	The number of active circuits supported.
Packet Sequencing	The type of packet sequencing in use (possible values are Modulo 8 or Modulo 128).
Number of PVCs	The number of Permanent Virtual Circuits configured.
X.121 Address	The X.121 address assigned to this interface.
CCITT Version (Also referred to as ITU-T version.)	The version of X.25 supported.








## Using the X.25 Operational Table applet

**To start the X.25 Operational Table applet:**

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose X.25 > Operational Table. From the application view, right-click the X.25 icon and choose Operational Table.
3. Choose the applet parameters and click OK. The applet opens and X.25 configuration information appears.

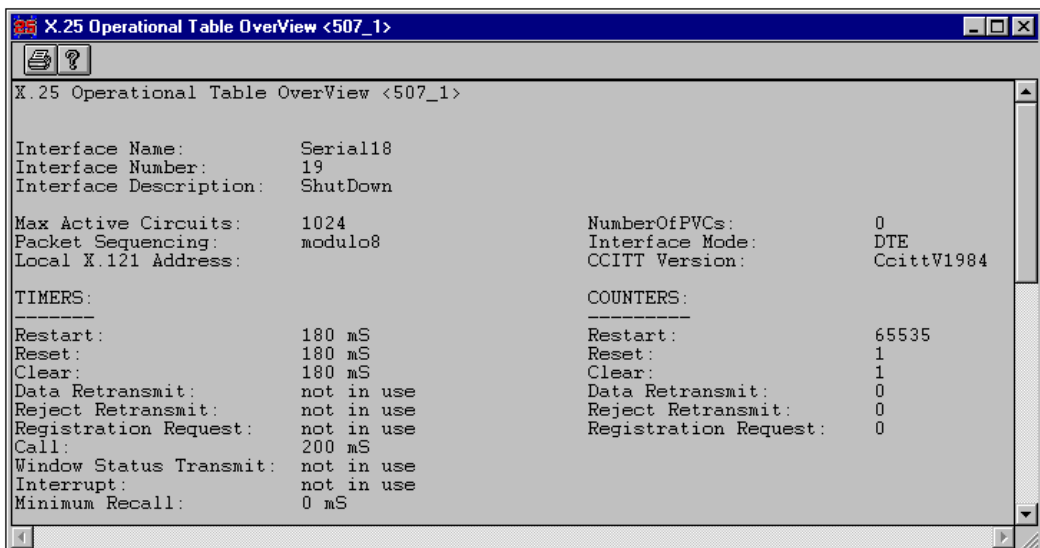
## Network Performance

In addition to the global toolbar buttons, there are seven specialized buttons on the right-hand side of the X.25 Operational Table toolbar.

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.
	<b>[X.25 Overview] button</b> Opens the X.25 Operational Table Overview applet for a selected row. Displays consolidated interface information.
	<b>[Show the Timer Variables] button</b> Opens the X.25 Operational Table Timer Variables applet for a selected row. Displays timer information, such as restart, reset and clear times.
	<b>[Show the Counter Variables] button</b> Opens the X.25 Operational Table Counter Variables applet for the selected row. Displays counter information, such as restart count, reset count, etc.
	<b>[Show the Call Parameters Table] button</b> Opens the X.25 Call Parameters Table applet which for the selected row. Displays call parameter information, such as status, in and out packet size, etc.
	<b>[Show the X.25 Statistics] button</b> Opens the X.25 Statistics applet which displays the values of the monitored X.25 statistics for a particular interface. Information presented is the aggregated totals for all virtual circuits configured for the interface.
	<b>[Show the X.25 Circuits] button</b> Opens the X.25 Circuits applet which displays information on an existing, established virtual circuit. Virtual circuits that are not established are not displayed in this table. The detailed information about the circuit includes the Calling and Called DTE address - the source and destination of the call.

## X.25 Operational Table Overview applet

The **X.25 Operational Table Overview** provides consolidated interface information including the timers, counters and call parameters. The device name and interface that is the source of the information is displayed in the top of the screen.



There are three sections to the X.25 Operational Table OverView screen:

- General Information
- Timers
- Counters

The following general information is displayed at the top of the X.25 Operational Table Overview screen:

Title	Definition
Interface Name	The name of the interface.
Interface Number	The interface number.

## Network Performance

---

Title	Definition
<b>Description</b>	The interface description defined in the Description applet for the interface.
<b>Max Active Circuits</b>	The number of active circuits supported.
<b>Packet Sequencing</b>	The type of packet sequencing in use (possible values are Modulo 8 or Modulo 128).
<b>Local X.121 Address</b>	The X.121 address assigned to this interface.
<b>Number of PVCs</b>	The number of Permanent Virtual Circuits configured. The PVCs use channel numbers from 1 to this number.
<b>Interface Mode</b>	Defines the mode of operation. Possible values are: <b>DTE:</b> Data Terminal Equipment <b>DCE:</b> Data Circuit-terminating Equipment <b>DXE:</b> Indicates the mode will be determined by exchange identification.
<b>CCITT Version (Also referred to as ITU-T version.)</b>	The version of X.25 supported.

The following information is displayed in the Timers section of the window.

Title	Definition
<b>Restart timer (T20)</b>	The time-out period in milliseconds for receiving a Restart confirmation.
<b>Reset timer (T22)</b>	The time-out period in milliseconds for receiving a Reset confirmation.
<b>Clear timer (T23)</b>	The time-out period in milliseconds for receiving a Clear confirmation.

Title	Definition
<b>Data Retransmit timer (T25)</b>	<p>The time-out period in milliseconds that a transmitted frame can remain unacknowledged before the protocol translator polls for an acknowledgment.</p> <p>The retransmit timer setting should match that of the network.</p> <p>On leased-lines, this setting is very important. The timer setting must be long enough that a maximum-sized frame can complete a round-trip on the circuit. If the setting is too brief, acknowledgment polling will occur before the round-trip is completed, which will waste bandwidth. If the setting is too long, too much time will pass before the translator requests acknowledgment, which also reduced bandwidth.</p>
<b>Reject Retransmit timer (T27)</b>	The time-out period in milliseconds for receiving information after using a Reject.
<b>Registration Request timer (T28)</b>	The registration time-out period in milliseconds.
<b>Call timer (T21)</b>	The time-out period in milliseconds for receiving a Call Accepted packet.
<b>Window Status Transmit timer (T24)</b>	The windows status transmission timer in milliseconds.
<b>Interrupt time (T26)</b>	The interrupt time in milliseconds.
<b>Minimum Recall timer (T29)</b>	The minimum time between unsuccessful call attempts in milliseconds.

The following information is displayed in the Counters section of the window.

Title	Definition
<b>Restart Count (R20)</b>	The Restart retransmission count
<b>Reset Count (R22)</b>	The Reset retransmission count
<b>Clear Count (R23)</b>	The Clear retransmission count

Title	Definition
Reject Count (R27)	The Reject retransmission count
Data Retransmit Count (R25)	The Data retransmission count
Register Request Count (R28)	The Registration retransmission count

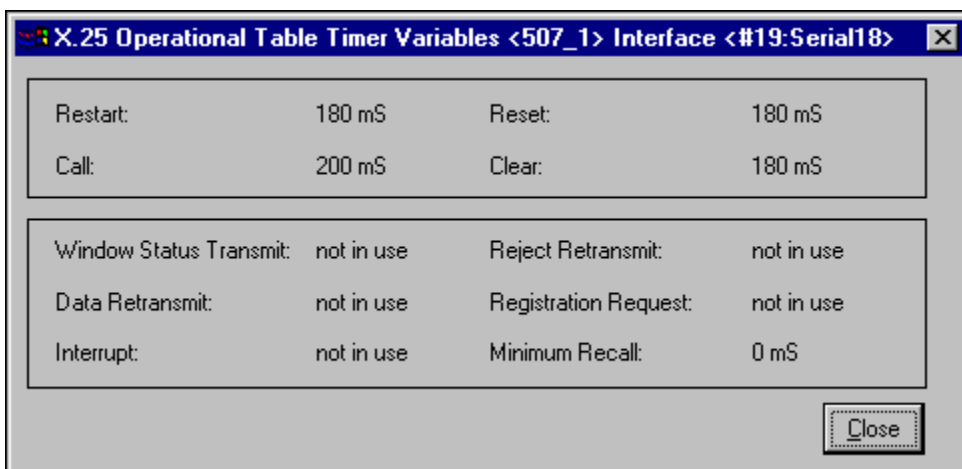
### Using the X.25 Operational Table Overview applet

To start the X.25 Operational Table Overview applet:

1. Open the X.25 Operational Table applet.
2. Highlight an interface and click the [X.25 Overview] button. The applet opens and X.25 information appears.

### X.25 Operational Table Timer Variables applet

The **X.25 Operational Table Timer Variables** applet is launched from within the X.25 Operational Table applet by selecting a row in the table and clicking on the [Timer Variables] button. It shows information specific to the timer variables.



The following information is displayed in the Timer Variables window.

Title	Definition
<b>Restart timer (T20)</b>	The time-out period in milliseconds for receiving a Restart confirmation.
<b>Reset timer (T22)</b>	The time-out period in milliseconds for receiving a Reset confirmation.
<b>Call timer (T21)</b>	The time-out period in milliseconds for receiving a Call Accepted packet.
<b>Clear timer (T23)</b>	The time-out period in milliseconds for receiving a Clear confirmation.
<b>Window Status Transmit timer (T24)</b>	The windows status transmission timer in milliseconds.
<b>Data Retransmit timer (T25)</b>	<p>The time-out period in milliseconds that a transmitted frame can remain unacknowledged before the protocol translator polls for an acknowledgment.</p> <p>The retransmit timer setting should match that of the network.</p> <p>On leased-lines, this setting is very important. The timer setting must be long enough that a maximum-sized frame can complete a round-trip on the circuit. If the setting is too brief, acknowledgment polling will occur before the round-trip is completed, which will waste bandwidth. If the setting is too long, too much time will pass before the translator requests acknowledgment, which also reduced bandwidth.</p>
<b>Interrupt time (T26)</b>	The interrupt time in milliseconds.
<b>Reject Retransmit timer (T27)</b>	The time-out period in milliseconds for receiving information after using a Reject.
<b>Registration Request timer (T28)</b>	The registration time-out period in milliseconds.

Title	Definition
Minimum Recall timer (T29)	The minimum time between unsuccessful call attempts in milliseconds.

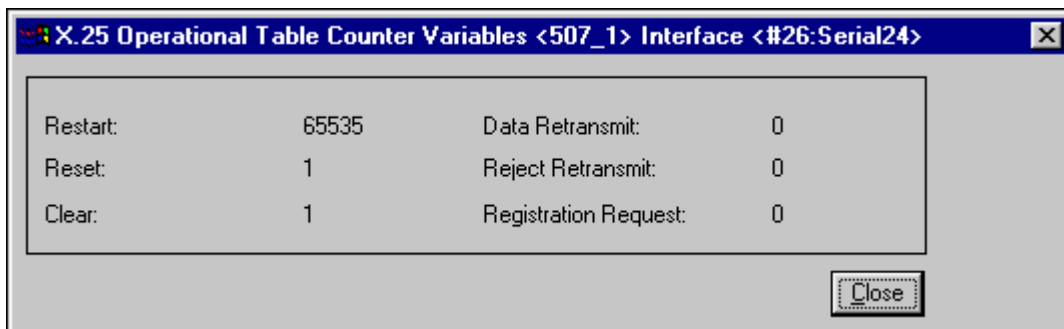
### Using the X.25 Operational Table Timer Variables applet

To start the X.25 Operational Table Timer Variables applet:

1. Open the X.25 Operational Table applet.
2. Highlight an interface and click the [Timer Variables] button. The applet opens and X.25 timer variable information appears.

### X.25 Operational Table Counter Variables applet

The **X.25 Operational Table Counter Variables** applet is launched from within the X.25 Operational Table applet by selecting a row in the table and clicking on the [Counter Variables] button. It shows information specific to the counter variables.



The following information is displayed in the Counter Variables window.

Title	Definition
Restart Count (R20)	The Restart retransmission count
Reset Count (R22)	The Reset retransmission count
Clear Count (R23)	The Clear retransmission count

Title	Definition
<b>Data Retransmit Count (R25)</b>	The Data retransmission count
<b>Reject Count (R27)</b>	The Reject retransmission count
<b>Register Request Count (R28)</b>	The Registration retransmission count

## Using the X.25 Operational Table Counter Variables applet

To start the X.25 Operational Table Counter Variables applet:

1. Open the X.25 Operational Table applet.
2. Highlight an interface and click the [Counter Variables] button. The applet opens and X.25 timer counter information appears.

### **Bridging tools**

Bridging tools are available for all routers that support bridging. Available tools are:

- **The Learned Bridging applet**  
Provides detailed information on bridging, including MAC address, number of ports, root information and more.
- **The Spanning Tree Port Table applet**  
Displays Spanning Tree protocol information, such as interface name and index, state, path cost, root ID, etc.
- **The Static Bridging Table applet**  
Provides information for static bridge entries, such as Interface name and index, receive port and status.
- **The Base Port Table applet**  
Displays bridge management information, such as port, interface name and index, delay exceeded discards, etc.
- **The Source Route Bridging applet**  
Provides details on source routing bridging, including MAC address, number of ports, Spanning Tree Explorer information and more.
- **The Static Bridging Table, source route**  
Provides information for static bridge entries in the Source Route table, such as Interface name and index, receive port and status.
- **The Bridge Telnet Show Commands applet: Cisco specific**  
Provides Telnet show commands for Cisco routers.

## The Learned Bridging applet

The **Learned Bridging** applet provides detailed information on bridging, including MAC address, number of ports, root information and more.

**Learned Bridging <Bart>**

**Bridge Configuration**

Address: AA0004000308      Type: srl(4)      No. of Ports: 2  
 Learned Entry Discards: 0      Aging Time: 300

**Spanning Tree Configuration**

Specification: ieee8021d(3)      Designed Root: 8000AA0004000308  
 Bridge Max Age: 2000      Priority: 32768  
 Root Cost: 0      Bridge Hello Time: 200  
 Time Since Topology Changes: 0 Days, 0 Hrs, 0 Mins      Root Port: 0  
 Bridge Forward Delay: 1500      Topology Changes: 2  
 Max Age: 2000      Hold Time: 200  
 Forward Delay: 1500      Hello Time: 100

Port	Interface In	Interface Name	Address	Status
1	1	eth0/net0 SCC Ethernet	00001B33A7F3	learned
1	1	eth0/net0 SCC Ethernet	00609771A526	learned
1	1	eth0/net0 SCC Ethernet	006097791070	learned
1	1	eth0/net0 SCC Ethernet	00609779529E	learned
1	1	eth0/net0 SCC Ethernet	0060977952AF	learned
1	1	eth0/net0 SCC Ethernet	0060977952B9	learned
1	1	eth0/net0 SCC Ethernet	0060977952C1	learned
1	1	eth0/net0 SCC Ethernet	0060977952C8	learned
1	1	eth0/net0 SCC Ethernet	006097A87684	learned
1	1	eth0/net0 SCC Ethernet	00AA005FE424	learned
1	1	eth0/net0 SCC Ethernet	00AA00D30020	learned
1	1	eth0/net0 SCC Ethernet	080002040BDE	learned
1	1	eth0/net0 SCC Ethernet	0800170415A3	learned
1	1	eth0/net0 SCC Ethernet	0800170415B0	learned

The top of the screen is divided into two sections: **Bridge Configuration** and **Spanning Tree Configuration**.

## Network Performance

---

The Bridge Configuration includes the following information:

Field Name	Description
<b>Address</b>	The MAC address used by this bridge when it must be referred to in a unique fashion.
<b>No. of Ports</b>	The total number of ports.
<b>Aging Timer</b>	The value that all bridges use for MaxAge when this bridge is acting as the root.
<b>Type</b>	Indicates what type of bridging this bridge can perform.
<b>Learned Entry Discards</b>	The total number of Forwarding Database entries, which have been or would have been learned, but have been discarded due to a lack of space to store them in the Forwarding Database.

Spanning Tree Configuration includes the following information:

Field Name	Description
<b>Specification</b>	An indication of what version of the Spanning Tree Protocol is being run.
<b>Designed Root</b>	The bridge identifier of the root of the spanning tree.
<b>Bridge Max Age</b>	The value that all bridges use for MaxAge when this bridge is acting as the root..
<b>Priority</b>	The value of the write-able portion of the Bridge ID.
<b>Root Cost</b>	The cost of the path to the root as seen from this bridge.
<b>Bridge Hello Time</b>	The value that all bridges use for HelloTime when this bridge is acting as the root.
<b>Time Since Topology Changes</b>	The time (in hundredths of a second) since the last time a topology change was detected by the bridge entity.

Field Name	Description
<b>Root Port</b>	The port number of the port which offers the lowest cost path from this bridge to the root bridge.
<b>Bridge Forward Delay</b>	The value that all bridges use for ForwardDelay when this bridge is acting as the root.
<b>Topology Changes</b>	The total number of topology changes detected by this bridge.
<b>Max Age</b>	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded.
<b>Hold Time</b>	This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node.
<b>Forward Delay</b>	The value determines how long the port stays in a particular state before moving to the next state. For example, how long a port stays in the Listening state when moving from Blocking to Learning.
<b>Hello Time</b>	The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so.

In the lower half of the screen is the **Learned Bridging table**. The Learned Bridging table includes the following fields:

Field Name	Description
<b>Port</b>	The port number this MAC address was learned from.
<b>Interface Index</b>	The interface number on which the station was learned. If this number is 0, then the learning bridge has not discovered which interface the station is accessible on.

Field Name	Description
Interface Name	The name of the circuit group of this interface.
Address	The MAC-level address of the station described by this entry in the table.
Status	<p>The Status of this entry. Possible values are:</p> <p><b>invalid</b> This entry is no longer valid (e.g., it was learned but has since aged-out), but has not yet been flushed from the table</p> <p><b>learned</b> The entry was dynamically learned and is being used.</p> <p><b>Self</b> The entry represents one of the bridge's addresses</p> <p><b>mgmt</b> This is a statically configured entry.</p> <p><b>Other</b> None of the above.</p>





## Using the Learned Bridging applet

To start the Learned Bridging applet:

1. Right-click on a device icon and select **Boxmap**.
2. From the physical view, right-click on a blank area in the window and choose **Bridge > Learned Bridging**. From the application view, right-click on the Bridge icon and select **Learned Bridging**.
3. Choose the applet parameters and click OK. The applet opens and Bridging statistics will begin to appear in the window, based on the polling interval.

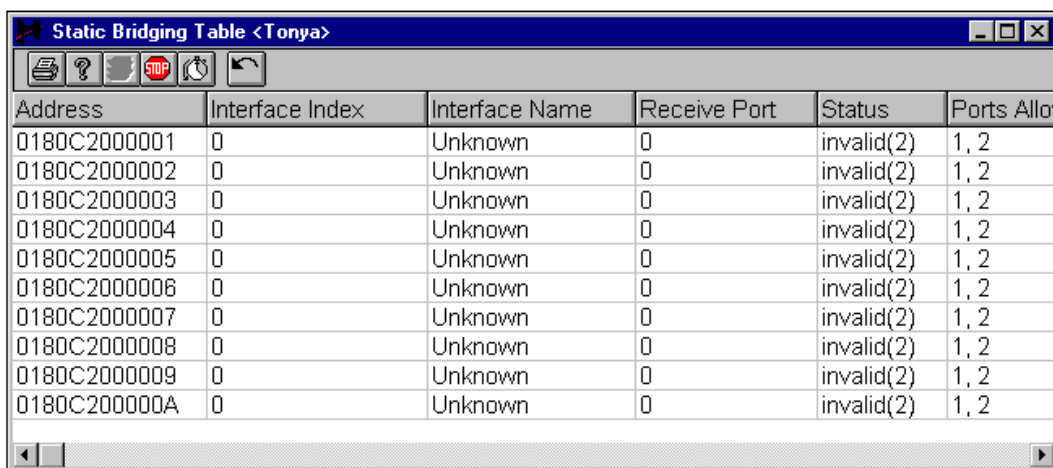
### Other buttons

In addition to the global toolbar buttons, the Learned Bridging applet has four specialized buttons on the right hand side of the toolbar:

Button	Description
	<b>[Static Bridging Table] button</b> Opens the Static Bridging Table which provides information for static bridge entries, such as Interface name and index, receive port and status.
	<b>[Spanning Tree Port Table] button</b> Launches the Spanning Tree Port Table applet which displays Spanning Tree protocol information, such as interface name and index, state, path cost, root ID, etc.
	<b>[Base Port Table] button</b> Launches the Base Port Table applet which displays bridge management information, such as port, interface name and index, delay exceeded discards, etc.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The Static Bridging Table

The Static Bridging Table is launched from the [Static Bridging Table] button in the Learned Bridging applet.




Address	Interface Index	Interface Name	Receive Port	Status	Ports Allowed
0180C2000001	0	Unknown	0	invalid(2)	1, 2
0180C2000002	0	Unknown	0	invalid(2)	1, 2
0180C2000003	0	Unknown	0	invalid(2)	1, 2
0180C2000004	0	Unknown	0	invalid(2)	1, 2
0180C2000005	0	Unknown	0	invalid(2)	1, 2
0180C2000006	0	Unknown	0	invalid(2)	1, 2
0180C2000007	0	Unknown	0	invalid(2)	1, 2
0180C2000008	0	Unknown	0	invalid(2)	1, 2
0180C2000009	0	Unknown	0	invalid(2)	1, 2
0180C200000A	0	Unknown	0	invalid(2)	1, 2

The Static Bridging Table contains the following information:

Field Name	Definition
Address	The MAC Address of this static bridge entry.
Interface Index	The interface number of this static bridge entry.
Interface Name	The interface name of this static bridge entry.
Receive Port	The port number of the port a frame MUST be received on, or 0 for all ports.
Status	The current status of the entry
Ports Allowed to Go	The set of ports to which frames received from a specific port and destined for a specific MAC address, are allowed to be forwarded

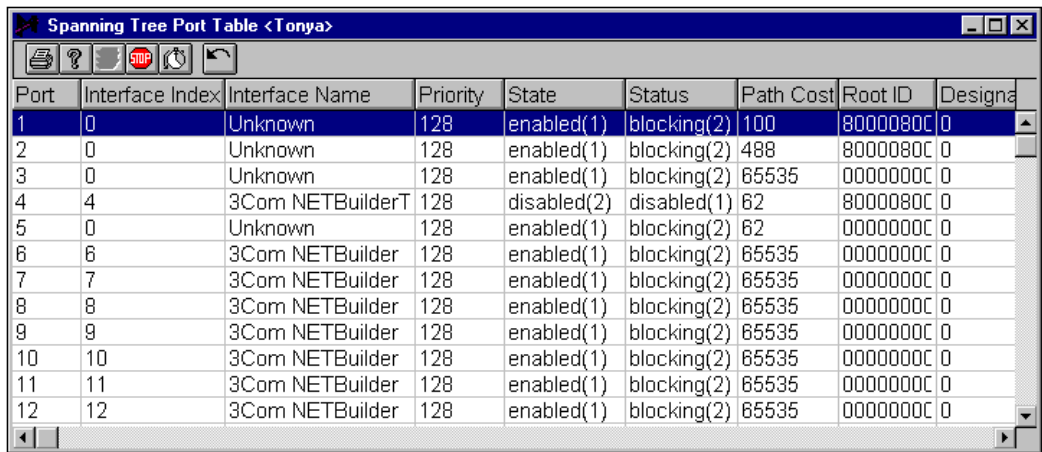
### Other buttons

In addition to the global toolbar buttons, the Static Bridging Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The Spanning Tree Port Table

The Spanning Tree Port Table is launched from the [Spanning Tree Port Table] button in the Learned Bridging applet.



