Ascend

NavisXtend

ARCHITECTURE GUIDE

Table of Contents

1. Introduction

The NavisXtend™ Architecture Guide contains detailed information about the features and structure of the NavisXtend applications. It also presents an overview of the core common NavisXtend architecture and how it is positioned to comply with the Telecommunications Management Network (TMN) framework.

2. Executive Overview

All of the NavisXtend applications share a common architecture that delivers next-generation management capabilities. Features include the following:

- Scalable client/server technology to meet the growth of large service provider networks; components can be added as necessary to expand management capabilities
- Completely distributed end-user access, distributed server deployment, distributed management functionality
- Reliability and security features that strengthen the integrity of the data network information
- Open, standards-based design for seamless integration into existing management infrastructure and third-party value-added applications
- Web-based access used to ease end-user access and reduce access costs associated with the purchase of client software and eliminate platform dependence

Each of the NavisXtend applications uses these core architecture features to deliver a scalable and distributed solution that grows with service provider networks, reduces operational costs, and enables the provisioning of new services.

3. Product Overview

The NavisXtend family consists of six applications, each of which fall under the Management Functional Areas (MFAs) defined under the TMN framework. Each application is responsible for a specific network management task (network provisioning, statistics collection, report generation, etc.). This ensures that NavisXtend is ideal for complex service provider networks that must perform multiple operations and distribute tasks regionally, nationally or globally. The NavisXtend suite of network management applications provides complete, multiservice, standards-based management of Ascend IP, ATM, Frame Relay, and SMDS backbone networks.

The NavisXtend applications today consist of the following:

- ***Provisioning Server*** automates configuration of cards, ports, circuits to speed delivery of new services.
- ***Accounting Server*** gathers detailed call information to support new customer billing plans.
- ***Statistics Server*** and ***Report Generator*** customize reports on all network operational information for operations planning or for distribution to customer accounts.
- ***Fault Server*** intelligently correlates fault data to focus trouble-shooting tasks and improve prevention of network outages.
- ***Standby Server*** increases database reliability to support disaster recovery plans.
- ***Customer Network Management Server*** enables implementation of new services, such as customer network viewing, to increase revenues and pave the way for Quality of Service (QoS) and Service Level Agreement (SLA) offerings.

NavisXtend applications can be run independently or together. Every NavisXtend application is based on client/server technology and runs under Sun Solaris UNIX on a SPARCstation. Applications can be run on stand-alone machines or bundled together on a shared machine.

Table 1 lists the NavisXtend applications and the products they manage.

Table 1 – NavisXtend Applications

Product Name	Fault Server V.1.0	Standby Server V.1.0	Provisioning Server V.2.0	Stat Server V.1.0/ Report Gen V.1.0	Accounting Server V.1.0	CNM Server V.1.1
CBX500	Yes	Yes	Yes	Yes	Yes	Planned 2.0
B-STDX 8000/9000	Yes	Yes	Yes	Yes	Planned 2.0	Yes
STDX	Yes	Yes	Yes	Yes	Planned 2.0	Yes
SA 100/600	Planned	Yes	Planned	Planned	Planned 3.0	Planned
IP Navigator™	Planned	Planned	Planned 3.0	Planned 3.0	Planned	Planned

Provisioning Server 1.0 manages Frame Relay and SMDS services. Provisioning Server 1.2 manages Frame Relay services only.

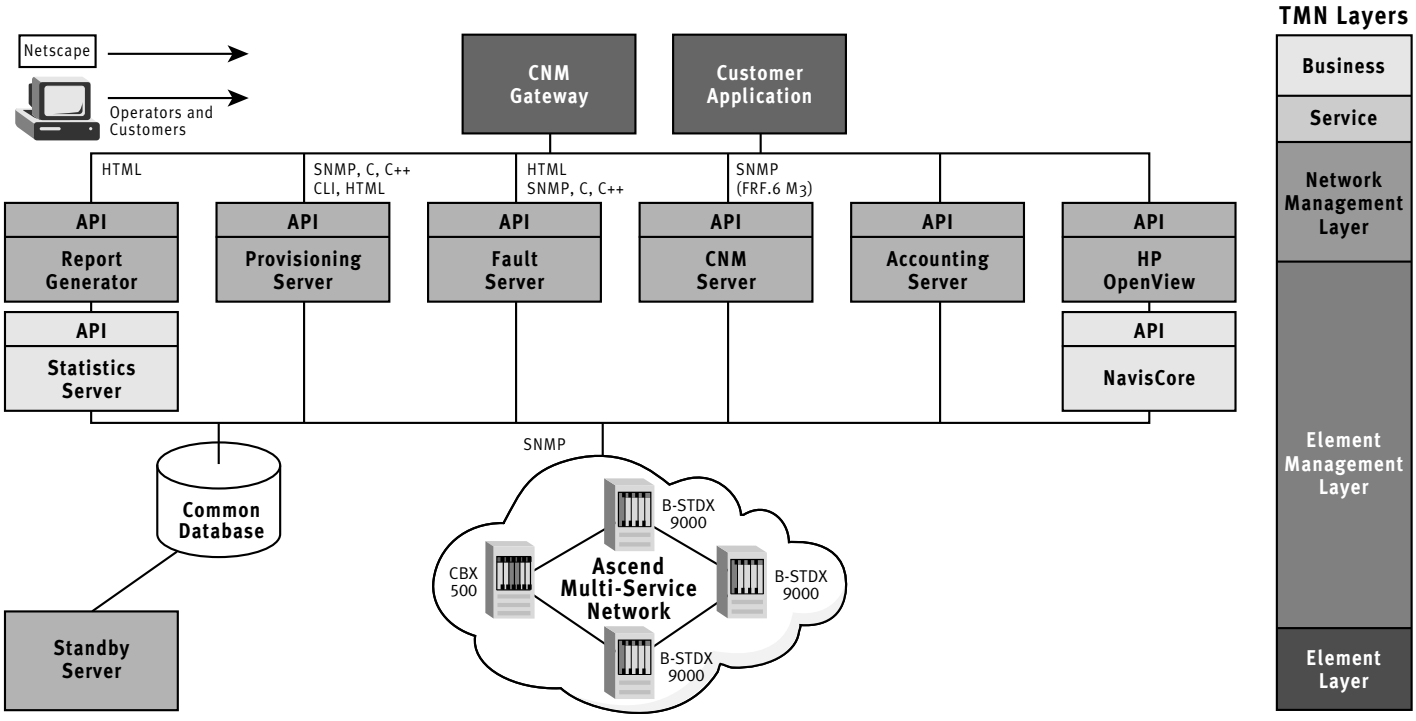


Figure 1 – NavisCore and NavisXtend applications work together to deliver comprehensive network management for Ascend switch networks.

4. Architecture Overview

All NavisXtend applications are built around a client/server architecture, with published Application Programming Interfaces (APIs) to allow for seamless integration into the service providers existing management infrastructure and any third-party applications in use.

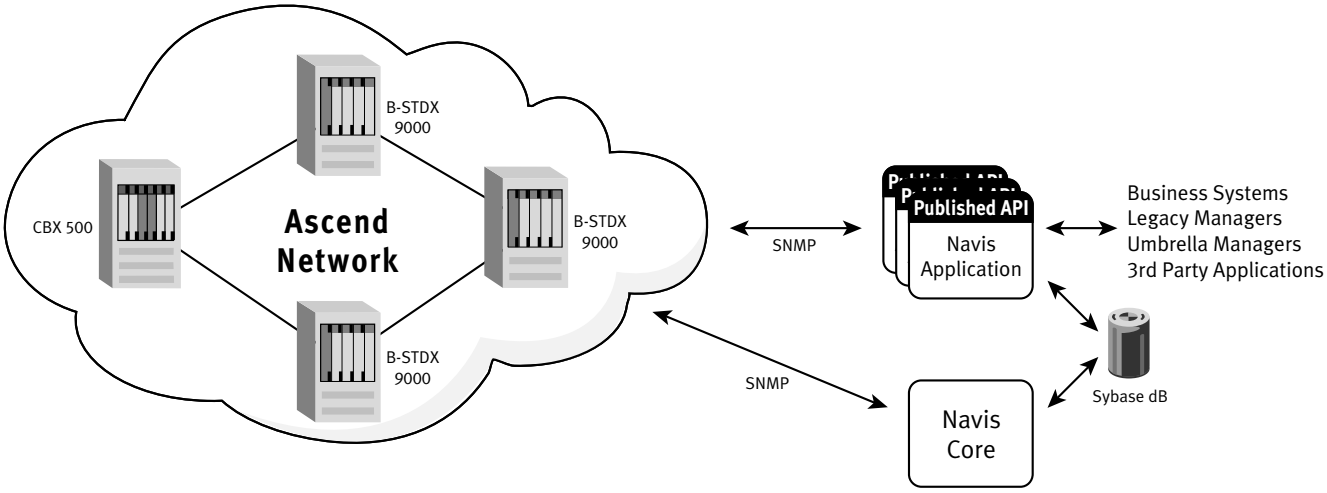


Figure 2 – NavisCore/NavisXtend Architecture Overview

As shown in Figure 2, each NavisXtend application communicates to all Ascend switch devices via SNMP. All applications provide multiservice support, handling Frame Relay, ATM, SMDS, and IP from within the single application. Accounting Server (currently ATM only) and CMN (currently Frame Relay only) are the exceptions.

The APIs are published, so that service providers can interface these applications into their existing systems, or use the Ascend Advanced Applications group to provide custom consulting and engineering.

The client/server architecture also allows the NavisXtend applications to be completely distributed. (See Figure 3.)

- Distributed end-user access
- Distributed management functionality, and
- Distributed geographic locations.

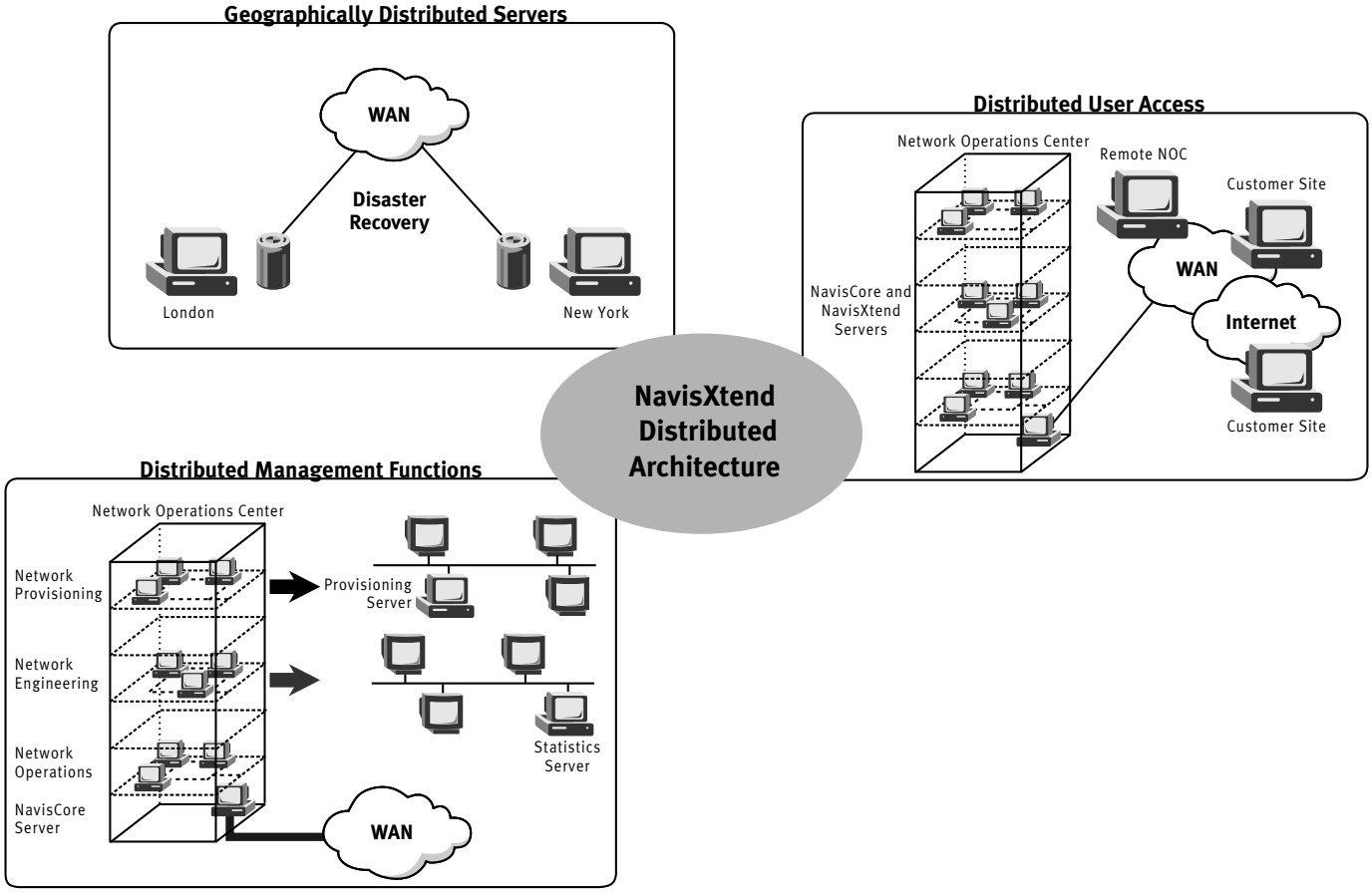


Figure 3 – NavisXtend Distributed Server Architecture

NavisCore™ (formerly CascadeView) and NavisXtend are both members of the Ascend Navis™ network management family umbrella. NavisCore provides centralized control of an Ascend switch network from a common NMS, using HP OpenView, Sybase and the NavisCore application software. The NavisXtend applications extend the functionality of the NavisCore application.