The screenshot shows a window titled "Spanning Tree Port Table <Tonya>". It contains a table with the following data:

Port	Interface Index	Interface Name	Priority	State	Status	Path Cost	Root ID	Designa
1	0	Unknown	128	enabled(1)	blocking(2)	100	8000080C	0
2	0	Unknown	128	enabled(1)	blocking(2)	488	8000080C	0
3	0	Unknown	128	enabled(1)	blocking(2)	85535	0000000C	0
4	4	3Com NETBuilderT	128	disabled(2)	disabled(1)	82	8000080C	0
5	0	Unknown	128	enabled(1)	blocking(2)	82	0000000C	0
6	6	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0
7	7	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0
8	8	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0
9	9	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0
10	10	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0
11	11	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0
12	12	3Com NETBuilder	128	enabled(1)	blocking(2)	85535	0000000C	0


The Spanning Tree Port Table contains the following information:

Field Name	Definition
Port	The port number for which this entry contains Spanning Tree Protocol management.
Interface Index	The routers interface where the bridge port resides.
Interface Name	The interface name where this bridge port resides.
Priority	The priority field contained in the first octet of the Port ID.
State	The ports current state.
Status	The ports current status, Enabled or Disabled.
Path Cost	The total path cost towards the spanning tree root.
Root ID	The Bridge Identifier of the root bridge.
Designated Port	The path cost of the designated port.

Field Name	Definition
Cost	
Designated Bridge	The next bridge accessible from this port.
Designated Port	The port identifier of the designated bridge.
Forward Transition	The number of times this port has transitioned from the learning state to the forwarding state.

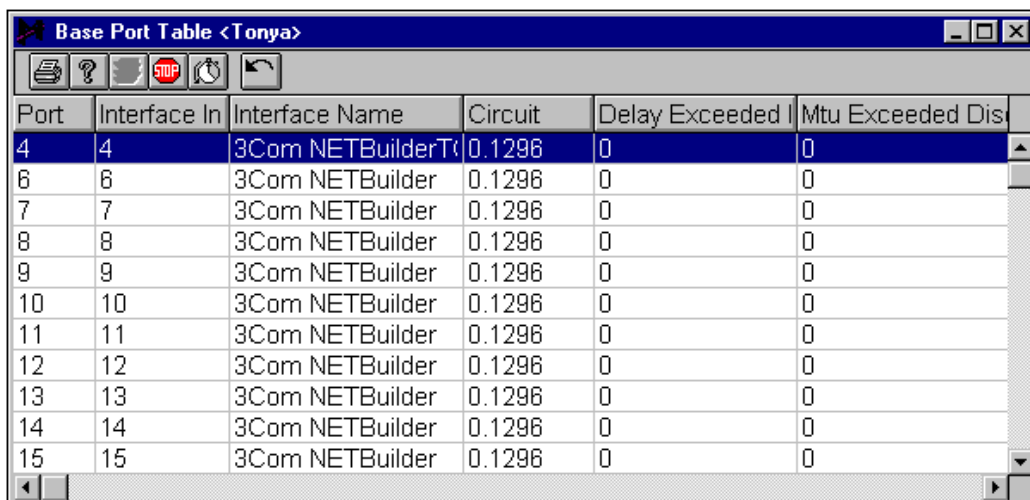
#### Other buttons

In addition to the global toolbar buttons, the Spanning Tree Port Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The Base Port Table

The Base Port Table is launched from the [Base Port Table] button in the Learned Bridging applet.



Port	Interface Index	Interface Name	Circuit	Delay Exceeded	Mtu Exceeded	Discards
4	4	3Com NETBuilderT	0.1296	0	0	
6	6	3Com NETBuilder	0.1296	0	0	
7	7	3Com NETBuilder	0.1296	0	0	
8	8	3Com NETBuilder	0.1296	0	0	
9	9	3Com NETBuilder	0.1296	0	0	
10	10	3Com NETBuilder	0.1296	0	0	
11	11	3Com NETBuilder	0.1296	0	0	
12	12	3Com NETBuilder	0.1296	0	0	
13	13	3Com NETBuilder	0.1296	0	0	
14	14	3Com NETBuilder	0.1296	0	0	
15	15	3Com NETBuilder	0.1296	0	0	


The Base Port Table contains the following information:

Field Name	Definition
<b>Port</b>	The port number for which this entry contains bridge management information.
<b>Interface Index</b>	The router's interface where the bridge port resides.
<b>Interface Name</b>	The interface name where this bridge port resides.
<b>Circuit</b>	A Unique object Instance for entries with a duplicate Interface Index. Value is 00 otherwise.
<b>Delay Exceeded Discards</b>	The number of frames discarded due to excessive transit delays through this bridge.
<b>Mtu Exceeded</b>	The number of frames discarded due to excessive size.

Field Name	Definition
Discards	

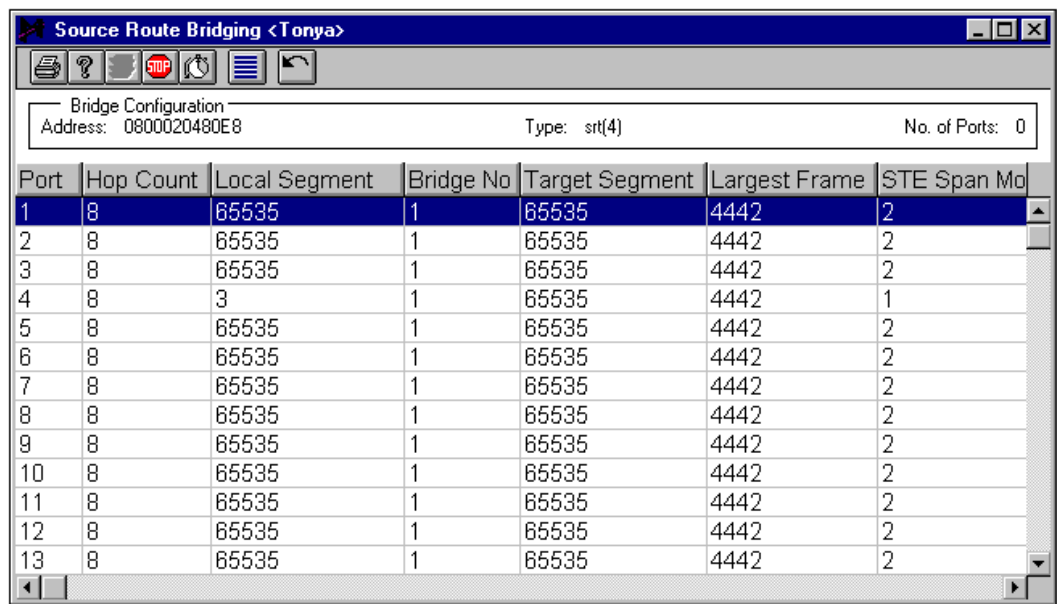
#### Other buttons

In addition to the global toolbar buttons, the Base Port Table applet has one specialized button on the right hand side of the toolbar:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

The Source Route Bridging applet

The **Source Route Bridging** applet provides details on source routing bridging, including MAC address, number of ports, Spanning Tree Explorer information and more.



The Bridge Configuration information in the top panel includes:

Field Name	Definition
Address	The MAC address used by this bridge when it must be referred to in a unique fashion.
Type	Indicates what type of bridging this bridge can perform. If a bridge is actually performing a certain type of bridging this will be indicated by entries in the port table for the given type.
No. of Ports	The number of ports controlled by this bridging entity.

The Source Route Bridging table includes the following information:

Field Name	Definition
<b>Port</b>	The port of the source routing bridge.
<b>Hop Count</b>	The maximum number of routing descriptors allowed in an All Paths or Spanning Tree Explorer frame.
<b>Local Segment</b>	The segment number which uniquely identifies the segment where this port is connected.
<b>Bridge No.</b>	The unique bridge number which identifies a bridge, when more than one bridge is used to span the same two segments.
<b>Target Segment</b>	The segment number of the target segment.
<b>Largest Frame</b>	The maximum size of the INFO field that this port can send/receive.
<b>STE Span Mode</b>	Determines how this port behaves when presented with a Spanning Tree Explorer frame. The value 'disabled(2)' indicates that the port will not accept or send Spanning Tree Explorer packets; any STE packets received will be silently discarded. The value 'forced(3)' indicates the port will always accept and propagate Spanning Tree Explorer frames.
<b>Spec In Frames</b>	The number of specifically routed frames that have been received from this port's segment.
<b>Spec Out Frames</b>	The number of specifically routed frames that this port has transmitted on its segment.
<b>Ape In Frames</b>	The number of path explorer frames that have been received by this port from its segment.
<b>Ape Out Frames</b>	The number of path explorer frames that have been transmitted by this port on its segment.
<b>Ste In Frames</b>	The number of spanning tree explorer frames that have been received by this port from its segment.
<b>Ste Out Frames</b>	The number of spanning tree explorer frames that have been transmitted by this port on its segment.
<b>Segment Mismatch Discards</b>	The number of explorer frames that have been discarded by this port, because the routing descriptor field contained an invalid

Field Name	Definition
	adjacent segment value.
<b>Duplicate Segment Discards</b>	The number of frames that have been discarded by this port, because the routing descriptor field contained a duplicate segment identifier.
<b>Hop Count Exceeded Discards</b>	The number of explorer frames that have been discarded by this port, because the Routing Information Field has exceeded the maximum route descriptor length.



## Using the Source Route Bridging applet

### To start the Source Route Bridging applet:

1. Right-click on a device icon and select Boxmap.
2. From the physical view, right-click on a blank area in the window and choose Bridge > Source Route Bridging. From the application view, right-click on the Bridge icon and select Source Route Bridging.
3. Choose the applet parameters and click OK. The applet opens and Bridging statistics will begin to appear in the window, based on the polling interval.

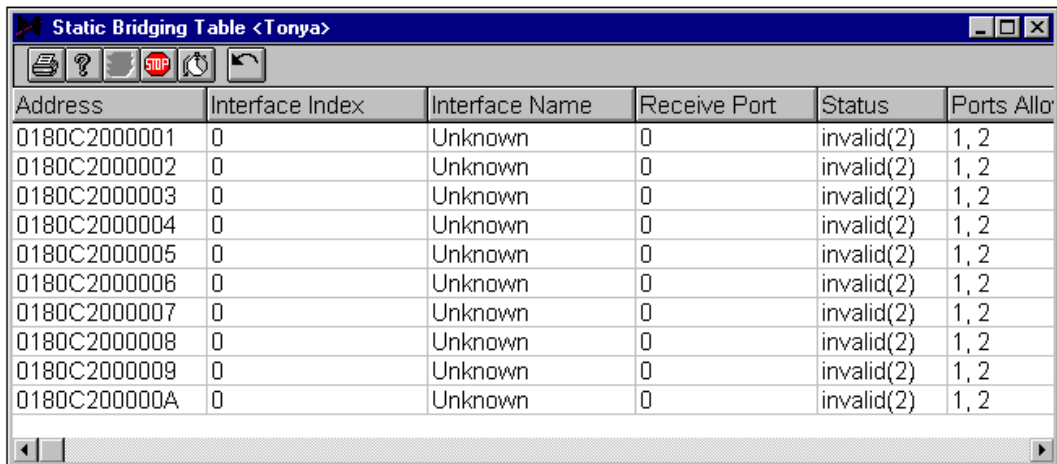
### Other buttons

In addition to the global toolbar buttons, the Learned Bridging applet has four specialized buttons on the right hand side of the toolbar:

Button	Description
	<b>[Static Bridging Table] button</b> Opens the Static Bridging Table source route applet.
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

## The Static Bridging Table, source route

The Static Bridging Table is launched from the [Static Bridging Table] button in the Source Route Bridging applet.



Address	Interface Index	Interface Name	Receive Port	Status	Ports Allowed
0180C2000001	0	Unknown	0	invalid(2)	1, 2
0180C2000002	0	Unknown	0	invalid(2)	1, 2
0180C2000003	0	Unknown	0	invalid(2)	1, 2
0180C2000004	0	Unknown	0	invalid(2)	1, 2
0180C2000005	0	Unknown	0	invalid(2)	1, 2
0180C2000006	0	Unknown	0	invalid(2)	1, 2
0180C2000007	0	Unknown	0	invalid(2)	1, 2
0180C2000008	0	Unknown	0	invalid(2)	1, 2
0180C2000009	0	Unknown	0	invalid(2)	1, 2
0180C200000A	0	Unknown	0	invalid(2)	1, 2

The Static Bridging Table contains the following information:

Field Name	Definition
<b>Address</b>	The destination MAC address in a frame to which this entry's filtering information applies.
<b>Interface Index</b>	The interface number where this port lies.
<b>Interface Name</b>	The interface name where this port lies.
<b>Receive Port</b>	Either the value '0', or the port number of the port from which a frame must be received in order for this entry's filtering information to apply.
<b>Status</b>	This object indicates the status of this entry--(other(1) - this entry is currently in use but the conditions under which it will remain so are different from each of the following values) (invalid(2) - writing this value to the object removes the corresponding entry) (permanent(3) - this entry is currently in use and will remain so after the next reset of the bridge) (deleteOnReset(4) - this entry is

## Network Performance

---

Field Name	Definition
	currently in use and will remain so until the next reset of the bridge) (deleteOnTimeout(5) - this entry is currently in use and will remain so until it is aged out)
<b>Ports Allowed to Go</b>	The set of ports to which frames received from a specific port and destined for a specific MAC address, are allowed to be forwarded.

## The Bridge Telnet Show Commands applet: Cisco specific

### For Cisco Only

Right-click the Bridge icon and select **Telnet Show Commands** to provide the show commands menu options. Show commands available will vary considerably based on the router manufacturer and version of software running on the router.

## Port applet: for DEC Gigaswitch

### Port applets: overview

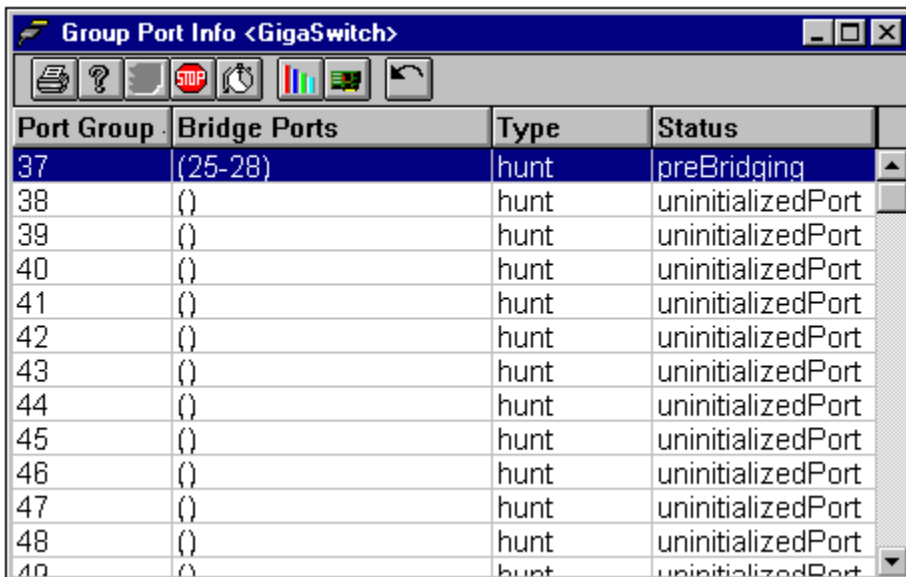
Port applets provide information about port groups for the Digital Equipment Gigaswitch.

Available applications are:

- **The Group Port Info applet**  
Lists all port groups assigned to the Gigaswitch.
- **The Port Utilization applet**  
Shows the utilization statistics for the selected port. (exponentially decayed) calculated by the Digital Equipment Gigaswitch.

### The Group Port Info applet

The Group Port Info applet lists all port groups assigned for the Digital Equipment Gigaswitch. The applet is launched from the Port icon in the Boxmap.



Port Group	Bridge Ports	Type	Status
37	(25-28)	hunt	preBridging
38	()	hunt	uninitializedPort
39	()	hunt	uninitializedPort
40	()	hunt	uninitializedPort
41	()	hunt	uninitializedPort
42	()	hunt	uninitializedPort
43	()	hunt	uninitializedPort
44	()	hunt	uninitializedPort
45	()	hunt	uninitializedPort
46	()	hunt	uninitializedPort
47	()	hunt	uninitializedPort
48	()	hunt	uninitializedPort
49	()	hunt	uninitializedPort

## Network Performance



---

The Group Port Info Table contains the following information:

Field Name	Definition
<b>Port Group</b>	The number of the port group. This will be a number between 37 and 64.
<b>Bridge Ports</b>	These are the bridge ports that are joined together into the Port Group. Bridge Ports are numbered between 1 and 36. A bridge port becoming a member of a port group ceases to operate as a normal bridge port, therefore filters on the port have no effect.
<b>Type</b>	<p>There are two Port Group types:</p> <p><b>Hunt Group</b> - all members of a hunt group work like a single bridge port as far as bridge functions are concerned.</p> <p><b>Reliability Group</b> - Only a single port in a reliability group is operational. All other ports are considered backup. When the operational port fails, a backup port will be selected to become operational.</p>
<b>Status</b>	<p>There are three status indications:</p> <p><b>Uninitialized Port</b> - This port has no member in it, is not powered on, or no ports in the group have successfully completed startup diagnostics.</p> <p><b>PreBridging</b> - Some ports in the port group have been initialized with the bridge functions, but no port is yet functioning as part of a bridge port. This is always the case if the datalink is not up.</p> <p><b>Bridging</b> - At least one port in the port group is functioning as part of a bridge port. The port group must be in this state to carry user data.</p>

### Other buttons

In addition to the global toolbar buttons, the Group Port Info applet has the following specialized buttons.

Button	Definition
	<b>[Top Ten Talkers] button</b> Opens the Top Ten Talkers applet which lists the ten busiest interfaces on the device.
	<b>[Port Utilization] button</b> Opens the Port Utilization applet which shows utilization statistics for the selected port.

## The Port Utilization applet

The Port Utilization applet shows the utilization statistics for the selected port. (exponentially decayed) calculated by the Digital Equipment Gigaswitch.

The applet is launched by clicking the [Port Utilization] button in the Group Port Info applet. The data is updated on the screen based on the Polling Interval.

### Other buttons

The Port Utilization applet uses the global toolbar buttons.

## Network Performance

---

# Accounting Applets: Bytes and packets

14

## Accounting applets

The Accounting applets provide information about the number of bytes and packets exchanged between two end stations over the IP or IPX protocols.

There are two accounting applets:

- IP Accounting applet
- IPX Accounting applet

### **To launch the accounting applets:**

1. Right-click on a device icon and choose Boxmap.
2. From the physical view, select **Accounting > IP Accounting** or **Accounting > IPX Accounting**. From the application view, right-click on the Accounting icon and select the appropriate applet.

Data is updated on the screen based on the polling interval.

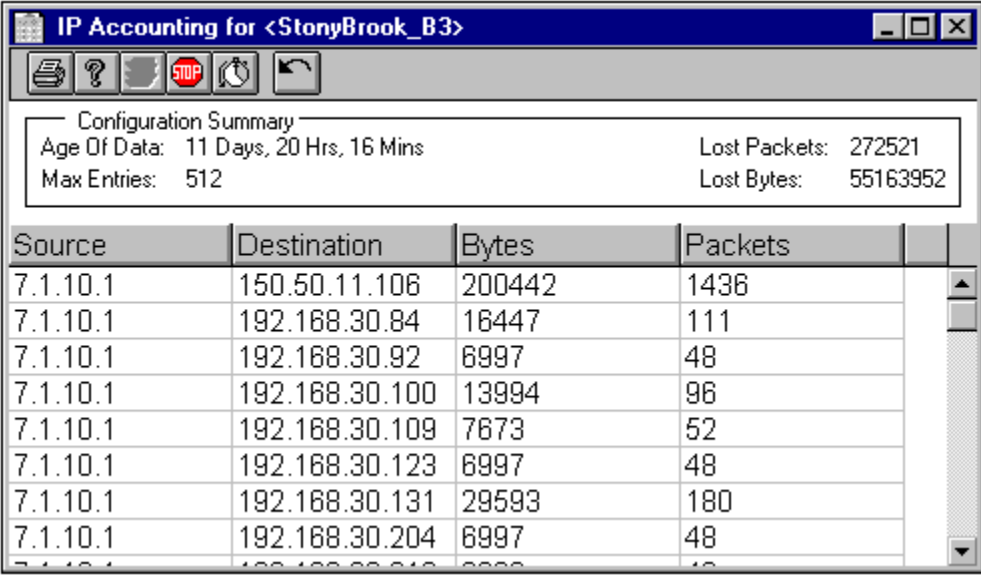
**NOTE:** The Accounting applet device specific and dependent on the device's configuration.

## **The IP Accounting applet**

The **IP Accounting** applet reports traffic accounting information which is important for understanding the total bytes contained in the IP packets that have been exchanged between any two end stations. From this information, the top talkers on the network can be determined. Long term utilization analysis can be applied for cost allocation and/or bill back.

## Accounting Applets

---



Source	Destination	Bytes	Packets
7.1.10.1	150.50.11.106	200442	1436
7.1.10.1	192.168.30.84	16447	111
7.1.10.1	192.168.30.92	6997	48
7.1.10.1	192.168.30.100	13994	96
7.1.10.1	192.168.30.109	7673	52
7.1.10.1	192.168.30.123	6997	48
7.1.10.1	192.168.30.131	29593	180
7.1.10.1	192.168.30.204	6997	48


The top pane contains Configuration Summary information that is retrieved from the router. It includes: Age of Data, Max Entries, Lost Packets, and Lost Bytes.

The table contains the following information:

Heading	Definition
Source	The IP Address of the source of the conversation.
Destination	The IP Address of the destination of the conversation.
Bytes	The total number of bytes transmitted between this source and destination IP Address.
Packets	The total number of packets transmitted between this source and destination IP Address.

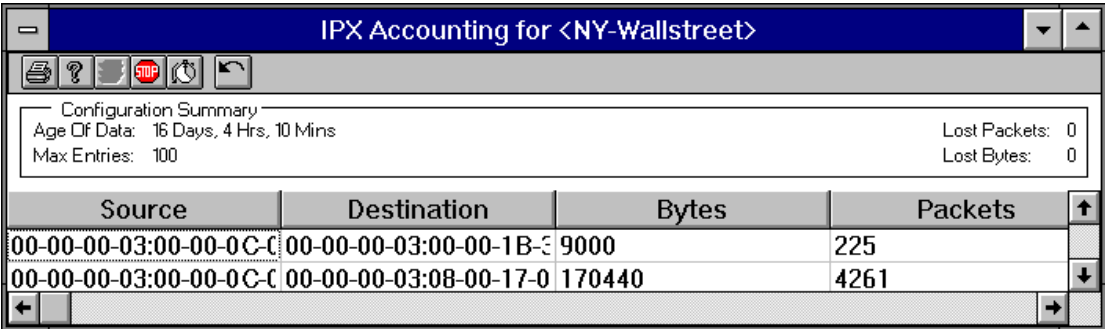
Other buttons

In addition to the global toolbar buttons, the IP Accounting applet has the following specialized button:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

The IPX Accounting applet

The **IPX Accounting** applet reports traffic accounting information which is important for understanding the total bytes contained in the IPX packets that have been exchanged between any two end stations. From this information, the top talkers on the network can be determined. Long term utilization analysis can be applied for cost allocation and/or bill back.



The top pane contains Configuration Summary information that is retrieved from the router. It includes: Age of Data, Max Entries, Lost Packets, and Lost Bytes.

The table contains the following information:

Heading	Definition
Source	The IPX Address of the source of the conversation.


## Accounting Applets

---

Heading	Definition
<b>Destination</b>	The IPX Address of the destination of the conversation.
<b>Bytes</b>	The total number of bytes transmitted between this source and destination IPX Address.
<b>Packets</b>	The total number of packets transmitted between this source and destination IPX Address.

### Other buttons

In addition to the global toolbar buttons, the IPX Accounting applet has the following specialized button:

Button	Description
	<b>[Export Data] button</b> Exports collected data to a comma separated variable file.

The Memory and Resource applets provide information about system resources. There are three applets:

- **The Small through Huge Buffer Information applets**  
Display the status of the system buffer pools. This is available only on Cisco routers running version 8.3 or higher software, properly configured.
- **The Memory Protocol Resource applet, Digital specific**  
Displays memory information.
- **The Buffer Protocol Resource applet, Digital specific**  
Displays information on system buffers.

### The Small through Huge Buffer Information applets

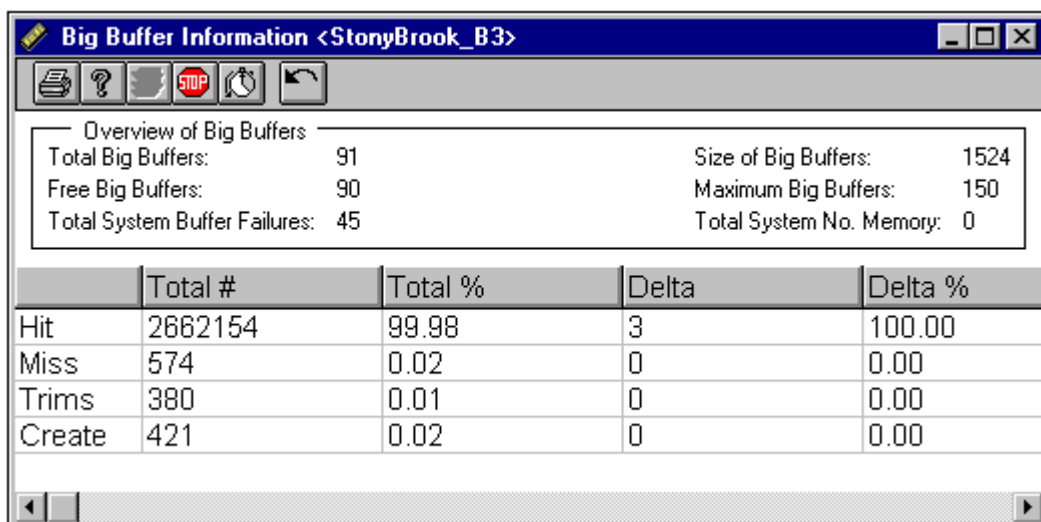
The Small through Huge Buffer Information applets display the status of the system buffer pools. These pools are used by the processor to buffer data packets. They are not the only buffers that are used to pass packets. IP, IPX, AppleTalk and bridging packets are also “fast switched.” This uses interface buffers and route caches without involving the central processor.

There are five different Buffer Information applets, each specific to a different buffer size:

- Small (Buffers)
- Medium (Buffers)
- Big (Buffers)
- Large (Buffers)
- Huge (Buffers)

Each applet opens a window with the buffer information specific to that size. For example:

## Memory and Resource



Overview of Big Buffers				
Total Big Buffers:	91	Size of Big Buffers:	1524	
Free Big Buffers:	90	Maximum Big Buffers:	150	
Total System Buffer Failures:	45	Total System No. Memory:	0	

	Total #	Total %	Delta	Delta %
Hit	2662154	99.98	3	100.00
Miss	574	0.02	0	0.00
Trims	380	0.01	0	0.00
Create	421	0.02	0	0.00

The screen is divided into two sections: Overview of “size” (e.g. small) buffers and a table of values. Overview of “Size” Buffers includes the following information:

Field Name	Definition
Total “size” buffers	bufferXxTotal
Size of “size” buffers	bufferXxSize
Free “size” buffers	bufferXxFree
Maximum “size” buffers	bufferXxMax
Total System buffer failures	bufferFail - global
Total System No Memory	bufferXxMem - global

Both “size” and Xx reflect the respective buffer pool

The table of values for the buffer information includes:

**TOTAL#**

<b>Total # Hit</b>	=	<b>bufferXxHit</b>
<b>Total # Miss</b>	=	<b>bufferXxMiss</b>
<b>Total # Trims</b>	=	<b>bufferXxTrims</b>
<b>Total # Create</b>	=	<b>bufferXxCreate</b>

**TOTAL%**

<b>Total % Hit</b>	=	<u><b>bufferXxHit</b></u> <b>bufferXxHit + bufferXxMiss</b>	<b>x</b>	<b>100</b>
<b>Total %Miss</b>	=	<u><b>bufferXxMiss</b></u> <b>bufferXxHit + bufferXxMiss</b>	<b>x</b>	<b>100</b>
<b>Total % Trims</b>	=	<u><b>bufferXxTrims</b></u> <b>bufferXxHit + bufferXxMiss</b>	<b>x</b>	<b>100</b>
<b>Total % Create</b>	=	<u><b>bufferXxCreate</b></u> <b>bufferXxHit + bufferXxMiss</b>	<b>x</b>	<b>100</b>

## Memory and Resource

---

### DELTA

Delta # Hit	=	e.g. bufferXxHitV2 - bufferXxHitV1 Where V1 is the first poll value and V2 is the second poll value
Delta # Miss	=	e.g. bufferXxMissV2 - bufferXxMissV1
Delta # Trims	=	e.g. bufferXxTrimsV2- bufferXxTrimsV1
Delta # Create	=	e.g. bufferXxCreateV2- bufferXxCreateV1

### DELTA%

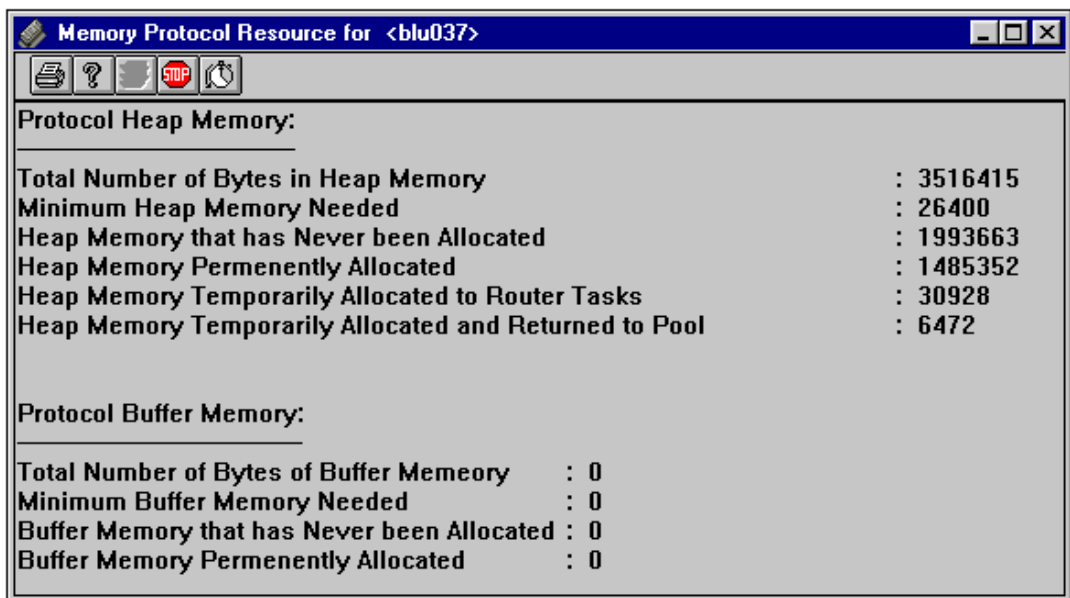
Delta % Hit	=	$\frac{\text{Delta\#Hit}}{\text{Delta\#Hit} + \text{Delta\#Miss}}$	x	100
Delta %Miss	=	$\frac{\text{Delta\#Miss}}{\text{Delta\#Hit} + \text{Delta\#Miss}}$	x	100
Delta % Trims	=	$\frac{\text{Delta\#Trims}}{\text{Delta\#Hit} + \text{Delta\#Miss}}$	x	100
Delta % Create	=	$\frac{\text{Delta\#Creates}}{\text{Delta\#Hit} + \text{Delta\#Miss}}$	x	100

### Launching the Small through Huge Buffer applets:

1. Right-click on a device icon and choose **Boxmap**.
2. From the physical view, select **Memory** > **Small/Medium/Big/Large/Huge**. From the application view, right-click on the Memory icon and select the appropriate applet.

## The Memory Protocol Resource applet for Digital

The Memory Protocol Resource applet lists information for Protocol Heap Memory and Protocol Buffer Memory. Total Heap Memory is shown, as well as the breakdown of Heap Memory into individual components.



The table information includes:

Heading	Definition
<b>Total Number of Bytes in Heap Memory</b>	The total amount of memory, in bytes, found on the device.
<b>Minimum Heap Memory Needed</b>	The total amount of memory, in bytes, found on the device.
<b>Heap Memory that has Never been Allocated</b> <b>Heap Memory Permanently Allocated</b>	These values show the breakdown of how the Heap Memory is being allocated at the moment of polling. Note that the combined value of these four items is equal to the value of Total Number of Bytes in Heap Memory.

## Memory and Resource

Heading	Definition
Heap Memory Temporarily Allocated to Router Tasks Heap Memory Temporarily Allocated and Returned to Pool	
Total Number of Bytes of Buffer Memory	The total amount of buffer memory, in bytes, found on the device, if any.
Minimum Buffer Memory Needed	The minimum amount of buffer memory needed.
Buffer Memory that has Never been Allocated Buffer Memory Permanently Allocated	These two values show the breakdown of how the Buffer Memory is being allocated.

### Launching the Memory Protocol Resource applet:

1. Right-click on a device icon and choose **Boxmap**.
2. From the physical view, select **Resource > Memory Protocol**. From the application view, right-click on the Resource icon and select **Memory Protocol**.

## The Buffer Protocol Resource applet for Digital

The Buffer Protocol Resource applet lists global buffer information (top pane of the window) and individual interface buffer information (bottom pane).

Buffer Protocol Resource for <RACentral_EW>								
Global Buffer Protocol resource								
Total number of global buffers in the system: 400			Total number of free buffers in the system: 393					
The fair number of buffers in each interface: 62			The low mark for free buffers: 80					
IF Index	IF Name	IF Description	Buffers Requested	Buffers Allocated	Low water mark	Current # Buffers	Size of Buffer	Total Bytes Allocated
1	eth0/net0	int desc 10000	100	100	50	100	1596	159600
2	eth1/net1	int Desc-2sss	100	100	50	99	1596	159600
3	sl0/net2	S inter Desc 3dc	24	24	4	24	2272	54528
4	sl1/net3	S	24	24	4	24	2272	54528
5	sl2/net4	S decsojkgne	24	24	4	24	2272	54528
6	sl3/net5	S	24	24	4	24	2272	54528
7	sl4/net6	S	24	24	4	24	2272	54528
8	sl5/net7	S	24	24	4	24	2272	54528
9	sl6/net8	S	24	24	4	24	2272	54528
10	sl7/net9	S this is 10	24	24	4	24	2272	54528

The interface table information includes:

Heading	Definition
<b>IF Index</b>	The index number of the interface.
<b>IF Name</b>	The name of the interface.
<b>IF Description</b>	The user-defined descriptive name for the interface as specified using the Description applet.
<b>Buffers Requested</b>	The number of buffers requested by the device for the specific interface.
<b>Buffers Allocated</b>	The number of buffers allocated by the device for the specific interface.
<b>Low Water Mark</b>	The low water mark for the interface.
<b>Current # Buffers</b>	The number of buffers currently in use.
<b>Size of Buffer</b>	The size of each buffer, in bytes.

## Memory and Resource

---

Heading	Definition
Total Bytes Allocated	The total number of bytes allocated to the interface. This number is calculated by Buffers Allocated x Size of Buffer.

### Launching the Buffer Protocol Resource applet:

1. Right-click on a device icon and choose **Boxmap**.
2. From the physical view, select **Resource > Buffer Protocol**. From the application view, right-click on the Resource icon and select **Buffer Protocol**.

NavisAccess provides several tools that make working with MIBs easier and more productive. Available tools are:

- **MIB Compiler**  
Compiles MIBs into machine-readable binary form. All Traps contained in the compiled MIBs are added to the events that the Trap Monitor interprets.
- **MIB Profile tool**  
Creates profiles of MIB variables that need to be queried routinely.
- **MIB Browser**  
Provides quick access to profiles created by the MIB Profile tool, allowing you to query MIBs with point-and-click ease.

## The MIB Compiler

The MIB Compiler takes ASN.1 formatted Management Information Base files and compiles them into a binary form. The traps contained in the MIB files are added to the events that the Trap Monitor interprets.

MIBs must be compiled for NavisAccess to interpret Traps successfully. If you do not compile the necessary MIBs, you will receive "Uncompiled Trap" messages in the Event Viewer.

MIB files are stored in the **NavisAccess/mibs** directory, under their respective vendor sub-directories. By default, the mibs directory already contains the Ascend MIBs and RFC1155 and RFC1213.

**NOTE:** At a minimum, all RFC and Ascend MIBs should be compiled. MIB RFC1213.mib *must* be included. Other MIBs can be compiled based on the vendor devices which are installed on the network.

## Using the MIB Compiler

To compile a MIB, the MIB file must be located in the **NavisAccess/mibs** directory. During installation, NavisAccess creates a number of vendor-specific sub-directories under the MIB directory. MIB files must be copied as needed from the sub-directories to the NavisAccess/mibs directory.

For example, if you wish to compile Traps from Cisco devices, copy all the

MIB files from the **NavisAccess/mibs/Cisco** directory up one level to the NavisAccess/mibs directory.

Regardless of the vendor devices you have, all the files from the **NavisAccess/mibs/RFC** directory should be copied and compiled. Some MIB files are dependent on these files to compile successfully.

### Unsuccessful compiles

If the MIB compiling is unsuccessful, error message(s) will be present and contain the line number where the error occurred. The user can correct the error and then rerun the MIB Compiler. See "MIB Compiler Errors" on page 600 for details on what the errors mean.

### To compile MIBs:

1. From the NavisAccess main menu bar, select **Tools > MIB Compiler**. Or, to run the MIB Compiler without starting NavisAccess, select the MIB Compiler icon from the NavisAccess program group.

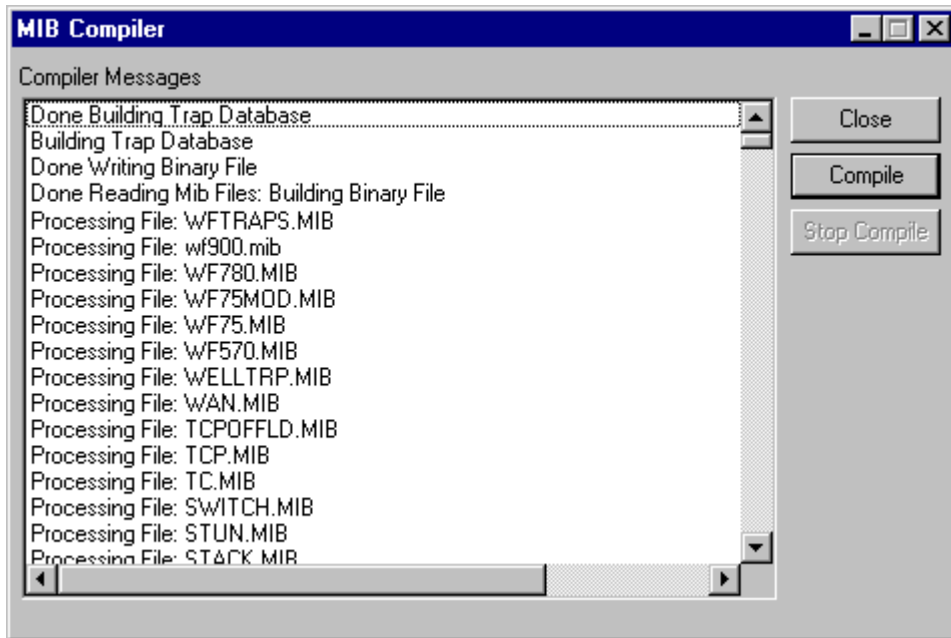
**NOTE:** If you compile MIBs with NavisAccess running, it will not read the compiled MIB file until it is restarted.

2. After making sure that all necessary MIB files are in the NavisAccess/mibs directory, click the [Compile] button. The compilation process will begin and will be displayed in the MIB compiler window.

Compiling of a MIB will generate messages reading: "Processing File: *<name of file>*."

3. Upon completion of the compiling process, the MIB Compiler will write a binary file and then build a Trap database. If the entire process is successful, a screen similar to the one below will be displayed. The top four messages will be the same as below. The "Processing File" messages will vary based on the MIBs being compiled.

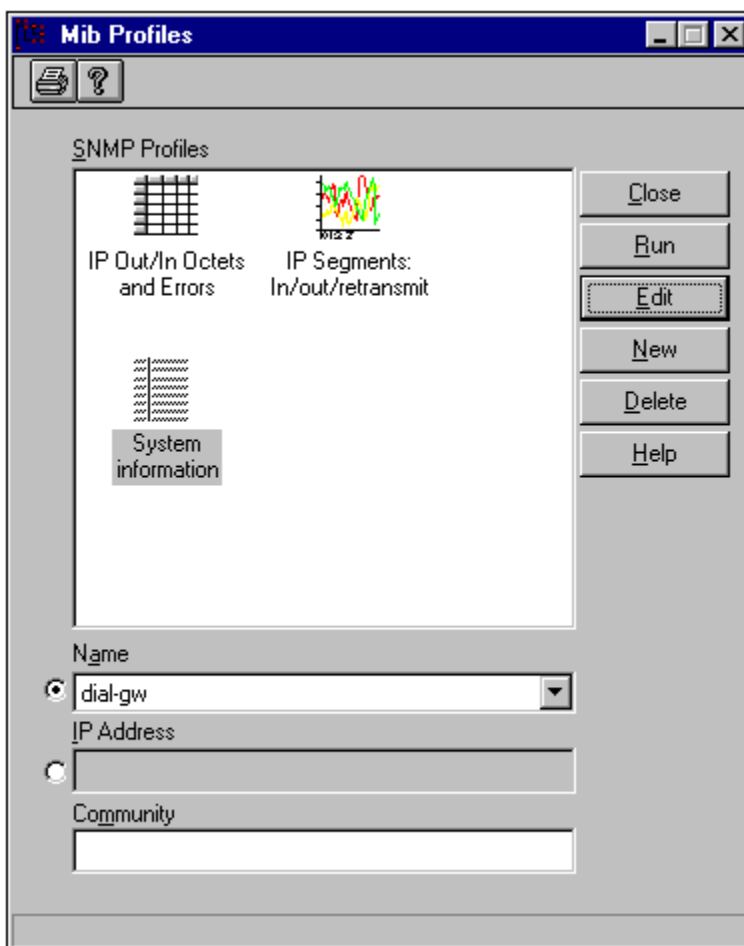
Depending on the number of MIBs compiled, it may take a few moments for the final stages of the process to complete.



## The MIB Browser: overview

The **MIB Browser** allows you to create profiles for MIB variables which you query often. When a profile is run, it queries the specified MIB variables on a device and returns values in chart, table or graph format, depending on the type of data involved. Returned values appear in real-time, updated based on the polling interval. Essentially, the MIB Browser functions as an easy-to-use application development tool which creates custom applications specifically tailored to the user's needs.

Because a MIB profile can be stored, you can use the same profile on multiple devices, and do not have to recreate it each time you need it. Easier still, each MIB profile appears in every device Boxmap, giving you quick, device-specific access for every box on your network.



### Using the MIB Browser

The MIB Browser is used to create, edit and run MIB profiles. Below is a general description of the MIB Profile creation process and the available tools. Following that are three specific examples of creating MIB Profiles (one of each type: table, column, graph ), including examples of the results of running the profiles.