NavisCore is a required network management element for an Ascend switch network. NavisXtend applications are optional additions.

The development intention is to phase away from the centralized NavisCore applications and to provide replacement functionality under the NavisXtend servers with an added integrated GUI by 1998.

5. Support for TMN

The NavisXtend architecture fully supports the emerging standards recommended under TMN. The product architecture is completely standards-based, unlike some offered by other vendors. As shown in Table 2, different servers address different TMN layers and network management functional areas.

Table 2 – TMN Structure Model

	Network Management Functional Areas				
TMN Layers	**Configuration**	**Fault**	**Performance**	**Accounting**	**Security**
Service Management		CNM Server	Report Generator Accounting Server CNM Server	Accounting Server Statistics Server	
Network Management		Standby Server			
Element Management	Provisioning Server	Fault Server			
Network	SNMP Agent		Statistics Server		

TMN Explained

The ITU-defined Telecommunications Management of Networks (TMN) describes network management functions and domains. Originally defined for telecommunications environments, the model now applies more generally to any network management environment, that is, any mix of telephony and data networking.

TMN organizes the management space and suggests a way to organize the NMS software itself. Many service provider customers are adopting the TMN framework to standardize system responsibilities and interfaces to control the complexity of their systems environment.

Table 3 lists and describes the TMN layers.

Table 3 – Telecommunication Network Management Layers

TMN Layer	Description
Network Layer	The Network Layer is the network itself, providing core communications functions. From a management perspective, it also includes operations interfaces to management functions and data, for example, the SNMP agent or a local Web server.
Element Management Layer	The Element Management Layer (EML) provides management functions for individual network elements. It may be located directly within the network element, or in an external management system. The EML typically manages objects such as switches, shelves, cards, ports (pports and lports), trunk and circuit terminations, fans, and power supplies.
Network Management Layer	The Network Management Layer (NML) provides management functions across a group of network elements. The groups may be defined by Class B or Class C subnetworks or by arbitrary combinations of nodes, for example, administrative groups monitored by different Network Operations Center (NOC) technicians. NML functions are usually provided by an external NMS. Objects typically managed by the NML are trunks, circuits, subnetworks, and networks.
Service Management Layer	The Service Management Layer (SML) provides management functions outside the cloud. The SML does not have knowledge of how customer services are routed through the network; it is concerned with details such as customer endpoints and Qualities of Service (QoS). SML functions are layered on top of NML functions. The SML typically manages objects such as customers, virtual private networks, and QoS.
Business Management Layer	The Business Management Layer supports items such as management of business plans, strategies, pricing and product packaging. Business management functions are not directly related to networking technology and are usually tailored to specific companies.

Table 4 lists and describes the network management functional areas and the related NavisXtend application.

Table 4 – Functional Network Management Areas

Network Management Functional Area	Description	NavisXtend Application
Configuration Management	Configuration Management (CM) applications initialize, configure, and control network resources. At the element level, CM includes creating, retrieving, updating, and deleting cards, pports, and lports, and downloading switch software. At the network level, CM includes read and write operations on network connections (trunks and circuits). At the service level, CM includes read and write operations on items such as customers and QoS.	Provisioning Server
Fault Management	Fault Management (FM) applications monitor and respond to network alarm conditions. FM includes alarm generation, filtering, correlation, routing, and display. FM also includes diagnostic tools and automatic control actions.	• Fault Server • Standby Server • CNM Server
Performance Management	Performance Management (PM) applications monitor, analyze, and control network performance. Networks generate a large number of network and service- and protocol- specific measures. PM provides access to these measurements, displaying thresholding, trending and analysis, and threshold crossing alerts. Basic measures include signal measures at the physical protocol layers and throughput, drops, and utilization at the higher protocol layers. PM also includes traffic management displays and controls.	• Statistics Server • Report Generator • CNM Server • Accounting Server
Accounting Management	Accounting Management (AM) applications measure and report on usage, principally to support billing.	• Accounting Server • Statistics Server
Security Management	Security Management applications relate to the network and management data systems themselves. Security cuts across all of the above management function areas.	This spans all NavisXtend applications.

6. NavisXtend Applications

The following sections describe the NavisXtend application architectures.

Fault Server

The NavisXtend Fault Server (FS) application is an intelligent manager of network fault information; it handles the following functions:

- Sifting the volume of faults (or events) generated by the network to provide the network operator with the most pertinent and concise information. When a trap is received, the FS application correlates, parses, filters, and ages a trap through a number of rules-based processes. This way, only the critical service-affecting traps are reported to the operator.
- FS also forwards the consolidated alarm information as an SNMP message to any application that can accept SNMP traps, such as help desks and trouble ticketing systems. This allows service providers to consolidate fault information in a multi-vendor environment.
- Storage of all underlying faults in a Sybase database.
- Reliable trap delivery to ensure that traps are received from the switch network; this is handled through packet sequencing. If a packet is determined to be missing from the sequence, a request is issued to the switch to retransmit the missing information.
- FS also deploys a Web server, so that fault information is accessible via a standard browser (such as Netscape or Explorer).

Architecture

The Fault Server is made up of a fault server engine, Web-based client , Web server and database interface layer. Figure 4 illustrates Fault Server operation and the relationships between its components.

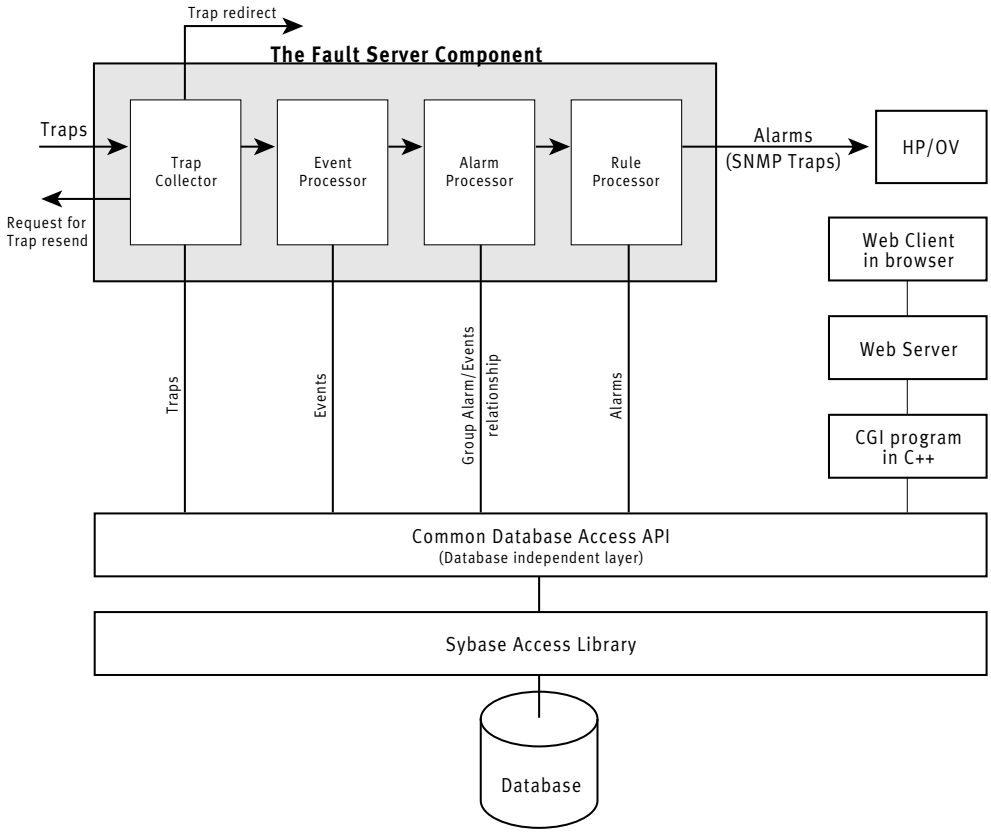


Figure 4 – Fault Server Architecture

A trap coming into the Fault Server application goes through the following steps (following the diagram from left to right):

1. The trap enters the Trap Collector that handles the collection and optional forwarding of traps to external applications.
2. Buffered traps are applied to the Event Processor to filter traps and map traps to events.
3. Buffered traps are applied to the Alarm Processor to filter, correlate, and group events into alarms. Events that generate alarms are forwarded to the Rules Processor.
4. The Rules Processor applies the alarms to the rule set that can include one of the following actions:
   - forwarding the alarm to another application
   - executing a script
   - aging the alarm
   - canceling the alarm
   - holding the alarm
   - incrementing the alarm
5. When the processing is complete, the user sees only the correlated trap that is forwarded to the third party application (such as HP OpenView node manager) as a standard SNMP trap. In addition to the HP (or third party) access, the operator can access the system via a standard browser (such as Netscape or Explorer). This access allows users a graphical view of the fault information from any platform.

All information is stored in the database so that the user can use standard SQL queries to the database to view network status to determine traffic trends and potential problems.

Table 5 describes the Fault Server components' architecture and their associated benefits.

Table 5 – Fault Server Architecture Components

Features	Description	Benefits
Trap Collector — SNMP Trap Collection, Filtering, and Forwarding	Switches send traps to the Fault Server where they are buffered, stored in a database, filtered, and optionally forwarded to other applications.	Reduces number of traps sent by switches (only need to send to the Fault Server, not to multiple NMS), amount of network bandwidth consumed by network management traffic, and load on gateway switches.
Event Processor — Mapping of Traps to Events	Traps are buffered and applied to an event map. The event map filters and maps traps into events.	Pre-processes traps and allows users to easily query the event database through the Web interface.
Alarm Processor — Mapping of Events to Alarms	Events are buffered and applied to an alarm map. The alarm map filters, correlates, and groups events into alarms. Events that generate alarms are forwarded to the Rules Processor.	Processes events into alarms (network problems that users are interested in); allows an event to generate an alarm, multiple alarms, or allows multiple events to generate one alarm; alarms are assigned a severity (critical, major, minor, warning, indeterminate, cleared) for easy identification and prioritization.
Rules-based processor — Cancel, Clear, Hold, Script Execution, Alarm Forwarding	Alarms are buffered and applied to a set of rules. Alarms are correlated and can be forwarded to other applications (as SNMP traps) or cause a script to be executed. Scripts can be used for alarm notification (e-mail, page, etc.). Scripts can also be used to execute other applications. Some alarm rules provided include aging, cancellation, clearing, holding, and incrementing.	Provides an intelligent alarm processing engine, condenses fault information presented to users, allows the Fault Server to be easily integrated with other management applications (such as help desks and trouble-ticketing systems).
Reliable Traps	Ascend switches with requisite software (B-STDX 8000/9000 [4.3 or later], Ascend CBX-500 [2.0 or later]) provide a sequence number within each trap sent. The Fault Server checks the sequence number, detects "lost" traps and attempts to recover them from the switches.	Ensures delivery of traps from switches to the Fault Server, attempts to recover "lost" traps, compensates for the "unreliable" nature of SNMP traps (SNMP over UDP/IP).
Web-based Graphical User Interface	Fault Server has a Web-based interface that uses Java applet technology. It displays Alarm Logs, Event Logs, Trap Logs, and Configurations (for Fault Server management).	Provides an easy-to-use, distributed, client/server interface; allows customers to use de facto standard Web browser applications on popular PC and UNIX computing platforms for Ascend switch fault management.

Features	Description	Benefits
Web-based Alarm Log	Alarm Log is the main monitoring interface. It lists all alarms (default is by severity) and allows the user to sort alarms based on date/time, type, or generation source. Users can perform complex queries to retrieve different subsets of alarms from the Fault Server. Alarms can be acknowledged, cleared, or assigned to a particular user. An alarm details window provides information on the alarm's probable cause, recommended action to take, a comments field for user-specific comments on the alarm, and the ability to set the state of the alarm. An alarm group window allows users to view all events associated with an alarm. Alarms can be printed or saved to a file.	Allows users to easily access alarms generated by Fault Server, understand the health of the Ascend network, and focus the troubleshooting efforts of network operations personnel.
Web-based Event Log	Event Log provides the ability to view some or all events in the event database. Users can perform complex queries to retrieve different subsets of events from the Fault Server. Events can be sorted based on date/time, event type, or generation source. Events can be printed or saved to a file.	Allows users to easily access events generated by the Fault Server.
Web-based Trap Log	Trap Log provides the ability to view some or all of the traps received by the Fault Server. Users can perform complex queries to retrieve different subsets of traps from the Fault Server. Traps can be printed or saved to a file.	Allows users to easily access traps collected by the Fault Server.
Web-based Configuration Interface	Configuration Interface allows users to show the Fault Server's status (CPU utilization, disk space used, and state [running, stopped]). It allows configuration of trap forwarding to other management stations/applications (IP addresses). Trap processing can be disabled in order to use the Fault Server to simply forward traps to other fault servers or other applications. It also provides the ability to start/stop the Fault Server.	Provides the ability to configure, control, and manage the Fault Server easily with a graphically-based interface; allows users to configure which management stations/applications received processed alarm information.
Fault Server Database	All traps, events, and alarms are stored in a Sybase relational database.	Allows the Fault Server to buffer traps/events/alarms (supporting high rates of trap generation from many switches), store fault information, and perform user queries through the client interface or standard SQL commands.

Provisioning Server

The NavisXtend Provisioning Server application automates the configuration of Ascend IP, Frame Relay, SMDS, and ATM networks to dramatically reduce provisioning overhead costs, through the following:

- Using an open API to tie provisioning tasks into the existing service provider order entry system. The API must be customized through the Provisioning Server toolkit which is included with the product and provides several coding options, including: C, C++, SNMP, or Command Line Interface (CLI). The API interface can be built by the service provider or by the Ascend Advanced Applications Group.
- The operator can chose batch processing options, allowing for scheduled release of configuration information to the network.
- If the CLI is used, the operator can also take advantage of script macros that can be tied into order entry systems as a speedy means to implement the integration.
- Provisioning Server and NavisCore share the same database to ensure that all updates are performed, even if both configuration methods are used.