### Creating a MIB Profile: general overview

1. To open the MIB Browser, use one of the following:
  - a. From the NavisAccess main menu bar, select **Tools > MIB Browser**.
  - b1. Right-click on a device icon or backpanel and select **Boxmap**.
  - b2. From the physical view, right-click a blank area of the screen and select **MIB Information > MIB Browser**. From the application view, right-click the MIB Information icon and select **MIB Browser**.

The MIB Profiles window opens.

2. Click the [New] button to open the New MIB Profile window.

**New MIB Profile**

Mib Information

- iso
  - org
    - dod
      - internet
        - directory
        - mgmt
        - experimental
        - private
  - ccitt
  - joint-iso-ccitt

Add Remove Information

MIB Variables

Name	Type	Access

Display Type Polling Interval

30

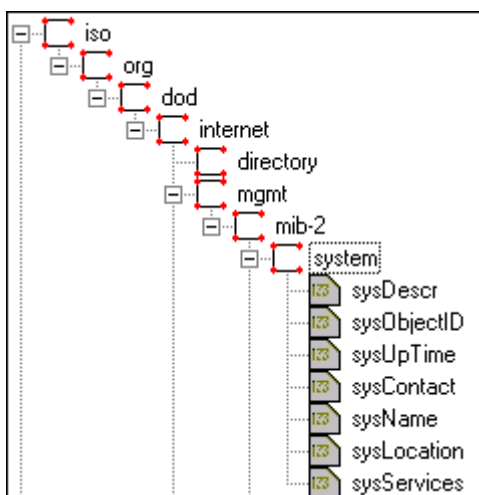
Description

☒ Show In Boxmap

Save Cancel Help

Creating a MIB profile involves searching through the MIB Information tree to find the variables you wish to query, adding them to the MIB Variables window, choosing a display type and giving the profile a name.

3. Search for MIB variables by drilling-down through the MIB Information tree by clicking on the directories. MIB variables are at the bottom of any given directory tree. The illustration following shows the full tree structure leading to the MIB II "system" variables: sysDescr, sysObjectID, etc.



Any of these variables can be selected for querying. To add a variable, double-click on it, or select it and click the [Add] button. Multiple selections are possible using standard [Ctrl] and [Shift] key techniques.

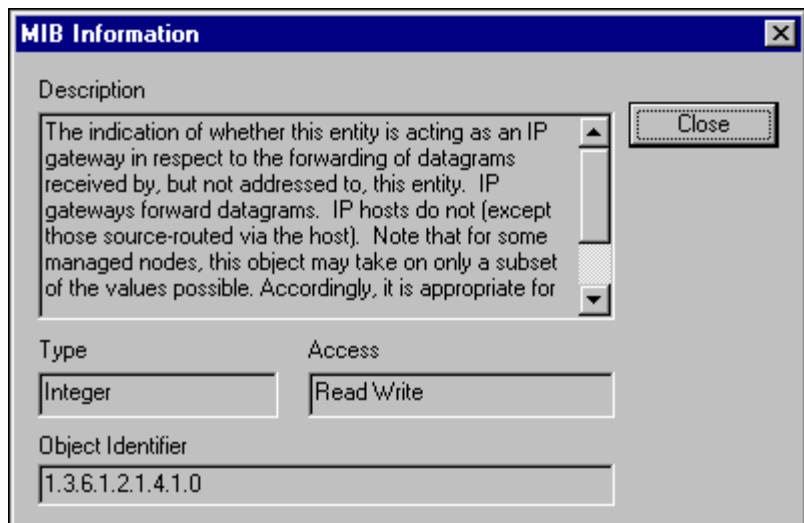
### Automated variable searching

If you know the exact variable name, you can quickly search the MIB directories by clicking the [Search for Variables] button at the top of the New MIB Profile screen and entering the variable name. Because the search process is top-down, you should click the top most directory before starting the search. The search is also case sensitive, so variables must be entered exactly as they exist in the MIB.

After the first search, you can continue to search the tree for further instances of the same variable by clicking the [Search for Next Occurrence of Variable] button.

### Instant variable information

4. If you do know what a particular variable represents, you can easily access that information. Once the variable is added to the MIB Variables window, either double-click on it or highlight it and click the [Information] button. This will open the MIB Information window, which will describe the MIB and display the object identifier. For example, following is the information for the MIB II **ipForwarding** variable:



5. After making all variable selections, select the manner in which you want the variables to display when queried. Choose from three options in the Display Type drop-down box:

#### Column Display

Data is displayed as text with a blank background. Certain fields may change, and they will update based on the polling interval. Text fields (such as Octet Strings) will remain the same.

#### Table Display

Data is arrayed in a table format, with column headings running across the top of the table, and data aligned underneath. Table values are updated based on the polling interval.




#### Graph Display

Data is displayed as a moving line graph. Each graphed variable is color coded, with value and time-stamp information displayed on the x- and y-

axis respectively. Graph points are plotted based on the polling interval.

**NOTE:** Not all variables will support all three types of graphs, and some will support only one type. If you choose a graph type that is incompatible with the variables chosen, you will receive an error message requesting that you select a different graph type.

- 6. Set the polling interval using the Polling Interval spin box. The default value is 30 seconds.
- 7. Enter a name for the MIB Profile in the Description field. Since this name will be used to access the MIB Profile, it should be descriptive of the variables selected.
- 8. Select the Show in Boxmap option if you want to be able to access this profile through the individual device Boxmaps. This option is selected by default, as it is extremely useful.
- 9. Click [Save] when done. This will create a labeled icon in the MIB Profiles window. Each type of profile has an individual icon associated with it.

Icon	Profile Type
	Column
	Table
	Graph

## Running a MIB Profile

MIB Profiles can be run either from the MIB Browser or from the Boxmap.

**NOTE:** A profile is only accessible from the Boxmap if you did not de-select Show in Boxmap when you created the profile.

### From the MIB Browser

1. From the main menu bar of NavisAccess, select **Tools > MIB Browser** to open the MIB Browser.

The MIB Browser can also be opened by right-clicking the MIB Information icon in the Boxmap and selecting **MIB Browser**.

2. Select the device for which you want to create a MIB profile. There are two methods by which you may select the device:

#### **Name**

Click the Name radio button and choose a device from the drop-down list. The drop-down list contains all devices discovered by NavisAccess.

#### **IP Address**

Click the IP Address radio button and enter a device IP address.

3. You may optional specify a Community String for the device. The Community String you specify here overrides the default Community String set during Configuration of the System Options.
4. Select a profile from the SNMP Profiles field.
5. Click the [Run] button.

The selected device will be queried, and the MIB values returned based on the profile.

For examples of what a MIB profile can generate, see the following:

- MIB Profile Example 1: Table Display
- MIB Profile Example 2: Column Display
- MIB Profile Example 3: Graph Display

### MIB profile example 1: Table display

The MIB Profile Table Display retrieves MIB data and displays it in a table format. The table is accessed from within the MIB Browser by clicking the Table icon.

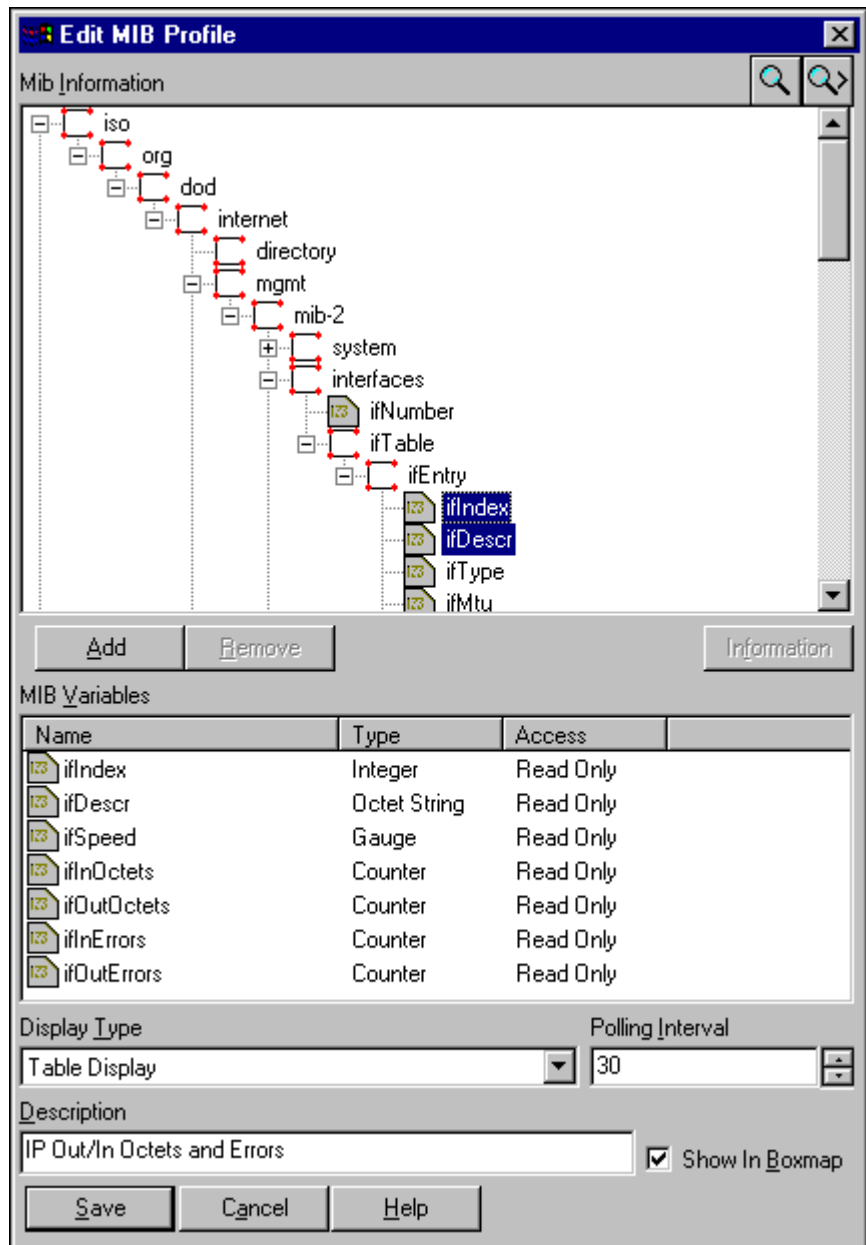
The following example will create a MIB Profile to query devices for the following information and return values in a table format:

- Interface index
- Interface description
- Interface speed
- Incoming/Outgoing octets
- Inbound/Outbound packets with errors

You may wish to recreate this profile to become familiar with the MIB Browser.

#### To create the profile

1. Open the MIB Browser and click [New].
2. Drill-down to the MIB-2 "ifEntry" directory, as shown below.



3. Highlight the following variables:

**ifIndex:** the interface index

**ifDescr:** the interface description

**ifSpeed:** the configured speed of the interface

**ifInOctets:** incoming octets

**ifOutOctets:** outgoing octets

**IfInErrors:** inbound packets with errors

**ifOutErrors:** outbound packets with errors

4. Click [Add] to move them to the MIB Variables window. Remember, you can double-click any variable in the MIB Variables window to see detailed information on what the variable represents.

**NOTE:** When the table is generated, the variables will appear in the order they appear in the MIB Variables window. That is why we have put **ifIndex** and **ifDescr** as the first two entries. It is advisable to put descriptive variables in the first columns of the table. You can move variables within the MIB Variables window by simply clicking and holding the mouse and dragging them to a new position.

5. Choose Table Display from the Display Type drop-down box.
6. Name the profile "IP Out/In Octets and Errors."
7. Click [Save].
8. In the MIB Browser window, select a device, highlight the new profile and click [Run].

Following is an example of what this profile produces:

ifIndex	ifDescr	ifSpeed	ifInOctets	ifOutOctets	ifInErrors	ifOutErrors
1	Serial0	1544000	3663724889	2229112823	13921	0
2	Serial1	1544000	2557572917	726711734	13200	0
3	Serial2	1544000	291283356	318364774	71906	0
4	Serial3	1544000	655654998	2461126230	463204	0
5	Serial4	56000	163141218	3607619759	649	0
6	Serial5	56000	730734646	3556311533	5102	0
7	Serial6	56000	0	0	0	0
8	Serial7	56000	3380138137	1412611895	240	0
9	Serial8	56000	0	0	0	0
10	Serial9	56000	0	0	0	0
11	Serial10	56000	60260012	2550700271	2257	0

In this table, values are continually updated based on the polling interval. The graph will keep displaying data for as long as it remains open. All fields are sortable by clicking on the column heading.

## MIB profile example 2: Column display

The MIB Profile Column Display retrieves MIB data and displays it in a column format. The column is accessed from within the MIB Browser by clicking the Column icon.

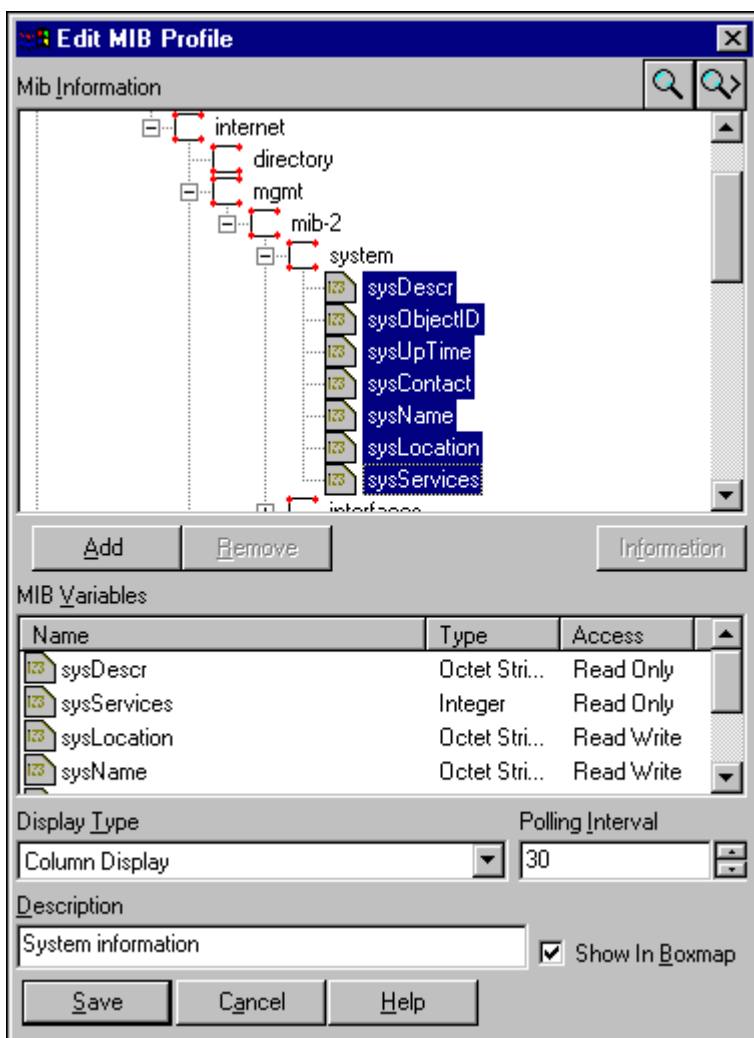
The following example will create a MIB Profile to query devices for the following information and return values in a column display format:

- System description and name
- System location
- Contact name
- System services
- System uptime
- Object ID

You may wish to recreate this profile to become familiar with the MIB Browser.

### To create the profile

1. Open the MIB Browser and click [New].
2. Drill-down to the MIB-2 "system" directory, as shown below.



3. Highlight the following variables:  
**sysDescr:** the interface index

**sysObjectID:** the device object ID

**sysUpTime:** the amount of time the system has been up

**sysContact:** the contact name for this device

**sysName:** the name of the device

**sysLocation:** the location of the device

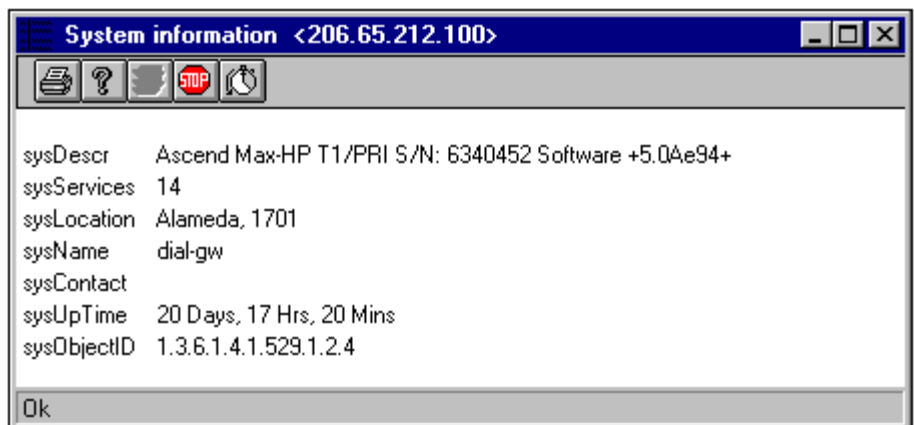
**sysServices:** the system services that run on this device

4. Click [Add] to move them to the MIB Variables window. Remember, you can double-click any variable in the MIB Variables window to see detailed information on what the variable represents.

**NOTE:** When the table is generated, the variables will appear in the order they appear in the MIB Variables window.

5. Choose Column Display from the Display Type drop-down box.
6. Name the profile "System information."
7. Click [Save].
8. In the MIB Browser window, select a device, highlight the new profile and click [Run].

Following is an example of what this profile produces:



In this window, most of the values are static and will not change. However, the sysUpTime field will be updated based on the polling interval.

### MIB profile example 3: Graph display

The MIB Profile Graph Display retrieves MIB data and displays it in a graph format. The graph is opened from the MIB Browser by clicking the Graph icon.

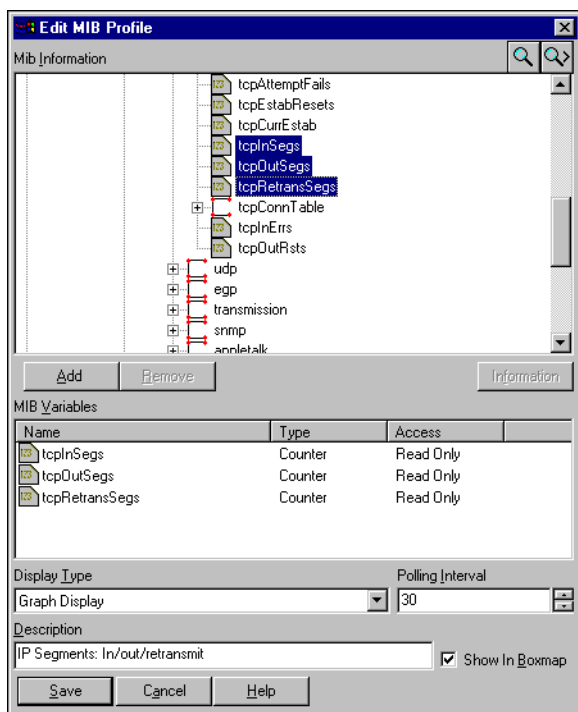
The following example will create a MIB Profile to query devices for the following information and return values in a graph display format:

- Number of IP segments sent
- Number of IP segments received
- Number of IP segments retransmitted

You may wish to recreate this profile to become familiar with the MIB Browser.

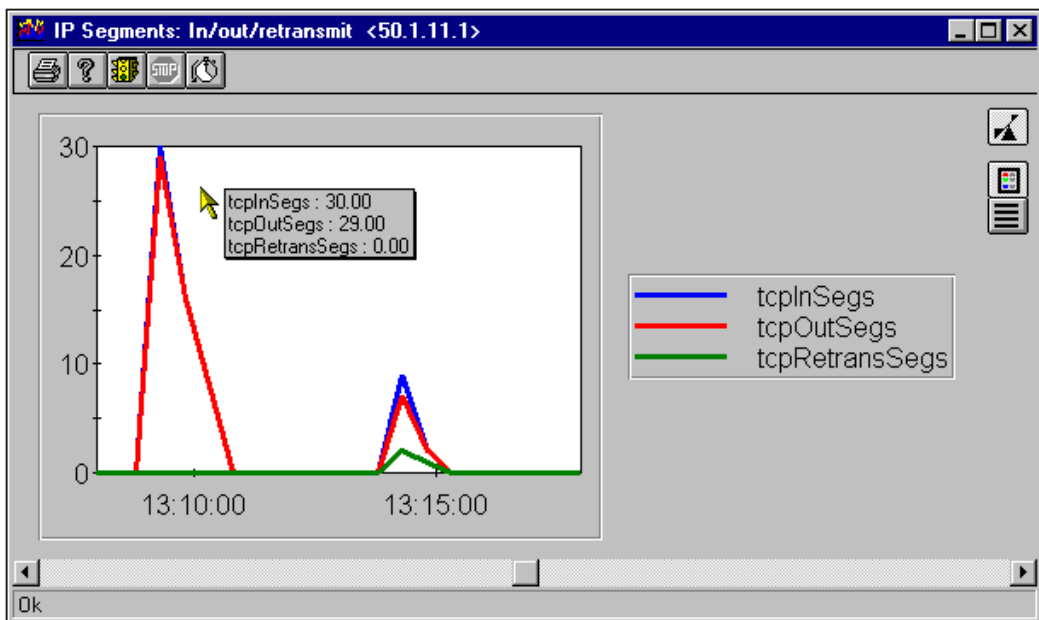
#### To create the profile

1. Open the MIB Browser and click [New].
2. Drill-down to the MIB-2 "tcp" directory.



3. Highlight the following variables:  
**tcpInSegs:** the number of incoming IP segments  
**tcpOutSegs:** the number of outgoing IP segments  
**tcpRetransSegs:** the number of retransmitted IP segments
4. Click [Add] to move them to the MIB Variables window. Remember, you can double-click any variable in the MIB Variables window to see detailed information on what the variable represents.
5. Choose Graph Display from the Display Type drop-down box.
6. Name the profile "IP Segments: In/out/retransmit."
7. Click [Save].
8. In the MIB Browser window, select a device, highlight the new profile and click [Run].

Following is an example of what this profile produces:



Values for the three variables are graphed in real-time. Note that by clicking the mouse in the graph window, the exact values are displayed.

Clicking the [Show/Hide Graph Legend] button displays the key which associates each color with a specific variable.

The graph will run as long as it remains open, and supports all standard NavisAccess line graph functions.