The Provisioning Server can also be used to inventory switch nodes, cards, physical ports, logical ports, and circuits, as well as SMDS address, screen, and group objects.

Table 6 describes the main Provisioning Server applications.

Table 6 – Provisioning Server Applications

Component	Function
Provisioning Server	The Provisioning Server runs on a UNIX workstation. It uses SNMP over UDP to access the Ascend switch network.
Application Toolkit	The client toolkit consists of the APIs and CLI. The API may be used to write a C or C++ program. It is supported by include files and run-time libraries in the client toolkit distribution. To use the API, the customer's program includes the header files, which provide function prototypes, to link with the Ascend-provided library of routines. Configuration options in the client's run-time environment allow the client software to locate and use the Provisioning Server. Another option in the client toolkit is a set of command-line programs which may be used by clients for either interactive or batch provisioning of network objects. These programs may be invoked from any UNIX shell. While not intended to be as user-friendly as the NavisCore GUI, these commands are sufficient for an experienced user to perform provisioning operations.

Figure 5 shows the flow of data through the Provisioning Server application, as well as the interface to the third party application (typically the service provider order/entry system).

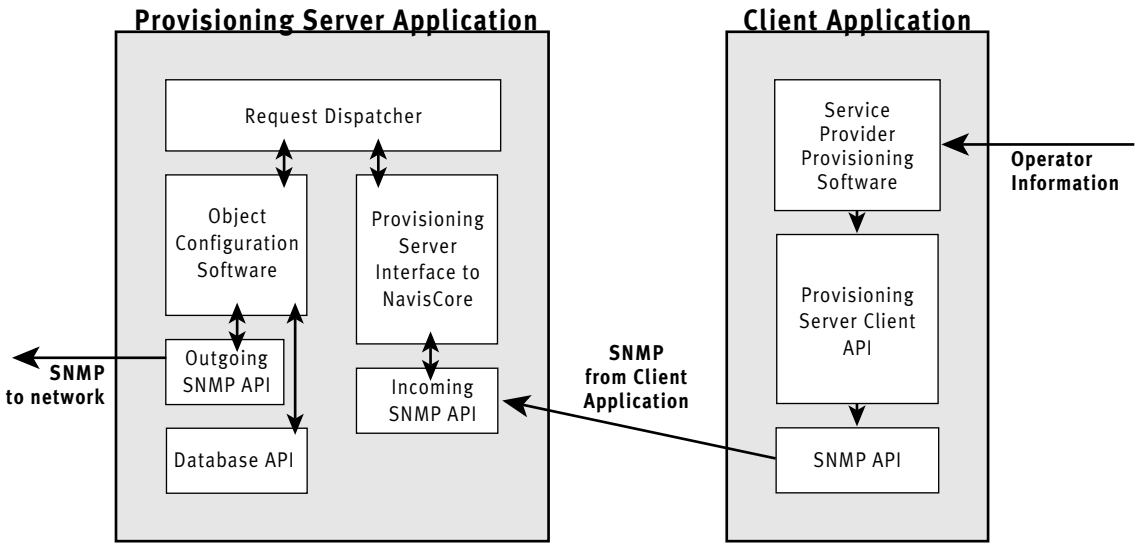


Figure 5 – Provisioning Server Architecture

Working from right to left, the following processes occur:

1. The service provider operator enters information into the client application regarding the end-user circuit configuration.
2. The information is sent to the Provisioning Server client API, which translates the request and forwards it as an SNMP message to the Provisioning Server application.
3. The Provisioning Server application receives the configuration request, maps the information to the Sybase database stored switch configuration, maps the appropriate SNMP command and issues the SNMP SET/s to the Ascend switch network.

The Provisioning Server supports the following major functions:

- AddObject(ObjectId, Attributes)
- DeleteObject(ObjectId)
- ModifyObject(ObjectId, Attributes)
- GetObject(Object, Attributes)
- ListContainedObjects(objectType, Attributes)
- ListAllContainedObjects(ObjectId, Attributes)
- AddMember(Object group, Object member)
- DeleteMember(Object group, Object member)

There are some restrictions on which functions can be performed, for example, the current release of Provisioning Server product does not support adding and deleting of entire switches or trunks, only the provisioning of those items already installed.

Statistics Server

The NavisXtend Statistics Server application collects real-time information on Ascend IP, Frame Relay, SMDS, and ATM networks for use by any standards-based, third-party application. (See Figure 6.) Service providers can use this real-time access to statistical information to extend their understanding and analysis of network operations, proactively plan for network growth, and uncover emerging network problems before service is affected. Service providers can also deliver tangible proof of service and QoS levels to their customer base, supporting the rollout of these new services and the generation of increased revenues.

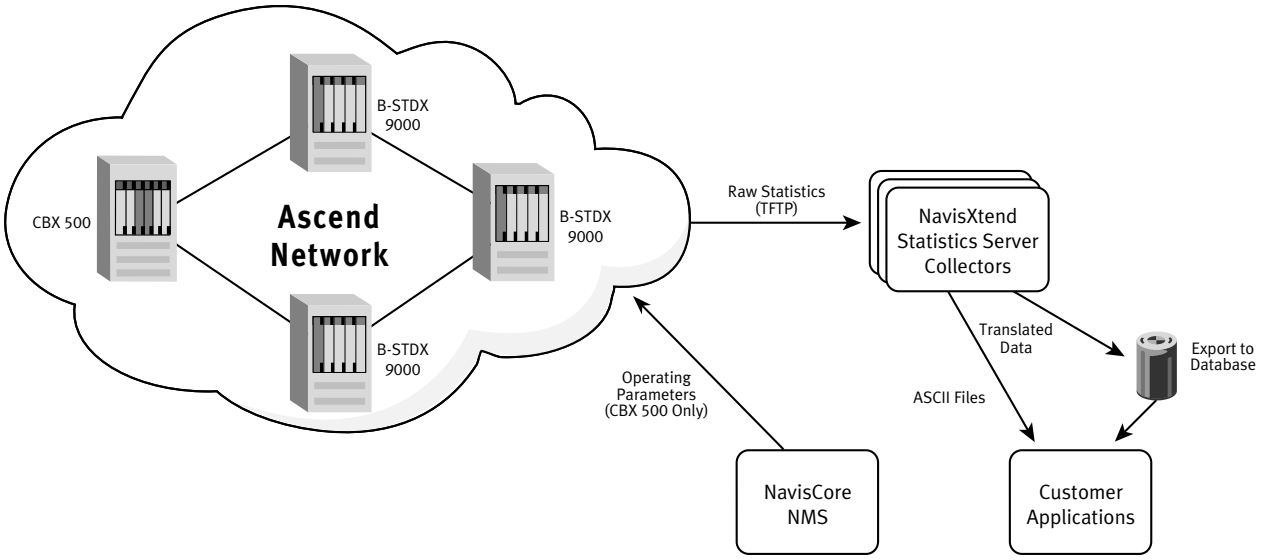


Figure 6 – NavisXtend Statistics Server Operation

Currently, two applications exist: one supports Frame Relay and SMDS; one supports ATM.