## MIB Compiler Errors

### General Errors

#### **Error Compiling MIBs, Binary File not Generated**

Occurs if any errors are encountered while compiling a MIB

#### **The MIB Description Doesn't Seem to be Consistent. Some nodes Couldn't be Linked under the "iso" Tree**

A MIB has compiled successfully, but cannot be linked into the MIB tree. This happens when the parent of the root MIB element defined in the MIB is undefined.

#### **Could Not Read rfc1213.mib**

There MUST be a file called rfc1213.mib in the MIBs directory. This should have been installed during installation.

### MIB Parser Errors

#### **Syntax Errors in MIBs**

##### **Comma, Not Valid for Object Identifier**

##### **Not Valid for Object Identifier**

##### **End Of File Parsing Constraint**

The parser encountered the end of the MIB file while parsing a constraint.

##### **Error Parsing Constraint**

Printed when an error occurs parsing a constraint.

##### **Error Parsing Constraints Expected NUMBER**

Defines the specific error which occurred when parsing a constraint

##### **Error Parsing Constraints Expected DOT**

Defines the specific error which occurred when parsing a constraint

**Error Parsing Constraints Expected .DOT**

Defines the specific error which occurred when parsing a constraint

**Missing End of OID**

While parsing an object identifier an error occurred.

**Bad Object identifier**

While parsing an object identifier an error occurred.

**No End to OID**

While parsing an object identifier an error occurred.

**Bad Format**

Printed while parsing an object identifier if there is no ":" after the keyword OBJECT IDENTIFIER as in:

**label OBJECT IDENTIFIER := ( parent 2 }**

Also printed if the := is missing after an OBJECT TYPE clause

**label OBJECT-TYPE**

**SYNTAX**

**ACCESS**

**STATUS**

**DESCRIPTION ""**

**::= { parent 1 }**

**No More Textual Conventions Possible**

The textual convention lookup table is full. Contact Digital Equipment Technical Support.

**Textual Convention doesn't Map to Real Type**

A textual convention specifies a translation which was undefined.

**Expected "{"**

The parser expected a token of the displayed type and did not receive one.

**Expected "}"**

The parser expected a token of the displayed type and did not receive one.

**Expected "("**

The parser expected a token of the displayed type and did not receive one.

**Expected ")"**

The parser expected a token of the displayed type and did not receive one.

**Expected a Closing Parenthesis**

The parser expected a token of the displayed type and did not receive one.

**Expected integer**

The parser expected a token of the displayed type and did not receive one.

**Expected a Number**

The parser expected a token of the displayed type and did not receive one.

**Bad Format for TRAP TYPE**

While parsing a TRAP TYPE clause, a syntax error occurred.

**Bad Format for TRAP-TYPE Expected Label**

While parsing a TRAP TYPE clause, a syntax error occurred.

**Bad Format for TRAP-type Expected EQUALS**

While parsing a TRAP TYPE clause, a syntax error occurred.

**Bad Format for TRAP-type Expected NUMBER**

While parsing a TRAP TYPE clause, a syntax error occurred.

**Node <name> with parent <name> could not be linked**

While parsing an ObjectID, the parser could not lookup the MIB element's parent. Therefore, the MIB element cannot be linked into the MIB tree.

**Bad DESCRIPTION**

While parsing a DESCRIPTION statement a quoted string was not found as the next token.

**DESCRIPTION "description"**

**Bad Syntax**

Type data type of a SYNTAX statement in an OBJECT TYPE clause was not understood.

**label OBJECT-TYPE**

**SYNTAX <bad syntax>**

**Should be ACCESS**

An access statement MUST follow the SYNTAX statement of an OBJECT TYPE clause

**Bad Access Type**

The access type of an ACCESS statement is not valid.

**Should be STATUS**

A STATUS statement MUST follow the SYNTAX statement of an OBJECT TYPE clause.

**Bad Status**

The status type of the STATUS statement is not valid.

**Bad Format of Optional Clauses**

Various syntax errors in OBJECT TYPE clause definitions.

**Bad Format for OBJECT TYPE**

While parsing an OBJECT TYPE clause the SYNTAX statement was not found as first:

**label OBJECT-TYPE**

**SYNTAX**

**ACCESS**

**STATUS**

**DESCRIPTION ""**

**::= { parent 1 }**

**Error, End before Start of MIB.**

An END statement was encountered without a corresponding begin

**<word> is a Reserved Word**

The <word> is a predefined keyword and cannot be used as an identifier.

**Error, Nested MIBS.**

A begin statement was encountered while a MIB definition was already in progress without an END statement.

**MIB Compiler Errors for Parser Type:**

These statements refer back to Parser and are printed if a Syntax Error, as described above, occurs while parsing any of the MIB statements defined in this section.

**Bad parse of module header**

**Bad parse of object type**  
**Bad parse of objecttype**  
**Bad parse of trap type**  
**Bad parse of object group**  
**Bad parse of objectgroup**  
**Bad parse of notification definition**  
**Bad parse of module compliance**  
**Bad parse of module identity**  
**Bad parse of object identity**  
**Bad parse of object id**  
**Bad parse of object type**  
**Bad parse of ASN type definition.**  
**Bad operator**

NavisAccess functions as a BOOTP Server for the network. As devices are booted, they send calls to a specified server, asking for system files. The BOOTP Server applet allows you to specify the files that will be used by a given device during the BOOTP startup process.

The BOOTP Server applet is launched automatically at startup and is seen in the Windows NT task bar, indicated by the BOOTP Server icon.

## Launching the BOOTP Server

To open the BOOTP Server applet, right-click on the TFTP Server icon and choose **Configure and Monitor BOOTP**.

## Configuring the BOOTP Server

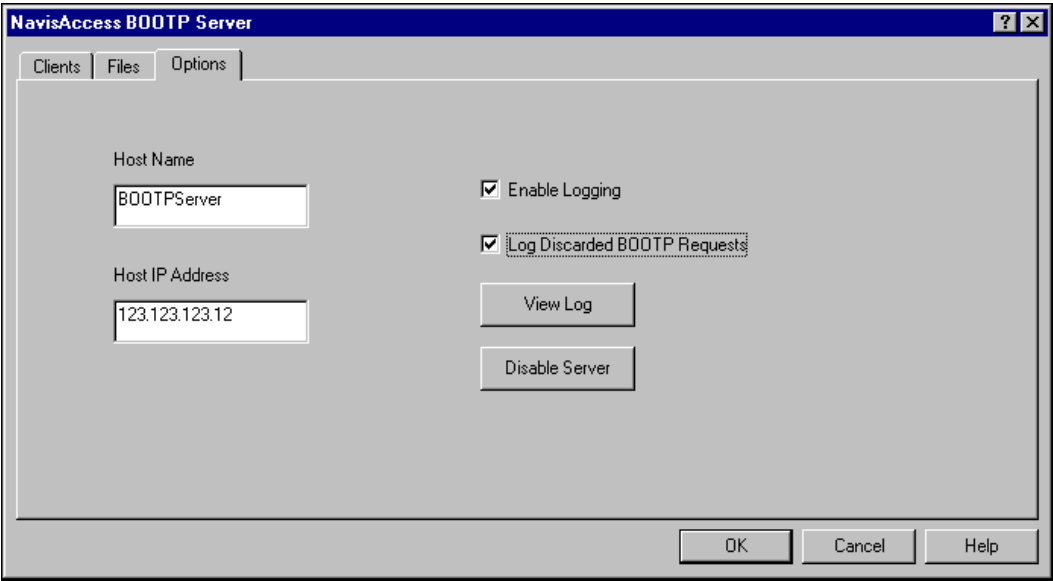
There are three screens used for configuring the BOOTP Server.

- **Options tab**  
Set the name and location of the BOOTP Server
- **Clients tab**  
Set the names and locations of the devices that will call the BOTP Server
- **Files tab**  
Change the file(s) that will be sent by the BOOTP Server

# BOOTP Server

## BOOTP Server Options tab

Use the BOOTP Server options tab to set the name and location of the NavisAccess machine that will be acting as the BOOTP server.



The Options tab displays the following fields:

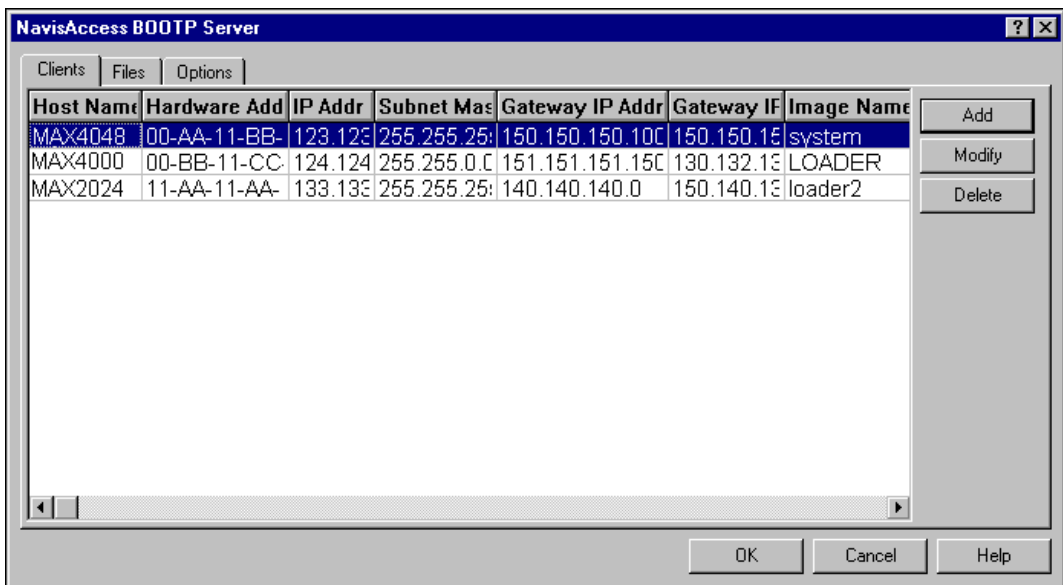
Field	Description
Host Name	The name of the NavisAccess machine that will be acting as the BOOTP server.
Host IP Address	The IP address of the BOOTP server machine.
Enable Logging	Select to enable BOOTP logging. Click the [View Log] button to view the BOOTP log file. This file is stored as BOOTP.LOG in the NavisAccess home directory (c:\NavisAccess by default).
Log Discarded BOOTP Requests	Select to enable logging of discarded BOOTP requests. This information is not normally logged.

### Disable the BOOTP Server

You can disable the BOOTP Server by clicking the [Disable Server] button. When disabled, the TFTP Server icon will change colors.

### BOOTP Server Clients tab

Use the BOOTP Server Clients tab to list the names and locations of the network devices that will call the BOOTP Server when they are booted.



The Clients tab displays the following fields:

Field	Description
Host Name	The name of the network device that will contact the BOOTP Server for information upon boot up.
Hardware Address	The Ethernet hardware address of the network device. The hardware address consists of six pairs of hexadecimal digits of the form: 00aa00bb00cc.
IP Address	The IP address of the network device.

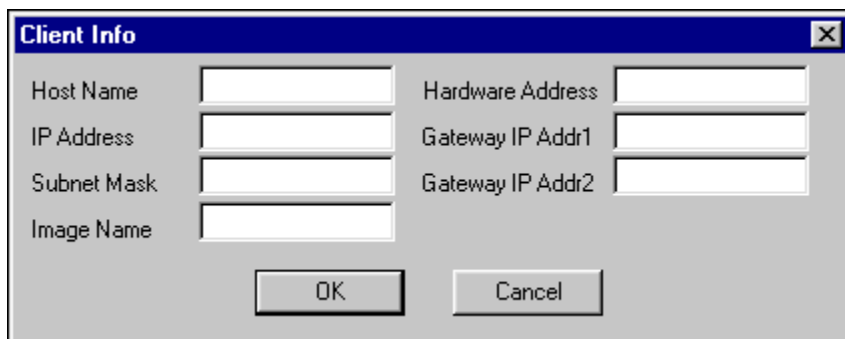
## BOOTP Server

Field	Description
Subnet Mask	The subnet mask of the network device.
Gateway IP Address 1 Gateway IP Address 2	The IP address of the gateway the network devices uses. You may specify two gateways.
Image Name	The name of the image file that the BOOTP server sends to the network device in response to a BOOTP request. This file must reside in the BOOTP server's default directory (e.g. c:\NavisAccess).

### Entering information

To add entries to the BOOTP Server Clients tab:

1. Click the [Add] button. This will bring up the Client Info window.

A screenshot of the 'Client Info' dialog box. It has a blue title bar with the text 'Client Info' and a close button (X) on the right. The dialog contains two columns of text input fields. The left column has four fields labeled 'Host Name', 'IP Address', 'Subnet Mask', and 'Image Name'. The right column has three fields labeled 'Hardware Address', 'Gateway IP Addr1', and 'Gateway IP Addr2'. At the bottom center are two buttons: 'OK' and 'Cancel'.

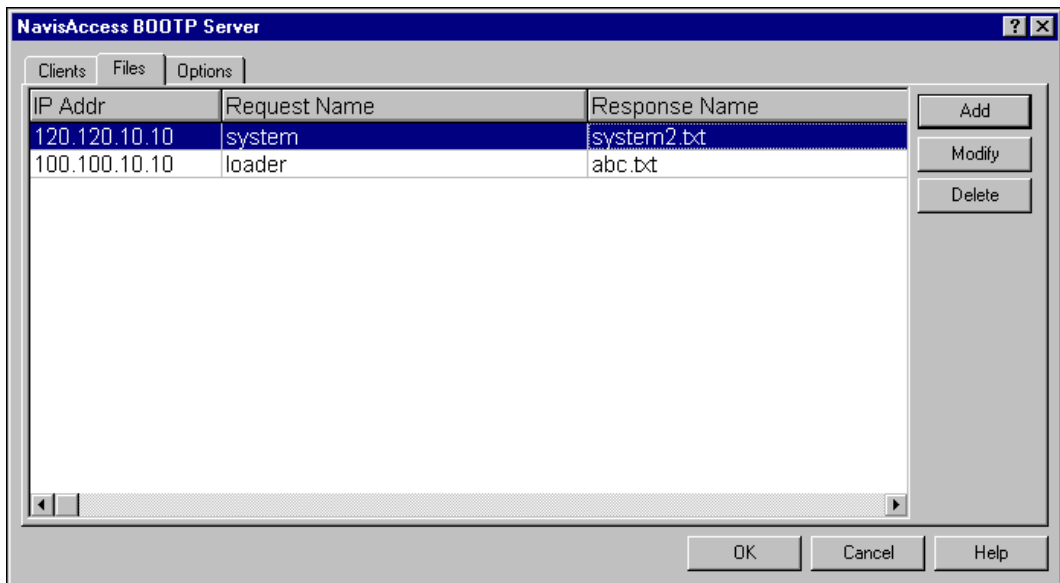
2. Enter the information in the appropriate fields.
3. Click OK to add entry to the Clients window. Repeat for as many devices as needed.

### Deleting/Modifying Entries

To delete or modify an entry in the Clients window, highlight the line and click [Delete] or [Modify] as needed.

## BOOTP Server Files tab

Use the BOOTP Server Files tab to specify which file a network device will be sent. The Files tab allows you to specify a file different from the specific file the device will call for. This is useful because many devices will call for generic file names, such as **system** or **config**. The Files tab gives you greater control over what files will be delivered.



The Files tab displays the following fields:

Field	Description
<b>IP Address</b>	The IP address of the network device that will receive the file in question. If you do not enter a value for IP address, all devices will call for the listed file.
<b>Request Name</b>	The name of the file that the network devices requests from the BOOTP Server.
<b>Response Name</b>	The name of the file that the BOOTP Server will send to the network device in response to a BOOTP request. The response file must be located in the BOOTP Server's default directory (e.g., c:\NavisAccess).

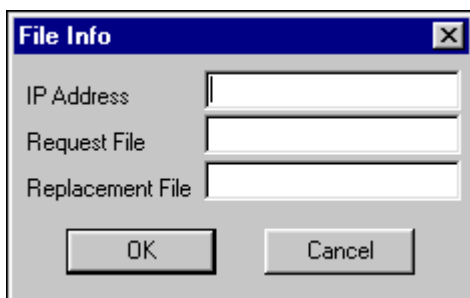
## BOOTP Server

---

### Entering information

To add entries to the BOOTP Server Files tab:

1. Click the [Add] button. This will bring up the File Info window.

A screenshot of a Windows-style dialog box titled "File Info". The dialog has a blue title bar with a close button (X) in the top right corner. Inside the dialog, there are three text input fields stacked vertically. The first field is labeled "IP Address", the second is labeled "Request File", and the third is labeled "Replacement File". At the bottom of the dialog, there are two buttons: "OK" on the left and "Cancel" on the right.

2. Enter the appropriate information click OK to add the entry to the Files list. Repeat the procedure as needed.

### What are "Applets"?

"Applets" are the NavisAccess designation for a sub-application providing information about a component. All functions have an applet, and every applet works in a similar way. Applets display information in graphs, pie charts, tables, and other graphical forms. Each applet's window has a customized toolbar. Certain toolbars are common to all applets, while others are specialized for their application.

### Protocol and performance applets

Protocol and Performance applets use graphs to display statistical information sent from a device. These applets log the data to a historical database for retrieval. Available options are specific for each type of applet.

**Performance** applets use graphs to display real-time statistics, such as line utilization, sent from a device.

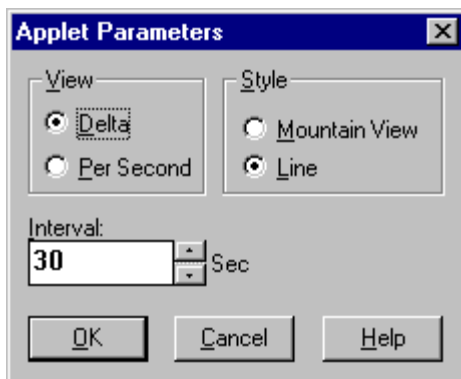
**Protocol** applets compare values retrieved from a device in two successive polling intervals. Protocol applets display statistics using either a Delta calculation or a Per Second calculation.

- **Delta** is the difference between a parameter's last value and its current value. The value plotted on the graph is the current value of a device variable measured against prior polling reports from the same device.
- **Per Second** is calculated by using the Delta value and dividing it by the actual polling interval. "Actual" takes into account network delays which may have caused errors in the reported polling interval.

Protocol and Performance applets can be started from multiple points within the program, typically by right-clicking on an icon or a device image.

### Applet parameters

Opening most applets brings up an "Applet Parameters" dialog box:

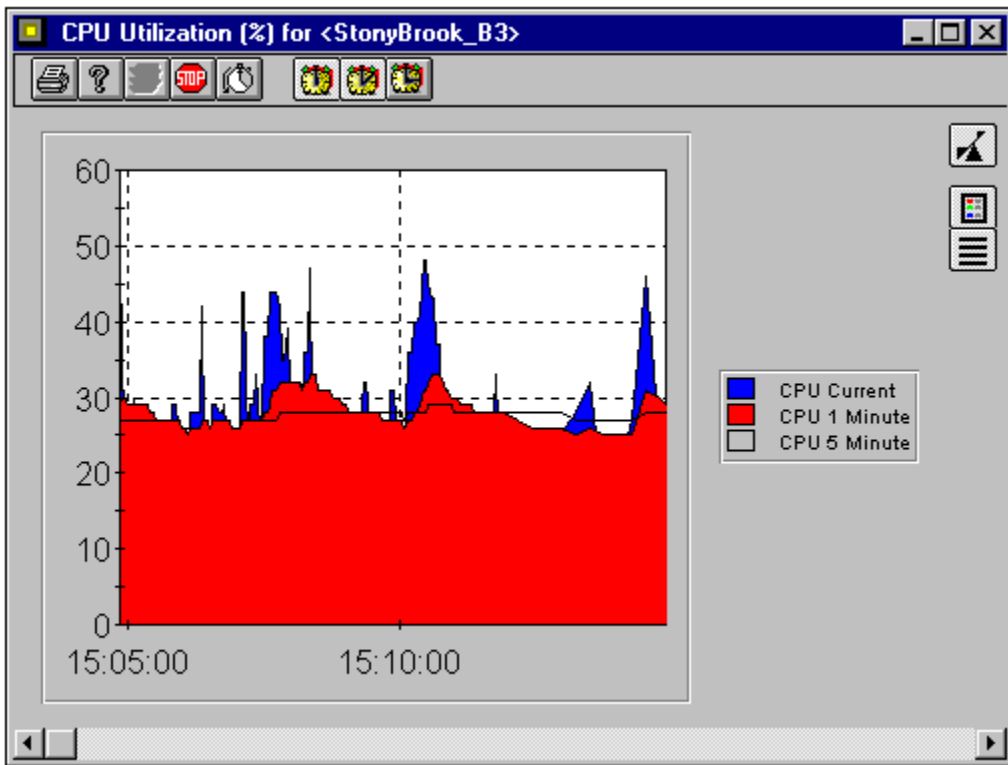


This dialog box performs several functions. Not every function setting is available for each Applet. If a setting is not available, it is grayed out. The Applet Parameters functions are:

- **View** shows the graphed information on a Per Second or Delta basis from the last polling interval. This applies only to Protocol Applets .
- **Interval** specifies the polling interval to use for the graph. The default is the value entered into the Applet tab of the Configuration Applet . If desired, the polling interval can be changed here.
- **Style** allows for the selection of the line graph preferred for tracking information. The two style options are Mountain Style (filled in line with peaks) or Line Style.

**Mountain style (filled in line with peaks):**

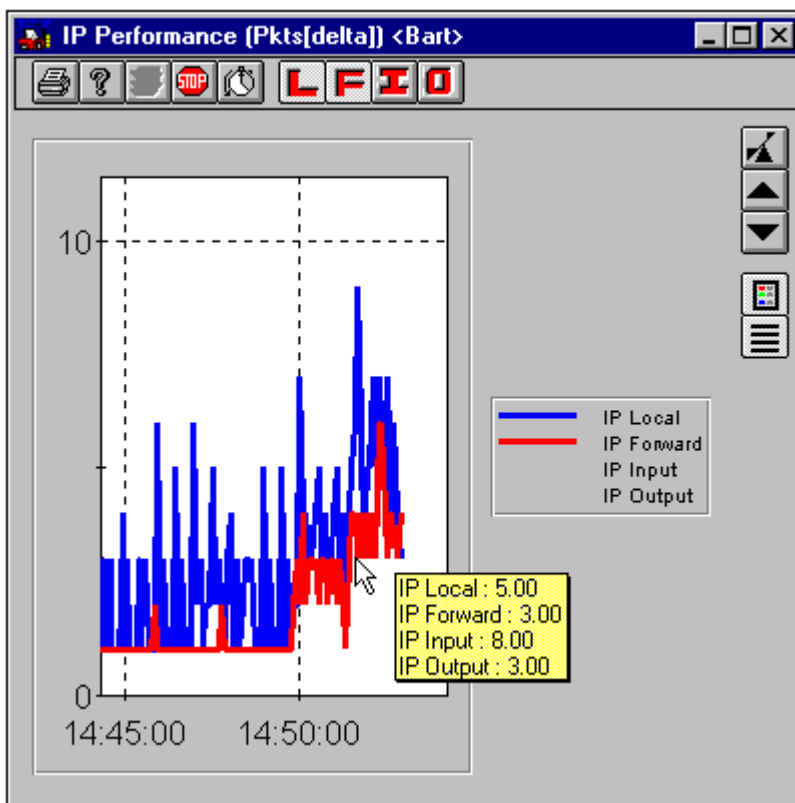
This sample Mountain Style graph shows CPU Utilization performance. The "CPU 5 Minute" line has been turned off by clicking the Show/Hide graph button. This allows clearer viewing of the "CPU Current" and "CPU 1 Minute" readings. Line viewing can be turned on and off by clicking the Show/Hide buttons.