The following statistics are measured:

- ATM PVCs/SVCs
- Frame Relay trunks, UNI, NNI, PVC
- SMDS DX1/SSI

The following steps detail the data flow in the Statistics Server application.

1. The ATM Statistics Server receives statistics from each switch on a schedule defined according to the aggregate measurement period configured for each switch. At the end of a measurement period, the switch collects and transfers the statistics via the Trivial File Transfer Protocol (TFTP) to the, where the data is stored in a raw statistics file. The B-STDX/STDX Statistics Server polls each switch in the network to initiate the transfer of statistics data to the collector.
2. Translation of Statistics Data: Once the data arrives at the Statistics Server collector component, a translation application converts the raw statistics into one or more ASCII comma-delimited files, partitioned by the type of data. (For example, trunk statistics are stored in a file separate from circuit statistics.) Utilization calculations are also performed as part of the translation process. After translation, the data is optionally bulk-copied into Sybase.
3. Archival and Reclamation Processing: At midnight each day, the Statistics Server performs the following operations to reclaim disk space and archive collected statistics:
    - An optional user-defined script or application is executed to allow the users to perform their own statistics-related tasks.
    - The day's raw statistics files are time-stamped with the date the files were collected. The files are then made available for transfer to off-line storage.
    - Archived statistics files that are older than a user-specified number of days are purged to reclaim disk space.
    - Statistics Server entries in the Sybase database that are older than a user-specified number of days are purged to reclaim storage space in Sybase.

The Statistics Server was developed based on customer requirements and the Network Data Collection (NDC) portion of the Network Traffic Management/Network Data Collection (NTM/NDC) specification. The NDC measurements detect violation of service subscription parameters on PVCs, and establish trends in network traffic patterns and loads. The traffic load measurements count all NDC valid cells-all user/OAM cells submitted to Usage Parameter Control/Network Policing Control (UPC/NPC) before policing actions are taken. These measurements apply to incoming and outgoing traffic for all UNI, B-ISSI and B-ICI interfaces and are also done on a PVC basis.

SVC statistics are derived from the set of MIB objects defined in the svcmgt group of the Ascend MIB. This data includes per-port measurements of the number of SVCs established, the number of failed SVCs, and the number of connection requests for both point-to-point and multipoint circuits.

The Statistics Server provides both measurement period totals and five-minute peak statistics, with the length of the measurement period and the capability to generate peaks and totals configured on a per-IOM basis. The base collection period can be configured on a per-card basis with allowable values of 15, 20, and 30 minutes; 1, 2, 3, 4, 6, 12, and 24 hours (default value of one hour). Additionally, the capability to record peak and total values can be controlled on a per-card basis on each switch. For example, the user can configure a CBX 500 ATM switch to report aggregate counts and disable the recording of five-minute peaks.

Table 7 details the Statistics Server features and benefits.

Table 7 – Statistics Server Features and Benefits

Features	Description	Benefits
Five Minute Peak	The switch measures five-minute sample periods over a time span selected by the user. (See next feature.) The switch reports the maximum value (peak) of those samples.	Reduces information presented to users by calculating and reporting peak measurements from one or more samples.
Configurable Aggregate Measurement Period	From NavisCore, the user can configure the measurement period for the aggregate total from 15 minutes to 24 hours for each card in the switch. The default measurement period is one hour.	Provides user flexibility. User controls the granularity of the data and how much load is placed on the network.
Logical Port Statistics	Peak and hourly data is reported for ATM, UNI, and NNI ports in addition to the trunk and PVC statistics. Both ingress and egress counts are supported for UNI and NNI on lports.	Allows users to monitor usage across logical ports
SVC Call Statistics	Call statistics are reported for each UNI port.	Allows users to monitor SVC call history
Immediate Translation	Raw statistics data is translated immediately into decimal format when received by the Statistics Server and then optionally bulk copied into Sybase for archival.	Provides near real-time data for the customer
Sybase 11 Support	Database table fields use ANSI standard types that are supported fully in Sybase 11 (for example, numeric).	Use of ANSI standard data types in database tables provides for a more open interface to applications.
Script to Purge Old Database Entries	Users can delete old database entries that are n days old, where n is set by the user.	Allows customers to easily “clean up” their database
Script to Purge Old Archived Raw Statistics	Users can delete old raw statistics file entries that are n days old, where n is set by the user.	Allows customers to easily “clean up” their collection station
Co-residence of Statistics Server for B-STDX/STDX and Statistics Server for ATM	The Statistics Server for CBX 500 can reside on the same server as the Statistics Server for B-STDX/STDX. Additionally, ATM statistics can be stored in the same Sybase database that contains B-STDX/STDX statistics.	Reduces capital equipment costs and shares Sybase database

Report Generator

The NavisXtend Report Generator application uses the data stored in the database by the Statistics Server application to build tables and graphs. This application is based on technology OEMed from Actuate Software Corp. with Ascend modifications for the service provider market.

The Report Generator gives service provider the ability to generate reports for internal and external customers. Reports can be generated directly from the collected data or be accessed in a view-only mode.

The Report Generator does not interface directly with the switch but depends on output stored in the databases as a result of the Statistics Server collection process and switch configuration data from the NavisCore database. This reduces the number of management hits on the Ascend network, improving overall performance.

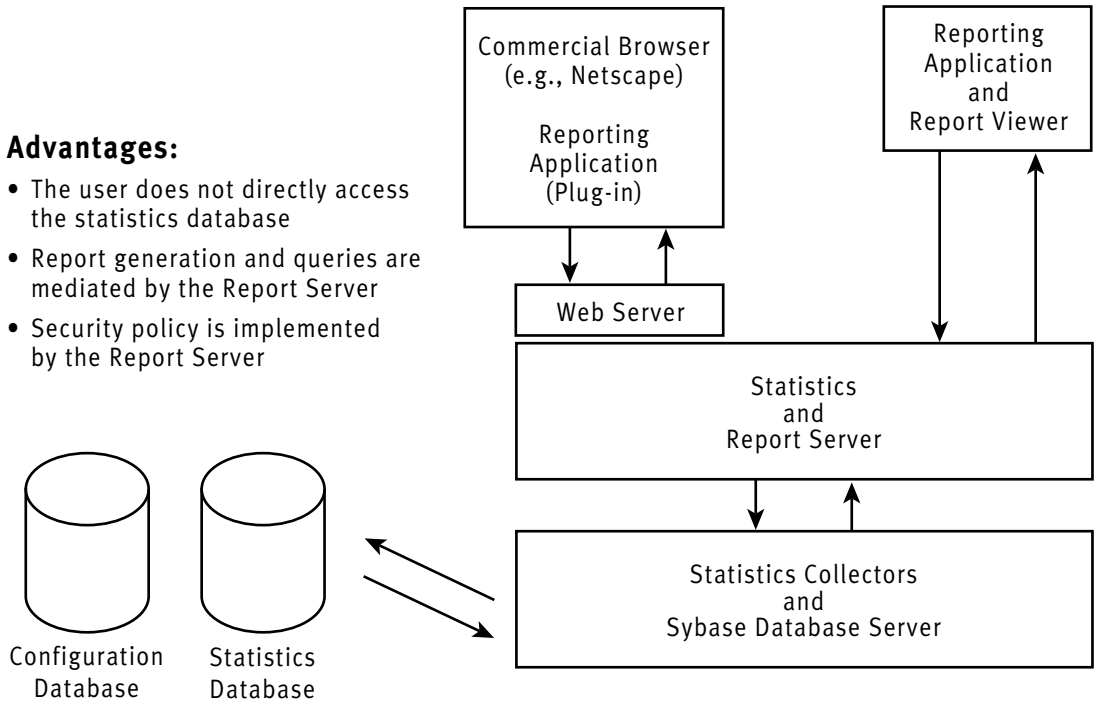


Figure 7 – Report Generator Architecture

Figure 7 shows the flow of data through the Report Generator application.

- A report request is made through either the Report Generator viewing application or a standard web browser.
- The Report Generator application mediates the request and also performs the security check to authorize the user access to the requested report.
- The data is retrieved from the database if the report is a new request, or the saved report is accessed; data collected from the separate data sources are filtered and correlated to provide meaningful output. The resulting report information is displayed to the end user.

As part of the Report Generator application, Ascend provides pre-formatted reports, including the following:

- Trunk Peak and Average Utilization Report
- PVC Peak and Average Utilization Report
- UNI/NNI Peak and Average Utilization Report
- DXI and SSI Peak and Average Utilization Report
- PVC Utilization Report
- Cell Trunk Utilization Report
- UNI/B-ICI Utilization Report
- SVC Call History Report

Both tables and graphs are available from these reports, and scope of the reports can be configured during the run request by the service provider. Figure 8 contains a report example.

Trunk Utilization Report per Hour (per Trunk)

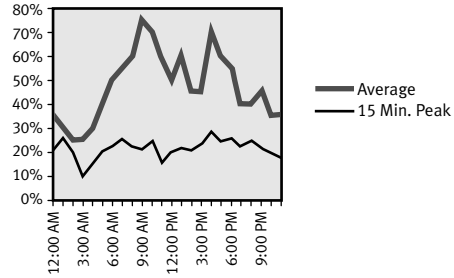
September 23, 1996

Node Name: aaaaaa **Slot:** qq **L Port:** xxx

TrunkName: nnnnnn **P Port:** nn **Port Speed:** 45 Mbps

	Inbound		Outbound	
Time	Average	15 Min. Peak	Average	15 Min. Peak
12:00 AM	20%	35%	20%	35%
1:00 AM	25%	30%	25%	30%
2:00 AM	20%	25%	20%	25%
3:00 AM	10%	25%	10%	25%
4:00 AM	15%	30%	15%	30%
5:00 AM	20%	40%	20%	40%
6:00 AM	22%	50%	22%	50%
7:00 AM	25%	55%	25%	55%
8:00 AM	22%	60%	22%	60%
9:00 AM	21%	75%	21%	75%
10:00 AM	24%	70%	24%	70%
11:00 AM	15%	60%	15%	60%
12:00 PM	19%	50%	19%	50%
1:00 PM	21%	60%	21%	60%
2:00 PM	20%	45%	20%	45%
3:00 PM	23%	45%	23%	45%
4:00 PM	28%	70%	28%	70%
5:00 PM	24%	60%	24%	60%
6:00 PM	25%	55%	25%	55%
7:00 PM	22%	40%	22%	40%
8:00 PM	24%	40%	24%	40%
9:00 PM	21%	45%	21%	45%
10:00 PM	19%	35%	19%	35%
11:00 PM	17%	35%	17%	30%

Hourly Trunk Utilization (Inbound)



Hourly Trunk Utilization (Outbound)

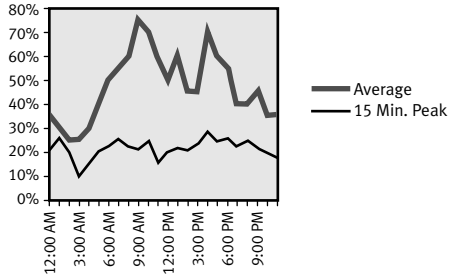


Figure 8 – Report Example

If the service provider wants to customize reports, a toolkit is available, or the work can be performed under contract by the Advanced Applications group in Westford.

Customer Network Management Server

The NavisXtend Customer Network Management (CNM) Server application works in conjunction with a service provider CNM Gateway to offer partitioned views of Ascend Frame Relay network to the service provider customers. CNM products allow service providers to deliver new services to their customers such as real-time status viewing, configuration checking, and fault forwarding. They also allow service providers to offer tangible proof of network operations to support QoS and SLA agreements. Today, Ascend offers one piece of the total solution. Over time, a more complete solution incorporating a gateway and support for other services will be offered.

CNM has gained increasing importance due to the end-user's need to monitor the health of their subscribed portion of the service provider's network. The overall function of CNM is to provide end users with "operator-like" information about their networks including operational status of network device and connections, performance statistics, trap alarm conditions, and configuration information.

The CNM Server allows Frame Relay end users the ability to administer and configure the status of logical ports and circuits that are assigned to them, by means of a proxy agent. The CNM Server is designed to work with a gateway that provides mediation services, such as user authentication and access level, between the end user (subscriber) and the CNM Server. The gateway receives end-user requests and communicates with the CNM Server via SNMP.