### Line style

This sample Line Style graph shows an IP Performance chart. The graph lines for IP Input and IP Output have been turned off by clicking the [I] and [O] buttons on the top of the window. This allows clearer viewing of the Local and Forward data.

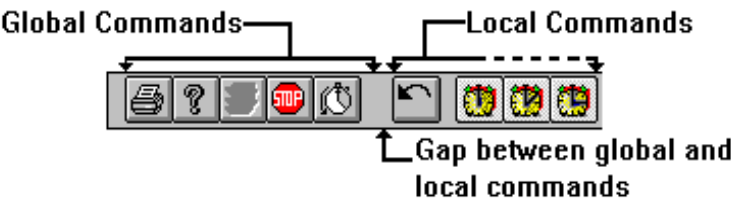
By clicking and holding the mouse button on the graph, precise performance information is displayed, as shown in the yellow pop-up window next to the mouse pointer.



Toolbars

Each applet has a toolbar that allows for certain tasks to be done more quickly. Global toolbar buttons common to all applets are found on the left hand side of the applet window. Other toolbar buttons (local commands) are specialized for certain applets. They are located on the right hand side of the toolbar.

A small gap separates global and local command buttons. A description of each toolbar button can be obtained by holding the mouse still on the selected button. The descriptive information displays in a small yellow information box.




Global toolbar buttons are described below:

Button	Description
	<b>[Print] button</b> Print all pages of the active applet.
	<b>[Help] button</b> Obtain help on the current applet.
	<b>[Start SNMP Requests] button</b> Start polling on the active applet. Since polling is turned on automatically when an applet starts, this button is only available if polling has been disabled by the Stop Polling button.
	<b>[Stop SNMP Requests] button</b> Stop polling on the active Applet.
	<b>[Set Polling Interval] button</b> Brings up a dialog box to change the polling interval for the current applet.

### Line graphs

Line graphs monitor real-time data, plotting quantitative values against time. Each type of data displayed appears as a counter, a colored line or shape plotted against time. Graphs are updated based on the frequency of polling intervals.


Each line graph has an optional [Legend] button . Press the [Legend] button to identify the lines by color. Place the mouse on any point in the graph to read the value at that point. The following table gives a breakdown of the legend parameters for the different types of Applet graphs.

Applet	Legend Parameters
Protocol	Input , Forward , Output , Local
Distribution	Active protocols (e.g., IP, IPX, etc.)
Alarm Monitor	Unknown, Critical, Major, Minor, Informational
Interface (for Utilization)	Input, Output

The styles for each Applet graph can be changed and customized. Two graph styles (line types) are available, Line and Mountain .

### Scaling

The Y-axis (vertical) of every line graph can be scaled.

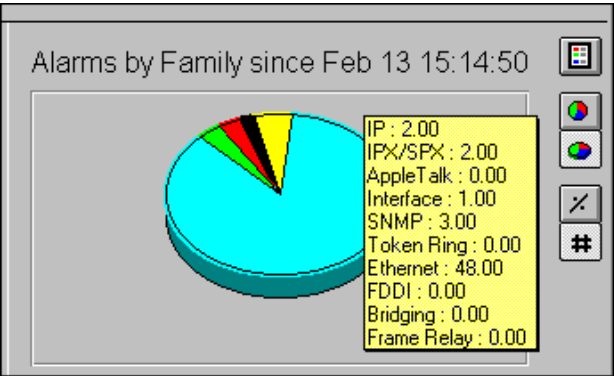
Click on the [Auto Scale Graph] button  to open the vertical axis scale buttons.




The Up and Down arrows allow you to increase or decrease the graph scale. The [Auto Scale Graph] button will automatically reset the graph to the default scale.

Pie charts

Pie charts are used to display real-time data such as packet distribution and device alarms. Each pie chart includes an optional legend identifying the respective parts by color in the pie chart.



To bring up the legend for a pie chart, click on the [Legend] control button

 . To remove the legend, re-press the [Legend] control button.

The legend window will look similar to the following, with entries varying based on the applet in use:



Values for the pie chart can be determined by clicking and holding the left mouse button on the pie chart. Values are displayed in a pop up window, as shown above.

Values can be displayed as either a percentage value (e.g. 10% of all alarms sent) or as an integer value (e.g., 10 alarms sent). To toggle between these two displays, click the [Show Values/Show Percent] buttons.



## Generic Functions

---

You can also toggle the pie chart between a 2D and 3D image, by clicking the [Show/Hide 3D Effect] buttons.

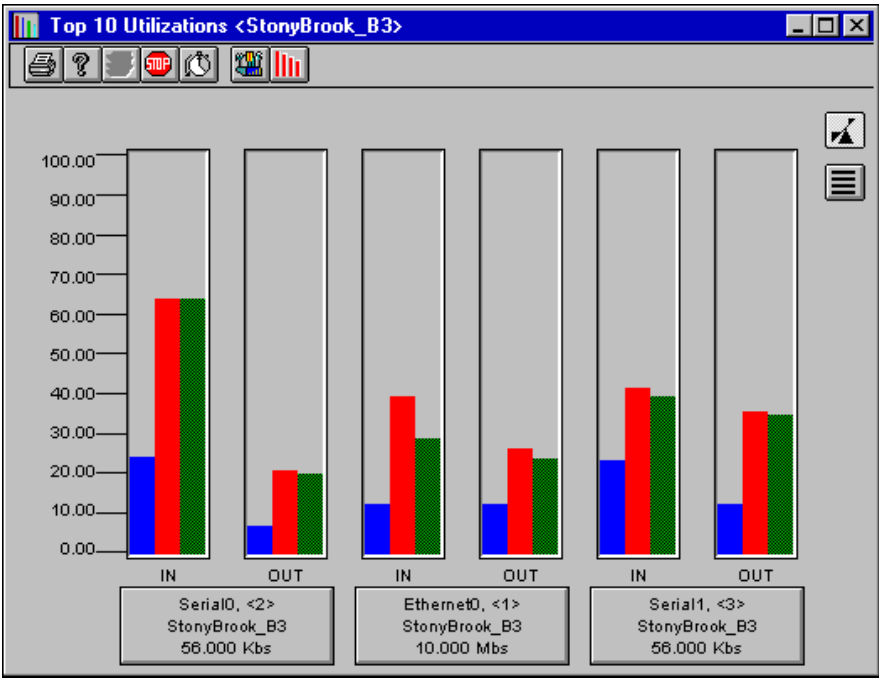


## Gauges

A gauge displays information in a vertical bar chart. The gauge monitors rising and falling of real-time quantitative data. Typically, at the bottom of each gauge you will see the name of the interface in question. Each colored bar represents a different statistic, such as current usage, historical high, and average usage.

By clicking the mouse on a colored bar, you can see precise usage statistics. Clicking the mouse outside the colored bar displays the type of information being displayed on the gauge.

In some gauges, double-clicking on the graph will drill-down into another applet, providing more detailed information.





### Scaling and Grids

The Y-axis (vertical) of every line graph can be scaled.

Click on the [Auto Scale Graph] button  to open the vertical axis scale buttons.



The Up and Down arrows  allow you to increase or decrease the graph scale. The [Auto Scale Graph] button will automatically reset the graph to the default scale.

As an aid in viewing the gauge, you can click the [Grid] button  to overlay a grid onto the gauge window.

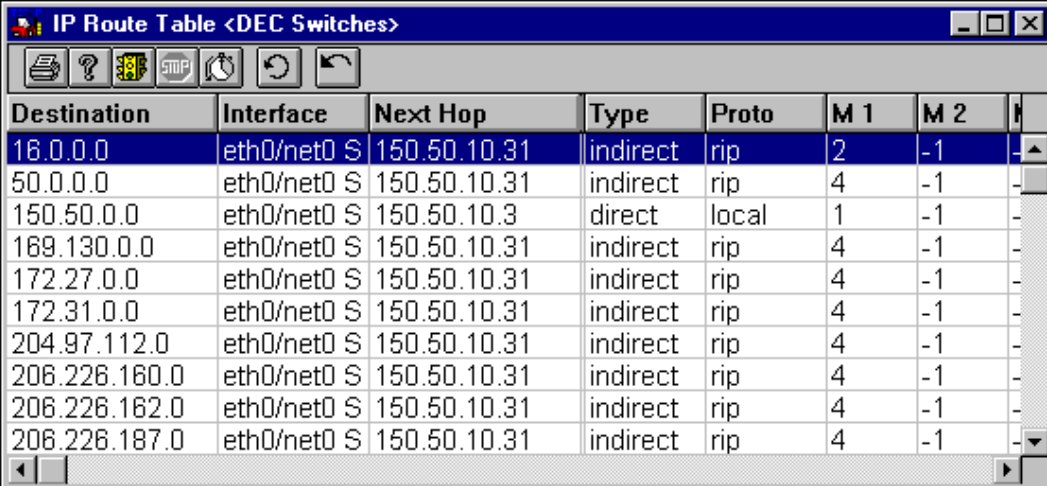
## Generic Functions

---

### Tables

A table displays information in a tabular format. Each row represents a device or interface, and columns display specific types of information about each device or interface.

In many instances, clicking on a line in a table will launch another applet. Also, some tables will allow you to launch other applets from the toolbar.




Destination	Interface	Next Hop	Type	Proto	M 1	M 2	
16.0.0.0	eth0/net0 S	150.50.10.31	indirect	rip	2	-1	▲
50.0.0.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	■
150.50.0.0	eth0/net0 S	150.50.10.3	direct	local	1	-1	-
169.130.0.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	-
172.27.0.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	-
172.31.0.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	-
204.97.112.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	-
206.226.160.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	-
206.226.162.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	-
206.226.187.0	eth0/net0 S	150.50.10.31	indirect	rip	4	-1	▼

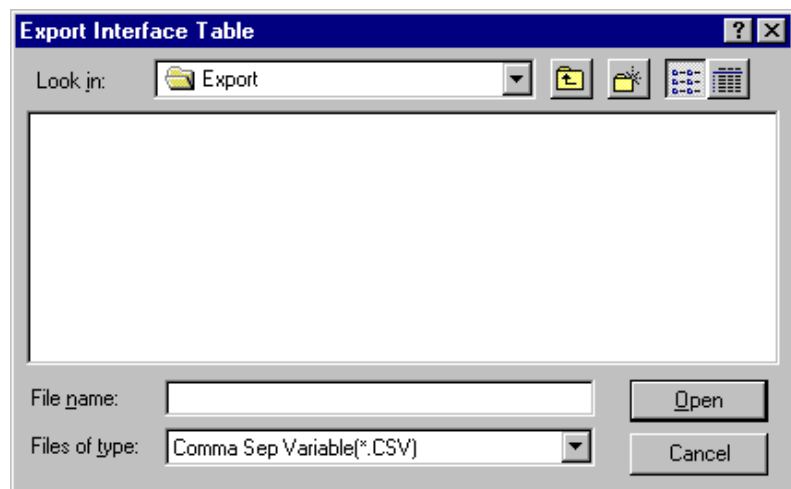
## Exporting data

Data can be exported from tables that collect calculated data. When data is exported, all fields within a table are enclosed in quotation marks and separated by commas.

### To Export Data

1. From the specific table, click the [Export Data] button  .

The Export Data dialog box appears:



2. Select the directory in which you want to store your data files.

By default, the data files are placed in the Export subdirectory of the directory to which you installed the program. If you want to store the data files in a different directory, use your pointing device to select the desired directory. Open directories are indicated by an open folder icon to the left of the directory name.

3. Specify the name of the file.

Type the name you want to assign to the file in the **File name** field. By default, data is exported to CSV (Comma Separated Variable) files. If you want to export your data to a different type of file, click the arrow at the right of the **Files of type** list box and select **All Files (\*.\*)**. Then, in the

## Generic Functions

---

File name field, type the full name you want to assign to the file, including the extension. For example, if you want to export to a text file named “iftable”, type “iftable.txt” in the File name field.

4. Click [Open].

The data is saved to the selected directory in the specified filename.

## The About applet

The **About** applet displays version, copyright, and user information for the program. Double clicking on the About icon in the Boxmap will display the About window.

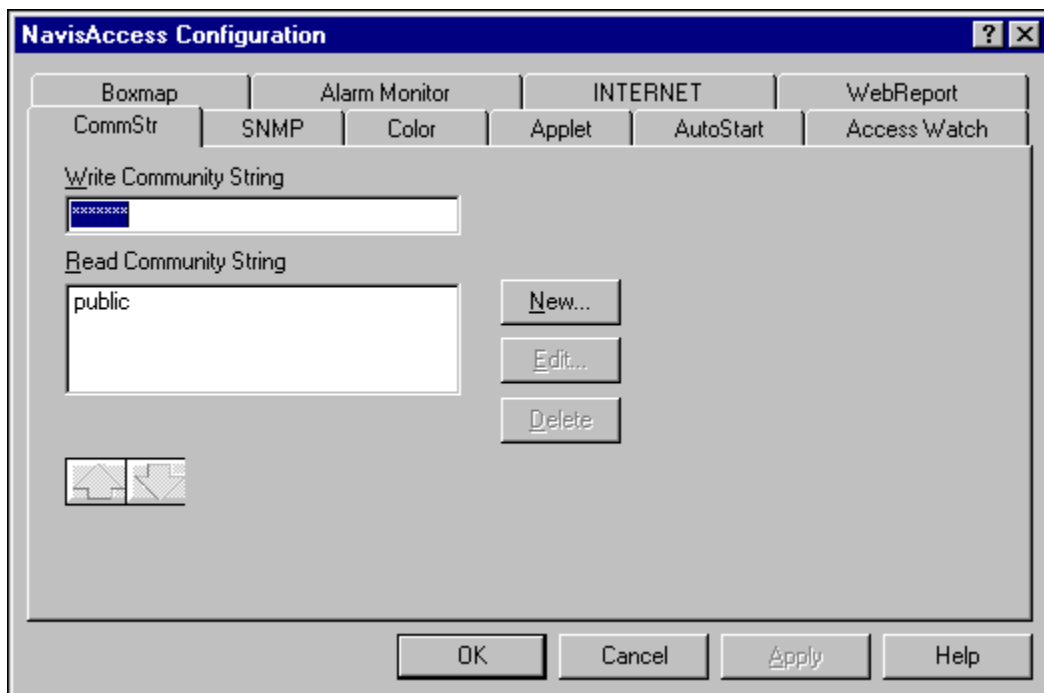
From the About icon, the information box will be specific for the device brand. You can also open the About information box by selecting, **Help > About** from the main menu.



## Introduction to configuring system options

**Menu Bar:** Config > System Options

NavisAccess allows for the setting of certain global configurations. These options are available from the System Configuration Dialog Box.



In order for a configuration change to take effect, the applet affected must be restarted. In some cases the parameters that have been changed will not take effect until after the full application has been restarted. These cases are noted below.

The following functions can be performed from the NavisAccess System Configuration Options dialog box:

- Changing the default read and write Community Strings that will affect new devices added to the NavisAccess database.
- Setting the SNMP options
- Configuring the Alarm options
- Setting the graph colors used by many of device's functions.
- Setting the Boxmap Default Poll Interval .
- Configuring the Boxmap Defaults to Show (or Hide) Interface(s) With Other Type.
- Changing the Applet Default Polling Interval which will affect new devices added to the NavisAccess database.
- Deactivating the [Stop] button (disables polling) on the IP Route Table toolbar.
- Setting the Internet map options
- Configuring the AccessWatch moving intervals, threshold levels and default secret.

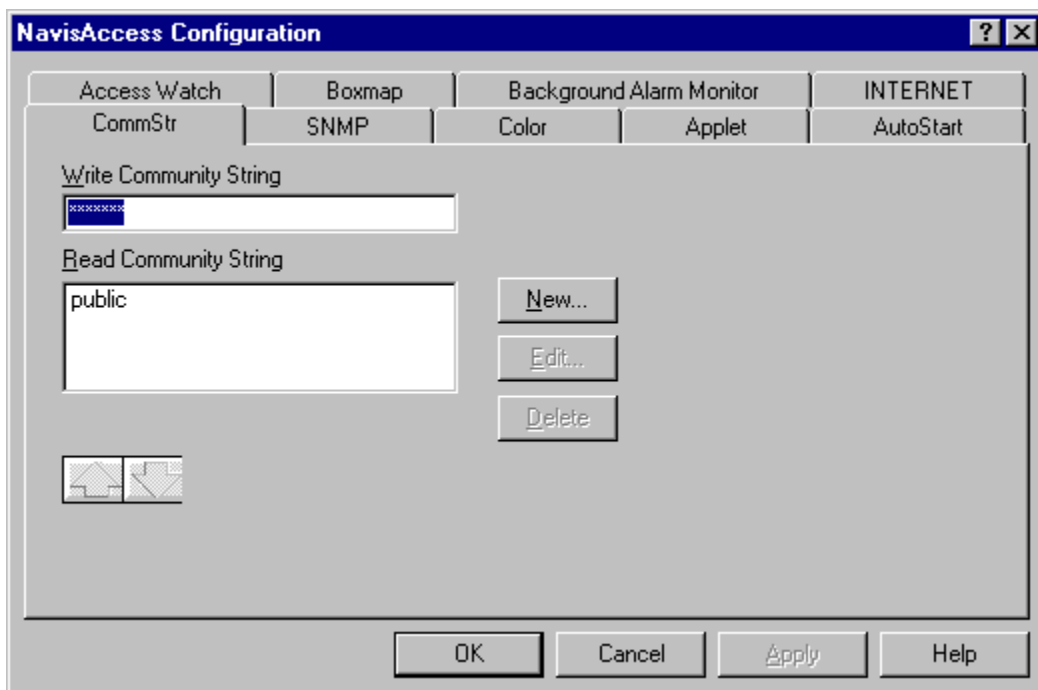
### The Community String tab

The CommStr tab allows you to enter a community string or strings. These strings are then available to use for any and all components of the network.

From the configuration CommStr Tab, click [New] to add additional Read Community Strings. New devices added to the database will try to establish communications through each of the Read Community Strings. As it cycles through the list from top to bottom, it finds the correct one, and then uses it. Select a listed Read Community String, and use [Edit] to change the string.

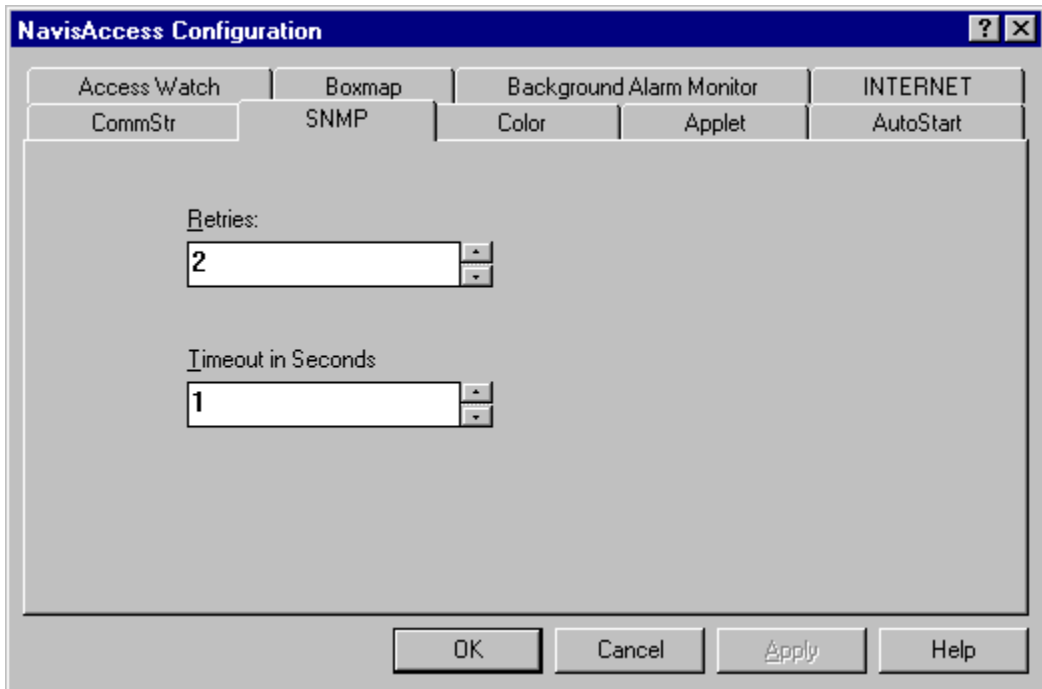
The [Delete] button will erase any selected Read Community String.

When all desired Read Community Strings are listed, click [OK] or [Apply] to add the list to the database.



## The SNMP tab

The SNMP tab allows you to specify the number of times the software will try to obtain the appropriate response, as well as the number of seconds each try will last.



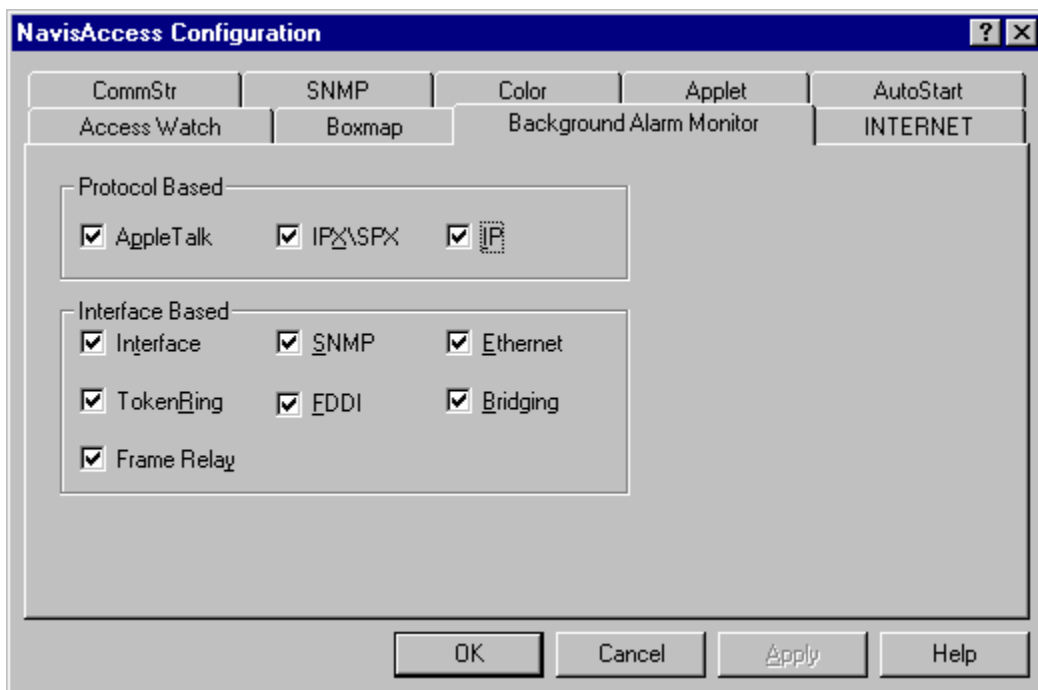
The image shows a screenshot of the 'NavisAccess Configuration' dialog box. The title bar is blue with the text 'NavisAccess Configuration' and standard window controls. Below the title bar is a tabbed interface with the following tabs: 'Access Watch', 'Boxmap', 'Background Alarm Monitor', 'INTERNET', 'CommStr', 'SNMP' (which is the active tab), 'Color', 'Applet', and 'AutoStart'. The 'SNMP' tab contains two settings: 'Retries:' with a spin box set to '2', and 'Timeout in Seconds' with a spin box set to '1'. At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

**NOTE:** This configuration item does not take effect until the next time NavisAccess is started.

### The Alarm Monitor tab

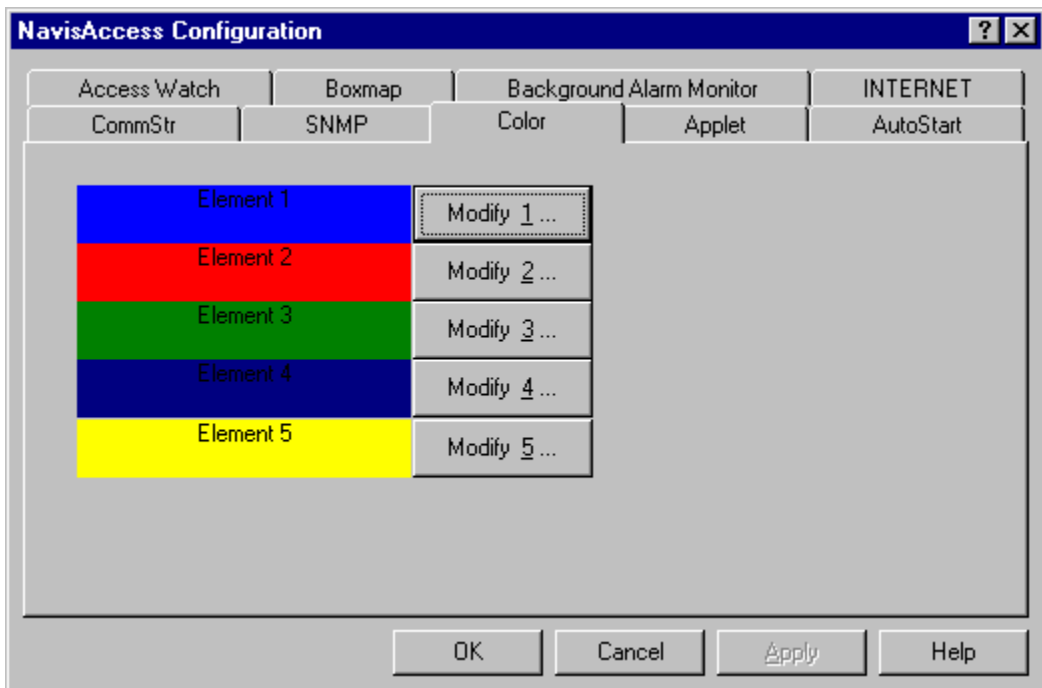
The Alarm Monitor lets you customize the Alarm options by specifying which protocols and interfaces will or will not generate alarms.

By de-selecting (un-checking) a check box, the Protocol/Interface associated with that check box **will not be monitored for Alarms**.



## The Color tab

The Colors used on graph displays can be changed from this tab. Each Element color box represents a color for a graph line. The color box labeled Element 1 displays the color for Element 1 on all graphs, the color box labeled Element 2 displays the color for Element 2, etc.

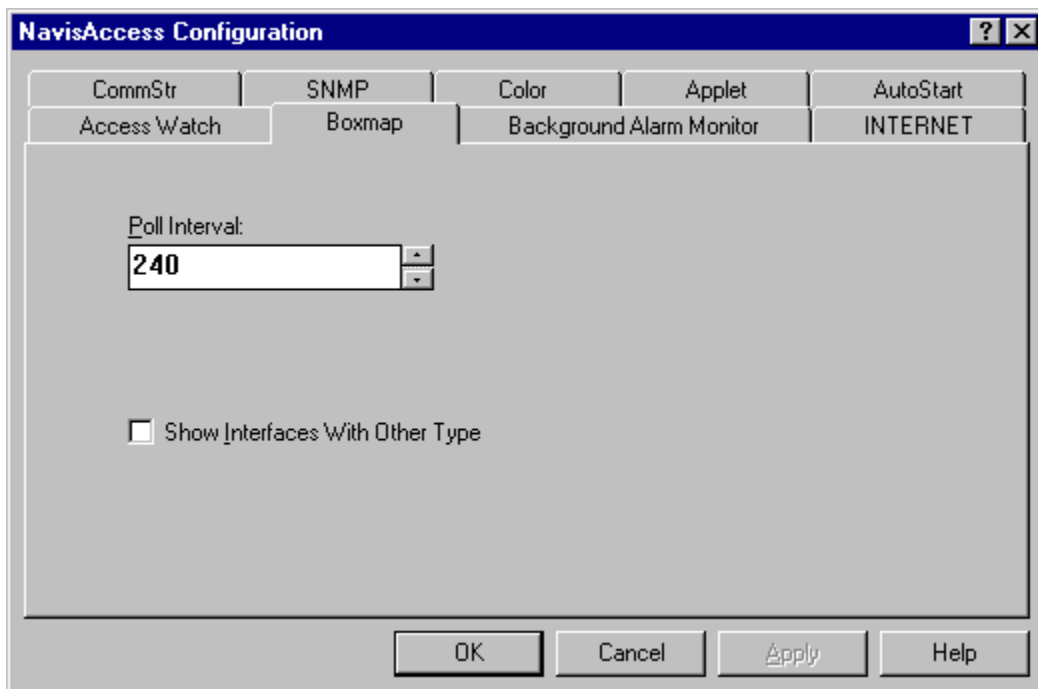


To change a graph element color, click the [Modify] button directly to the right of the corresponding element box in the System Options dialog box. This displays the Color dialog box which illustrates the available colors.

### To Change the Color of a Graph Element:

1. Click the desired color.
2. Click the [OK] button to change the color.
3. Or, click the [Cancel] button if no color changes are desired.

### The Boxmap tab



#### Poll Interval

The Poll Interval is the time period in seconds that passes before updating the contents of an open Boxmap. The polling interval for a specific Boxmap can be reset from within the Boxmap.

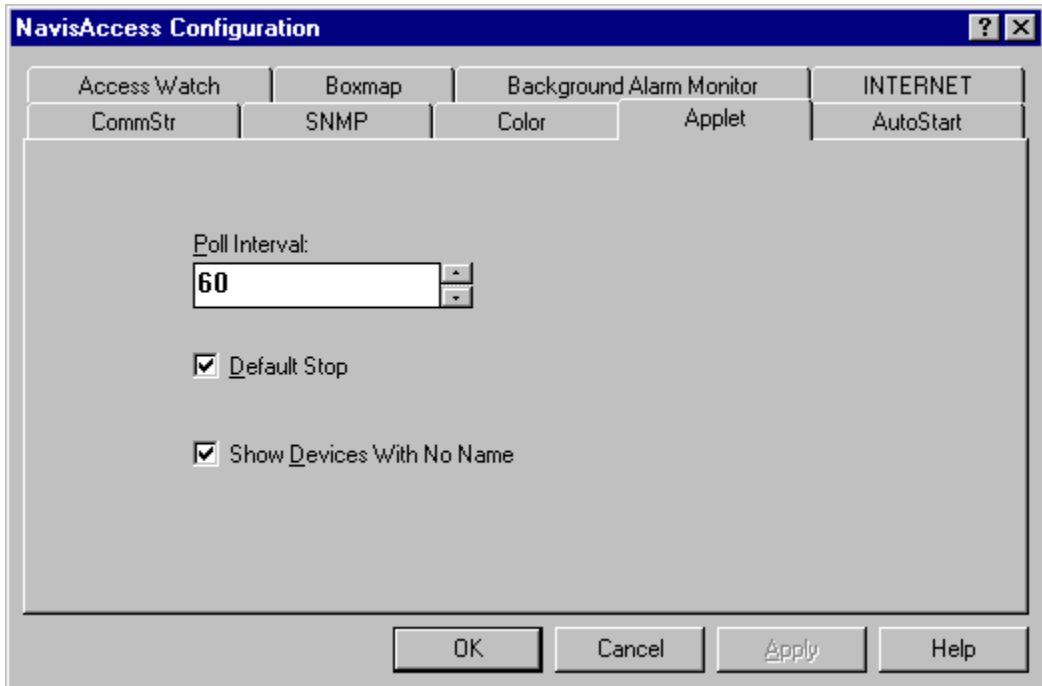
**NOTE:** This configuration item does not take effect until the next time NavisAccess is started.

#### Show Interface With Other Type

In the Device Boxmap interfaces are represented as icons. The status of each interface is indicated by the color-coded background. Boxmap Defaults can be configured to show/hide interfaces present in devices that have “other” type associated with them. They can be added to the database and viewed in the Boxmap. A check-mark activates the box.

## The Applet tab

The Applet Tab allows you to configure default settings for all applets.



The image shows the 'NavisAccess Configuration' dialog box with the 'Applet' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: 'Access Watch', 'Boxmap', 'Background Alarm Monitor', 'INTERNET', 'CommStr', 'SNMP', 'Color', 'Applet', and 'AutoStart'. The 'Applet' tab is active, showing a 'Poll Interval' spinner set to 60, and two checked checkboxes: 'Default Stop' and 'Show Devices With No Name'. At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Access Watch	Boxmap	Background Alarm Monitor	INTERNET
CommStr	SNMP	Color	Applet
AutoStart			

Poll Interval: 60

☒ Default Stop

☒ Show Devices With No Name

OK Cancel Apply Help

### Poll Interval

Set the Applet default polling interval for all new devices added to the database. (Polling intervals for individual devices can be changed at any time.)

### Default Stop

If the Default Stop check box is checked, when the IP Route Table applet is started, polling will be disabled. This will gray out the [Stop] button on the IP Route Table toolbar.

### Show Devices With No Name

The Show Device(s) function can be configured to show/hide devices which have been added to the database, but have no name. A check-mark activates the box.

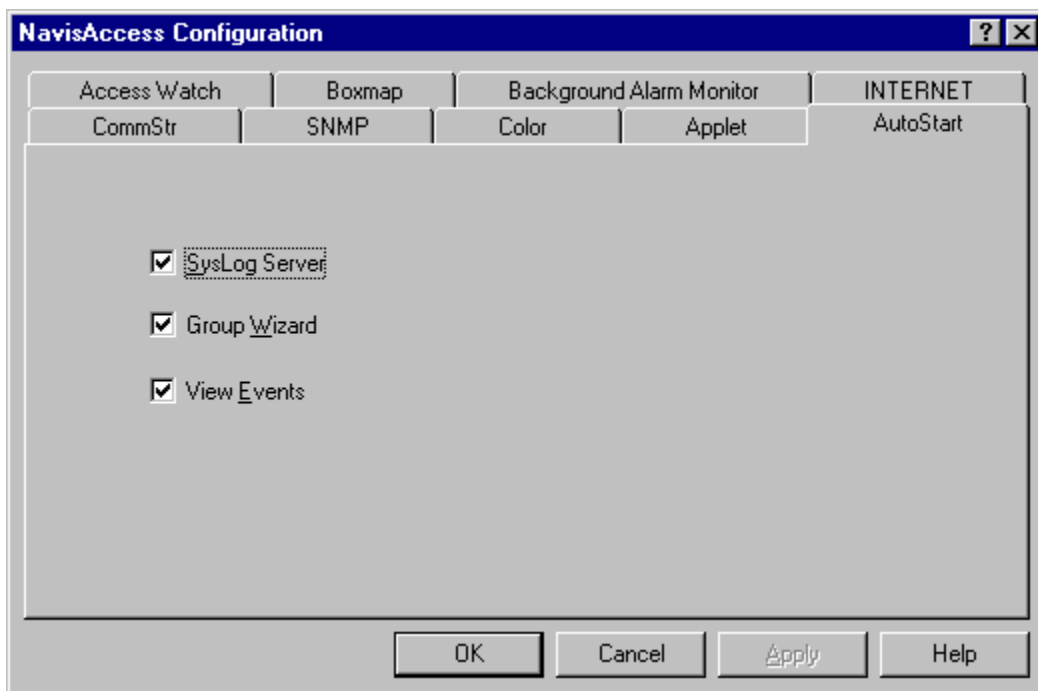
**NOTE:** This configuration item does not take effect until the next time NavisAccess is started.

## System Options

---

### The AutoStart tab

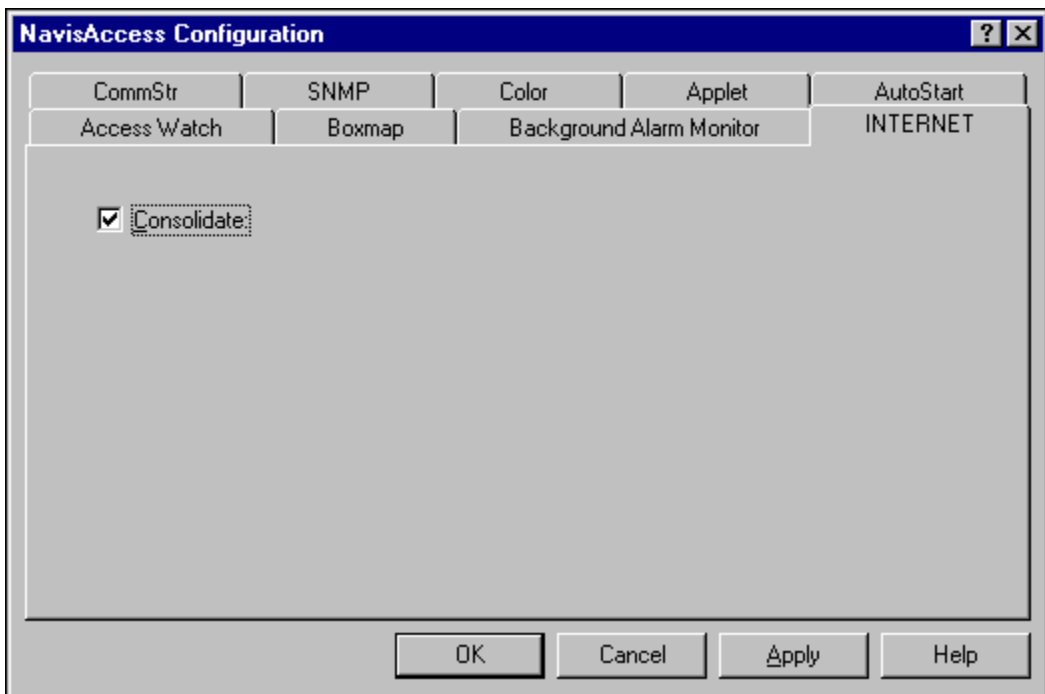
This tab allows you to select which of the three default screens launch when the program starts. All three options are selected by default. Choose from SysLog Server, Group Wizard, and View Events.



**NOTE:** This configuration item does not take effect until the next time NavisAccess is started.

## The Internet tab

This tab allows configuration of the Internet Map. The default setting for the Internet tab is **Consolidate** selected. If the default is removed, for large networks the map may be very busy with excessive components shown.



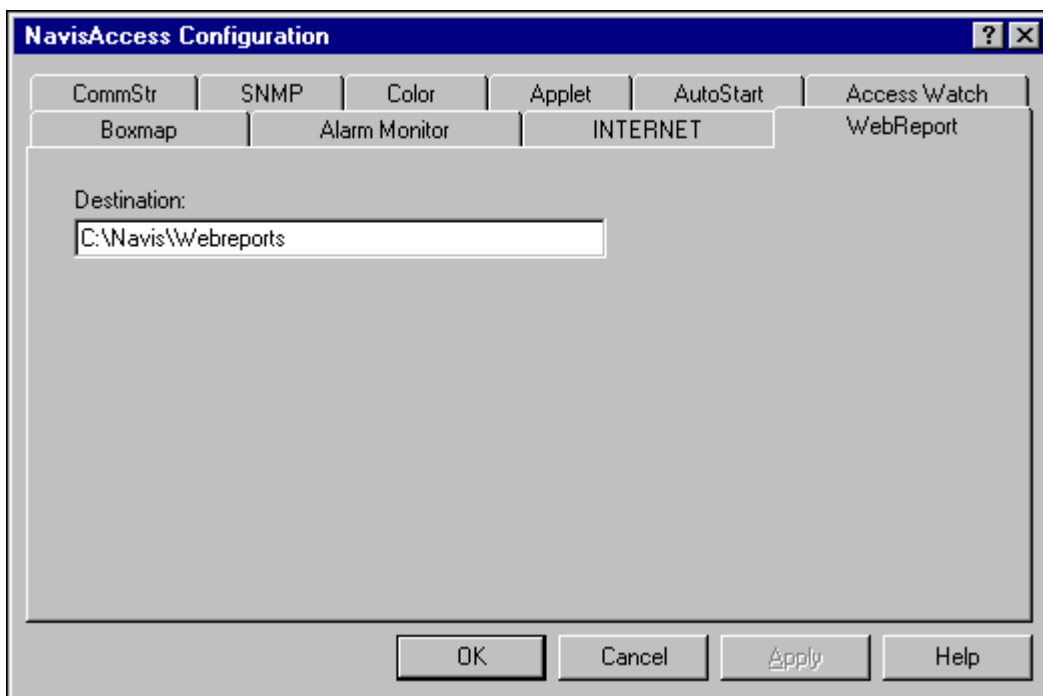
### Consolidate

When this option is selected, multiple IP addresses on the same physical segment are consolidated into one segment.

### The WebReport tab

The WebReport tab allows you to set the destination directory for HTML reports created by the DeviceDB program.

Enter the destination directory in the Destination field. Web-based reports will be delivered to the listed directory, into a sub-directory called **rootreportdir**.





**Applet**

A sub-application which can be run on a device. All Applets are started from the Boxmap.

**AppleTalk**

A communications protocol created by Apple Computer. There are two phases of AppleTalk. Phase 1 and Phase 2. Phase 2 has support for internetworks.

**ASCII**

American Standard Code for Information Interchange. Basic text file, to which IntraNet Manager will export information.

**ASN.1**

Abstract Syntax Notation One. An OSI language for describing data types independent of particular computer structures and representation techniques.

**Beacon**

A signal from a TokenRing device which indicates a serious problem. The beacon contains the address of the affected device.

**BECN**

Backward Explicit Congestion Notification. The number of frames received from the network indicating backward congestion.

**BRI**

Basic Rate Interface. An ISDN subscriber line, consisting of two 64 kbit/s B channels, or "bearer" channels, and one 16 kbit/s D channel, used for both data and signaling purposes.

**Checksum**

A means of testing the integrity of transmitted data. A checksum is a value computed using a sequence of octets. The value is computed before sending, re-computed upon receipt, and compared with the initial value for verification.

**CIR**

Committed Information Rate. The transport speed the frame relay network will maintain between service locations. CIR is typically contracted for at a specific capacity.

**Community Name**

A password entered for an SNMP read (get) or write (set) request.

**Critical Error**

A level of alarm severity in which an urgent problem has been detected. Immediate action is required to avoid critical degradation.

**Delta**

A calculation for protocol applets to display their real-time statistics. It is the difference between the parameter's last value and its current value.

**DLCI (Data Link Connection Identifier)**

In a Frame Relay network, DLCIs uniquely identify each virtual circuit. In most circumstances, DLCIs have strictly local significance at each Frame Relay interface.

**DS0**

1. A DS0 is a 64-kbps channel on a line using inband signaling.
2. A 64 kbit/s unit of transmission bandwidth. A worldwide standard speed for digitizing one voice conversation, and more recently, for data transmission. Twenty-four DS0's (24x64 kbit/s) equal one DS1.

**Element**

The word element can refer to a Virtual component (e.g. elements grouped together logically) or a Physical component of a network (e.g. device, switch or bridge).

**FCS**

Frame check sequence. Refers to extra characters added to a frame for error checking.

**FECN**

Forward Explicit Congestion Notification. The number of frames received from the network indicating forward congestion.

**Forward**

A packet received by a device and sent out to a destination is a forwarded packet.

### **Frame Relay**

A form of packet switching, but using smaller packets and less error checking than traditional forms of packet switching (such as X.25). Now a new international standard for efficiently handling high-speed, bursty data over wide area networks.

### **Framing**

At the physical and data link layers of the OSI model, bits are fit into units called frames. Frames contain source and destination information, flags to designate the start and end of the frame, plus information about the integrity of the frame. All other information, such as network protocols, and the actual payload of data, is encapsulated in a packet, which is encapsulated in the frame.

### **Grouping**

Specified individual devices can be selected for inclusion in a group. Typically used by a network manager for multiple devices contained within his/her area of responsibility.

### **ICMP (Internet Control Message Protocol)**

The Internet Control Message Protocol (ICMP) is an error reporting mechanism that is an integral part of the IP suite. Gateways and hosts use ICMP to send reports of datagram problems back to the sender. ICMP also includes an echo request/reply function (often referred to as PING) that tests whether a destination is reachable and responding.

### **Information Error**

A level of alarm severity in which information can be gathered.

### **Input**

A packet received by a device is an input packet.

### **IP**

Internet Protocol. A standard level 3 protocol in the TCP/IP protocol suite that directs packet forwarding between LANs.

### **IPX**

Internet Packet Exchange. The level 3 protocol used by Novell.

### **ISDN**

Integrated Services Digital Network. A system that provides simultaneous voice and high-speed data transmission through a single channel to the user's premises. ISDN is an international standard for end-to-end digital transmission of voice, data, and signaling.

**ITU**

International Telecommunications Union. A United Nations organization responsible for administering the X.25 protocol. The committee of the ITU responsible for data and voice communications is the International Telecommunication Union Telecommunication Standardization Sector, or ITU-T, formerly known as the CCITT.

**Kbs**

Kilobits per second. Also shown as Kbps.

**Local**

A packet generated by a device and sent to a destination is a local packet.

**Log Interval**

The time between writes to a database.

**Logging Data**

The storing of data (raw or calculated) in a historical database.

**MAC**

Media Access Control. The level 2 access mechanism used in Ethernet.

**Major Error**

A level of alarm severity in which a serious problem has been detected. Prompt attention is required to avoid major degradation.

**MIB**

Management Information Base. The database an SNMP-managed device uses to store information for TCP/IP networks.

**Minor Error**

A level of alarm severity in which attention is required for a problem that can be addressed under normal work schedules.

**MP**

Multilink PPP. A proposed standard for inverse multiplexing, a method of combining individually dialed channels into a single, higher-speed data stream. MP is an extension of PPP that supports the ordering of data packets across multiple channels.

### **MPP**

Multichannel Point-to-Point Protocol. A protocol that extends the capabilities of MP to support inverse multiplexing, session management, and bandwidth management. MPP allows you to combine up to 30 individual channels into a single high-speed connection.

MPP consists of two components: a low-level channel identification, error monitoring, and error recovery mechanism, and a session management level for supporting bandwidth modifications and diagnostics. MPP enables the Ascend unit to add or remove channels from a connection as bandwidth needs change without disconnecting the link. This capability is called Dynamic Bandwidth Allocation, or DBA.

Both the dialing side and the answering side of the link must support MPP. If only one side supports MPP, the connection uses MP or standard single-channel PPP.

MPP calls cannot combine an ISDN BRI channel with a channel on a T1 access line or a T1 PRI line.

### **NLM**

NetWare Loadable Module.

### **Octet**

Eight data bits.

### **OSI**

Open Systems Interconnection. A reference model used to describe layers of a network and the types of functions expected at each layer. The OSI model is used as a standard, letting developers of networks and communication systems rely on the presence of certain functions at certain places in a standard system.

Top to bottom, the seven layers are:

- application
- presentation
- session
- transport
- network
- data link

### ■ physical

The physical and data link layers have to do with hardware, wires, signals on wires, and basic addressing functions, such as media access control (MAC). In the network layer, information from different networking protocols is distinguished, which is where the Internet protocol (IP) functions. In the transport layer, data is packaged for transport in a size and organization appropriate for its intended environment. This is where transport control protocol (TCP) works. The session, presentation, and application layers keep information streaming in and convert it to a usable format.

### **Output**

A packet sent by a device is an output packet.

### **Packet**

A logical grouping of information that includes a header and, usually, data.

### **PDU**

Protocol Data Unit.

### **Per Second**

A calculation for protocol Applets to display their real-time statistics. It is the delta value divided by the actual polling interval. "Actual" takes into account network delays affecting the entered polling interval.

### **Polling Interval**

The time between requests to the device for real-time Applet information (e.g., performance statistics, alarms, utilization statistics, etc.). Each request is in actuality an SNMP get request.

### **PPP**

Point-to-Point Protocol. Provides a standard means of encapsulating data packets sent over a single-channel WAN link. It is the standard WAN encapsulation protocol for the interoperability of bridges and routers. PPP is also supported in workstations, allowing direct dial-up access from a personal computer to a corporate LAN or ISP. Using PPP ensures basic compatibility with non-Ascend devices. Both the dialing side and the answering side of the link must support PPP.

### **PRI**

Primary Rate Interface. An ISDN subscriber line, consisting of a single 64 kbit/s D channel plus 23 (for 1.544 Mbps) or 30 (for 2.048Mbps) B channels for voice and/or data.

**RIP**

Router Information Protocol. A protocol in the TCP/IP protocol suite which allows routers to advertise their known route addresses, indicating distance and difficulty of access, to other routers in an Internet.

**Router**

The words router and device are used interchangeably in this document

**SAP**

Service Advertising Protocol, a Novell IPX protocol through which network resources such as servers become known to clients.

**SNMP**

Simple Network Management Protocol. This is part of the TCP/IP protocol suite and allows a management station to query devices for information.

**SysDescr**

A MIB II system variable providing a textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this contain only printable ASCII characters.

**SysLocation**

A MIB II system variable indicating the physical location of the node (e.g., 'telephone closet, 3rd floor').

**SysName**

A MIB II system variable indicating an administratively-assigned name for a managed node. By convention, this is the node's fully-qualified domain name.

**SysObjID**

A MIB II system variable indicating the vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'XYZ, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'XYZ Router'.

**TCP/IP**

Transmission Control Protocol/Internet Protocol -- A family of protocols that defines the format of data packets sent across a network, and is the communications standard for data transmission between different platforms. The TCP/IP family consists of the following protocols and services.

**Transport protocols** - these protocols control data transmission between computers:

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)

**Routing protocols** - these protocols control addressing and packet assembly, and determine the best route for a packet to take to arrive at its destination:

IP (Internet Protocol)

ICMP (Internet Control Message Protocol)

RIP (Routing Information Protocol)

OSPF (Open Shortest Path First)

**Gateway protocols** - these protocols enable networks to share routing and status information:

EGP (Exterior Gateway Protocol)

GGP (Gateway-to-Gateway Protocol)

IGP (Interior Gateway Protocol)

**Network address services and protocols** - these services and protocols handle the way that each computer on a network is identified:

DNS (Domain Name System)

ARP (Address Resolution Protocol)

RARP (Reverse Address Resolution Protocol)

**User services** - these services provide applications a computer can use:

BOOTP (Boot Protocol)

FTP (File Transfer Protocol)

Telnet

Miscellaneous services

NFS (Network File System)

NIS (Network Information Service)

RPC (Remote Procedure Call)

SMTP (Simple Mail Transfer Protocol)

SNMP (Simple Network Management Protocol)

### **TFTP**

Trivial File Transfer Protocol. TCP/IP protocol usually is used for downloading software.

### **Traps**

Messages sent to a network management system by an SNMP agent. Traps are used to signify that a significant event has occurred, such as a network error or a threshold level being breached. Traps are sometimes referred to as events or alarms, but this documentation uses those terms for more specific purposes.

### **Unknown Error**

A level of alarm severity in which information is received by NavisAccess about a network event that may be the source of a problem.

### **Virtual Circuit**

A logical circuit set up to ensure reliable communication between two network devices. Data can travel through any number of intermediate nodes without dedicating any physical portions of the network. A virtual circuit can be either *Permanent* (known as a PVC) or *Switched* (temporary, known as an SVC).

### **X.121**

The address format used by the X.25 communications standard. X.121 addresses can be up to 14 decimal digits long. X.121 addresses are also referred to as International Data Numbers (IDNs).

### **X.25**

A communications standard that defines the packet format for data transfers in a public data network/wide area network. X.25 networks can be used to provide remote terminal access, and can be used for other types of data, such as DECnet and IP.

# INDEX

## 3

### 3Com specific

configuring	
line bandwidth .....	19
MIB variables .....	20
SNMP Community Names .....	17
SNMP managers .....	19
CPU Utilization applet .....	494
Ethernet Statistics applet .....	486
File Manager .....	179
Interface Tools	
overview .....	485
special considerations .....	17
TokenRing Statistics applet .....	488

## A

### About applet

details .....	613
---------------	-----

### Access Watch

Active Sessions.....	94
Call Monitor.....	94
configuring.....	90
configuring MAX and Pipeline.....	6
Dropped calls .....	83
Modem Pool .....	98
Modem Pools.....	96
overview.....	78
Slot Modem Table .....	99
starting .....	79
top level .....	80
WAN Line Channel Table .....	107
Wan Line Table.....	103

### Accounting applets

IP accounting.....	563
IPX accounting.....	565
overview.....	563

### Alarm Monitor

configuring.....	619
------------------	-----

---

overview.....	343
setup .....	343
starting .....	346
<b>Alert</b>	
overview.....	349
using .....	350
<b>AppleTalk</b>	
errors.....	326
<b>AppleTalk tools</b>	
overview.....	445
Route Table applet .....	448
Translation Table applet .....	450
<b>Applets</b>	
configuring.....	622
options .....	622
overview.....	603
parameters.....	604
types of .....	603
<b>Application View.....</b>	<b>115</b>
<b>Ascend specific</b>	
Chassis Report.....	205
configuring Call Logging	
MAX and Pipeline .....	6
MAX TNT .....	13
configuring SNMP community strings	
MAX and Pipeline .....	5
MAX TNT .....	11
configuring SNMP management	
MAX TNT .....	9
configuring SNMP Trap destinations	
MAX and Pipeline .....	3
MAX TNT .....	10
preparing devices for use with NetClarity .....	3
Radius Server applet.....	194
restricting SNMP manager access for the MAX .....	8
software uploads .....	177
special considerations.....	3
system reset .....	194
 <b>B</b>	
<b>Bay/Wellfleet specific</b>	
configuring	
line bandwidth .....	26

---

## Index

---

management priority to high.....	30
MIB variables .....	28
SNMP and Trap Sessions.....	21
File Manager .....	188
special considerations .....	20
<b>Binary Image applet</b>	
overview.....	177
<b>BOOTP Server</b>	
Clients tab .....	599
Files tab .....	601
Options tab.....	598
overview.....	597
<b>Boxmap</b>	
overview.....	112
<b>Bridging tools</b>	
Base Port Table .....	552
Learned Bridging applet .....	543
overview.....	542
Source Route Bridging applet .....	554
Spanning Tree Port Table .....	550
Static Bridging Table.....	548, 557
Telnet Show Commands applet.....	558
 <b>C</b>	
<b>Call Logging</b>	
MAX and Pipeline.....	6
MAX TNT.....	13
<b>Channels</b>	
active sessions .....	93
Wan Line Table.....	103
<b>Chassis Report</b>	
Ascend devices .....	205
Cisco devices .....	208
Digital devices.....	206
Digital Gigaswitch.....	208
overview.....	204
using .....	204
<b>Circuit maps</b>	
overview.....	139
<b>Cisco specific</b>	
Bridge Telnet Show Commands applet .....	558
Chassis Report.....	208
Clear ARP applet.....	416

---

clearing the interface .....	477
configuring	
line bandwidth .....	34
MIB variables .....	35
SNMP community names .....	32
SNMP packet size .....	34
SNMP Trap destinations .....	33
CPU Utilization applet.....	491
<b>Flash Manager</b> .....	183
Interface tools .....	472
ISDN Neighbor Table applet.....	496
Mean Packet Size applet .....	478
Mean Packet Size Distribution applet .....	481
special considerations .....	32
Utilization applet.....	472
Utilization Distribution applet .....	475
<b>Community string</b>	
configuring.....	617
<b>Configuration</b>	
changing community strings.....	155
Configuration applet.....	155
Configure Router applet.....	157
deleting a file from the database .....	166
<b>differences operation</b> .....	172
downloading a file.....	159
editing a file .....	167
erase memory .....	175
exporting a file .....	170
importing a file.....	171
overview.....	154
PathFinder.....	387
retrieving a file.....	167
saving a file.....	164
uploading a file.....	174
write memory .....	175
<b>Configuring</b>	
system options	
autostart .....	623
internet .....	624
WebReports .....	625
<b>CPU Utilization tools</b>	
overview.....	491

## Index

---

### D

#### Data

exporting .....612

#### Description applet

overview.....458

#### Device Database

backup and restore.....259

chassis information.....253

configuration file database.....256

database maintenance.....251

database tools.....258

deleting

    devices.....252

    interfaces.....252

    protocols.....252

overview.....249

reinitializing.....260

repairing.....261

reporting

    see Reports.....262

starting.....250

#### Digital Equipment specific

Buffer Protocol Resource applet.....573

Chassis report.....206

configuring

    interface bandwidth.....44

    SNMP Community Names.....40

    SNMP packet size (DECbrouter 90).....45

    SNMP System MIB variables.....43

    Traps.....40

Memory Protocol Resource applet.....571

special considerations.....39

#### Discovery

failure.....53

identifying an unknown device.....53

introduction.....47

multiple devices.....54

restarting.....53

troubleshooting.....53

visual indicators.....48

#### Dropped calls

disconnect codes.....83

---

**E****Errors**

AppleTalk .....	326
ethernet .....	329
FDDI.....	330
IP .....	327
IPX.....	327
source route bridging .....	331
TokenRing.....	328

**Ethernet**

errors.....	329
-------------	-----

**Event Report**

overview.....	356
using .....	358

**Event Viewer**

overview.....	351
using .....	355

**Explorer**

introduction.....	48
-------------------	----

**F****Fault detection**

Overview .....	315
----------------	-----

**FDDI**

errors.....	330
-------------	-----

**File Manager**

3Com .....	179
Bay/Wellfleet .....	188

**Files**

exporting .....	170
importing.....	171

**Flash Manager**

Cisco.....	183
------------	-----

**Frame Relay**

virtual circuit links .....	514
-----------------------------	-----

**Frame Relay tools**

DLCI Configuration applet.....	513
Frame Relay Interface Configuration applet .....	499
Frame Relay Virtual Circuit Link Statistics applet .....	509
Frame Relay Virtual Circuit Link Utilization applet.....	507
Frame Relay Virtual Circuit Statistics applet .....	504
Frame Relay Virtual Circuit Utilization applet .....	502

## Index

---

overview.....498

## G

### Graphs

colors .....620

### Group Wizard

creating groups.....70  
deleting groups.....74  
device grouping overview .....69  
editing groups.....74  
filtering devices .....67  
finding devices .....67  
linking groups.....74  
moving groups.....74  
overview.....64

### Groups

creating .....70

## I

### Icons

table of circuit icons .....153  
table of device icons .....149  
table of segment icons.....153

### Incident Monitor

overview.....360

### Interface Status Thresholds applet

overview.....339

### Interface Status thresholds

creating schedule.....341  
setting .....340

### Interface Table applet

overview.....452

### Interface tools

overview.....456

### Interface Utilization

overview.....333  
setting levels .....333

### Interface Utilization Thresholds

creating schedule.....335

### Internet Control Message Protocol (ICMP)

applet .....410

### Internet Map

---

adding a link.....	135
alarm functions.....	147
configuring.....	624
consolidate .....	143
cutting nodes .....	137
cutting, pasting, copying.....	126
drill down levels .....	139
grouping.....	130
launching applications .....	129
locating a device.....	124
moving icons .....	125
navigation and manipulation.....	122
Navigator.....	123
network filter.....	127
overview.....	116
reading .....	117
rollup .....	130
rollup example.....	131
saving.....	128
Search Node function.....	124
zooming in.....	146
<b>IP</b>	
errors.....	326
<b>IP tools</b>	
Address Table applet .....	407
Clear ARP applet.....	416
ICMP Statistics applet .....	410
IP Performance applet.....	400
overview.....	399
Route Table applet .....	403
SNMP statistics applet.....	413
Translation Table applet .....	408
<b>IPX</b>	
errors.....	327
<b>IPX tools</b>	
<b>compression information</b> .....	431
NLSP Area Addresses applet .....	438
NLSP circuit information.....	430
NLSP Learned Networks Table applet .....	443
NLSP Learned Routers applet .....	441
NLSP overview.....	435
<b>NLSP tools</b> .....	434
overview.....	417
Overview applet .....	427

## Index

---

Performance applet .....	418
Route Table applet .....	420
SAP Table applet.....	424
<b>ISDN Tools</b>	
Neighbor Table applet .....	496
overview.....	496
 <b>L</b>	
<b>Licenses</b>	
about .....	2
<b>Login</b>	
defaults .....	2
logging in.....	58
logging Out .....	62
 <b>M</b>	
<b>Mean Packet Size applet, Cisco specific</b>	
overview.....	478
<b>Mean Packet Size Distribution applet, Cisco specific</b>	
overview.....	481
<b>Memory applets</b>	
overview.....	567
<b>MIB tools</b>	
errors .....	592
MIB browser .....	577
examples.....	584, 587, 590
MIB compiler	
overview .....	575
using.....	575
overview.....	575
<b>Modems</b>	
active sessions .....	93
disconnecting a call .....	94
Dropped calls .....	83
modem pools .....	96
Slot Modem table .....	99
 <b>N</b>	
<b>NLSP circuit</b>	
information.....	430
<b>Novell MPR</b>	

---

configuring	
MIB variables .....	38
SNMP community names .....	36
SNMP traps .....	37
special considerations .....	35
 <b>O</b>	
<b>Output Queue Length applet</b>	
overview .....	464
 <b>P</b>	
<b>PathFinder</b>	
configuration .....	389
introduction .....	381
results .....	383
starting	
Internet Map .....	382
main window .....	381
virtual element .....	390
<b>Performance</b>	
<b>IP</b> .....	400
<b>IPX</b> .....	418
<b>Performance Distribution applet</b>	
introduction .....	393
using .....	394
<b>Physical View</b>	
overview .....	112
<b>Port applets</b>	
Group Port Info applet .....	559
overview .....	559
Port Utilization applet .....	561
 <b>R</b>	
<b>Radius configuration updates</b>	
Ascend devices .....	194
<b>Reports</b>	
Address Summary .....	309
AppleTalk Protocol Performance .....	299
Chassis Report .....	311
Configuration and Query	
creating .....	272

## Index

---

CPU Utilization .....	298
creating .....	267
Daily Active Sessions .....	291
Daily Average Network Connect Time.....	288
Daily Network Capacity.....	292
Daily Network Channel Availability/Utilization.....	287
Daily Number of Logins.....	290
Device Configuration.....	310
Device Summary .....	308
Device Version .....	312
exporting data.....	282
Frame Relay Daily Network Capacity .....	307
Frame Relay Hourly Network Capacity .....	306
Frame Relay Network Capacity Leaders.....	304
Frame Relay VC Utilization.....	302
graph functionality.....	314
Hourly Active Sessions .....	291
Hourly Average Network Connect Time.....	288
Hourly Modem Availability/Utilization .....	289
Hourly Network Capacity.....	294
Hourly Network Channel Availability/Utilization.....	287
Hourly Number of Logins .....	290
Interface Utilization As A Percentage Of Time.....	297
Interface Utilization Versus Time .....	296
Interface Utilization With Protocols .....	295
IP Protocol Performance.....	300
IPX Protocol Performance.....	302
Network Capacity Leaders .....	293
overview.....	262
performance report	
creating .....	265
running .....	270
Web reports.....	283
<b>Resetting</b>	
Ascend devices .....	194
<b>Resource applets</b>	
overview.....	567
<b>Route table</b>	
<b>AppleTalk</b> .....	448
<b>IP</b> .....	403
<b>IPX</b> .....	420

---

**S****SAP**

table applet .....	424
--------------------	-----

**Schedule Wizard**

## applications

AutoScan .....	216
Background Alarm Monitor.....	216
Background AppleTalk Performance.....	216
Background CIR Trending.....	217
Background CPU Utilization.....	217
Background Image Uploader.....	217
Background Interface Utilization.....	218
Background IP Performance.....	218
Background IPX/SPX Performance.....	219
Configuration Uploader.....	219
Database Groomer.....	220
Device Change Control .....	219
Explorer.....	221
Interface Status Monitor .....	221

## creating schedules

Configuration Uploader.....	236
Device Change Control .....	240
Explorer.....	244
Frame Relay.....	228
Image Uploader.....	233
protocols, CPU utilization .....	223

data collection .....	214
-----------------------	-----

overview.....	211
---------------	-----

using .....	221
-------------	-----

**Security**

changing passwords .....	59
--------------------------	----

logging in.....	58
-----------------	----

overview.....	56
---------------	----

## users

adding.....	59
assigning rights.....	59
deleting.....	59

**Segment maps**

overview.....	139
---------------	-----

**SNMP**

configuring.....	618
------------------	-----

statistics .....	413
------------------	-----

Starting NavisAccess.....	1
---------------------------	---

## Index

---

<b>Subnet maps</b>	
overview.....	139
<b>System Log Monitor</b>	
overview.....	361
using .....	362
<b>System options</b>	
configuring	
alarm monitor .....	619
applets .....	622
boxmap .....	621
colors .....	620
community string .....	617
introduction.....	615
SNMP .....	618
<b>System/Interface errors .....</b>	<b>328</b>
 <b>T</b>	
<b>Telnet applet</b>	
configuring.....	201
overview.....	201
Show Commands applet.....	202
starting .....	201
<b>TFTP Server.....</b>	<b>196</b>
statistics tab.....	198
<b>Threshold Manager</b>	
creating a schedule .....	324
error types .....	325
overview.....	319
setting levels .....	320
<b>Thresholds</b>	
interface status .....	340
<b>TokenRing</b>	
errors.....	328
<b>Toolbars</b>	
overview.....	607
<b>Top-10 utilization applet</b>	
introduction.....	396
using .....	397
<b>Translation Table</b>	
AppleTalk .....	450
<b>Trap Handler</b>	
overview.....	363

---

## U

<b>Utilization applet</b>	
overview.....	459
<b>Utilization applet, Cisco specific</b>	
overview.....	472
<b>Utilization Distribution applet, Cisco specific</b>	
overview.....	475

## V

<b>Virtual Circuit Utilization applet</b>	
overview.....	461
<b>Virtual Elements</b>	
configuring.....	148
overview.....	148
PathFinder.....	390
using .....	149

## X

<b>X.25 tools</b>	
Administrative Table applet.....	521
Administrative Table Counter Variables applet.....	530
Administrative Table Overview applet.....	524
Administrative Table Timer Variables applet.....	528
Call Parameters Table applet .....	531
Channel table .....	471
Circuits applet .....	466
Operational Table.....	532
Operational Table Counter Variables applet.....	540
Operational Table Overview applet.....	535
Operational Table Timer Variables.....	538
overview.....	519
Statistics applet .....	469