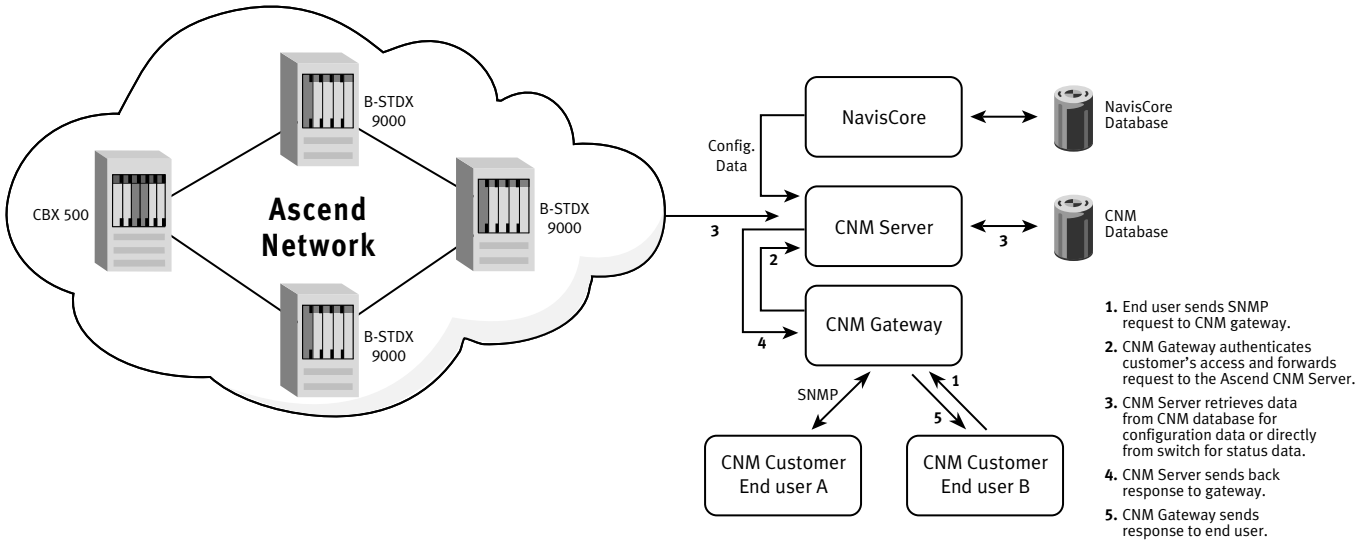


Figure 9 – CNM Server Response to End-user Requests

Figure 9 describes how CNM responds to end-user requests for configuration and status information.

1. The end-user NMS sends an SNMP request (GET or GETNext), which must pass through the service provider's CNM gateway.
2. Once the end-user request is validated, the gateway passes the request on to the CNM Server.
3. The Server then either goes directly to the Sybase database or to the switch, depending on whether the requested information is configuration information or statistical information respectively.
4. The Server then forwards the response back to the gateway which then passes the information back on to the end-user NMS.

For trap alarms and fault management purposes, the CNM Server receives the information directly from the switch. After converting the traps and validating against database, the CNM proxy agent sends the information to the gateway, which then forwards the information to the end user.

Table 8 describes the individual CNM components.

Table 8 – Customer Network Management Components and Functions

CNM Component	Function
CNM Server	The CNM Server acts as an external SNMP agent by responding to the CNM gateway's SNMP requests. It listens on two ports: the SNMP port and the Trap port. The SNMP port receives GET/GETNEXT requests from the CNM gateway. The CNM Server retrieves configuration requests from the CNM database and switch status information directly from the switch. The CNM Server sends the information back to the CNM gateway. The Trap port receives SNMP traps directly from the switch and forwards the traps to the CNM gateway.
CNM Gateway[1]	The CNM Gateway provides security and authentication and validates end-user requests. It also provides flow control on the number of end-user requests. After receiving configuration, operational status and fault management information from CNM Server, it forwards the information to the end user.
CNM Sybase Database	The CNM Sybase database stores the CNM tables and network configuration. The service provider must update the CNM database each time a circuit is added, modified or deleted.

[1]Note: The service provider provides this component.

Accounting Server

The NavisXtend Accounting Server application lets service providers collect information on ATM SVCs and PVCs on a per-call basis to bill customers based on network usage or duration. This detailed call information enables service providers to offer new, competitive data call plans and precise performance information on a per-call, real-time basis to their customer accounts.

The Accounting Server is responsible for the following:

- Storage/aggregation of raw usage data records
- Data record formatting
- Transmission of data records to other applications, such as billing systems

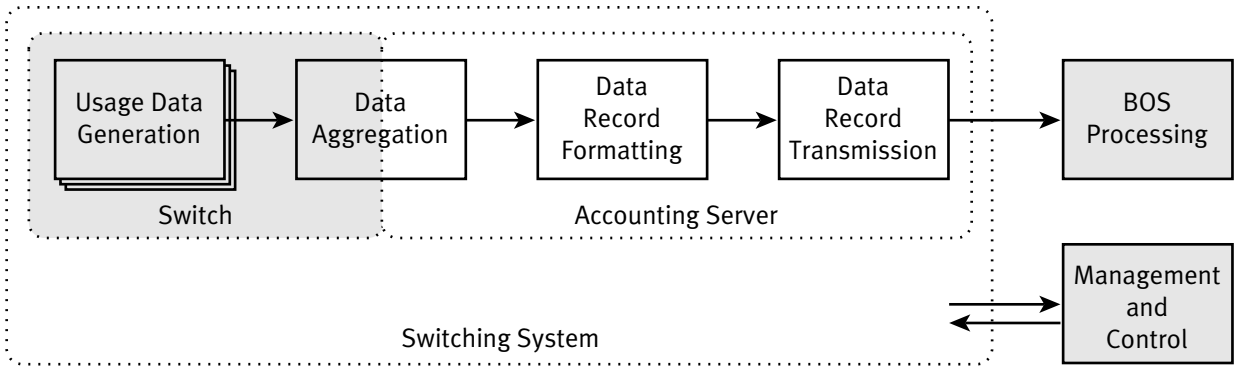


Figure 10 – Accounting Server Architecture

Figure 10 shows the data flow through the Accounting Server system, which includes both the Ascend switch to gather the statistics and the service provider billing software that actually handles the invoicing. Accounting Server sits between these two systems to provide efficient data collection by minimizing the number of SNMP requests to the network, as well as to handle data formatting.

The Accounting System is comprised of four main functions: Usage Data Generation, Data Aggregation, Data Record Formatting, and Data Record Transmission. Each one is described below:

- Usage Data Generation takes place within the Ascend switch. This function measures billable data traffic being switched through the network by interfacing with the lower level switching system components on the IOM, and the Data Aggregation function on the switch SP. It collects data based in response to normal asynchronous circuit events (e.g., call release), abnormal asynchronous events (e.g., trunk failure), as well as periodic synchronous events (e.g., end of recording interval).
- Raw usage data records are collected by the Data Aggregation function and stored in non-volatile storage on the Accounting Server hard disk until they can be retrieved by the Data Record Formatting function. The Data Aggregation function is also responsible for correlating multiple records pertaining to the same call (e.g., long-duration SVC updates).

- The Data Record Formatting function periodically collects the aggregated usage data and formats it into BAF records. The BAF Records are stored in Standard AMA files for later transport to the Billing Operation System (BOS) Processing function by the Data Transport function. After transferring the usage data to the Data Record Formatting function, the Data Aggregation function begins a new collection period.

  The length of time the Data Aggregation function collects usage data is different for SVCs and PVCs. For SVCs, the aggregation period is referred to as a *rate period*. For PVCs, this period is referred to as a *recording interval*. At the end of the aggregation period, the usage data is transferred to the Accounting Server; the Data Aggregation function then immediately begins a new aggregation period.

- Finally, the Management and Control function is used to configure the operational parameters of the network, and to view statistics on the performance of the Accounting System.

Within the switch network, the calls can be recorded at either the originating switch, the terminating switch, or both. All other switches along the circuit are referred to as intermediate switches and usage measurement statistics for billing are not collected at these points to increase efficiency.

Table 9 describes the functions found within Accounting Server.

Table 9 – Accounting Server Functions

Function	Description
SVC and PVC accounting	Usage measurement of intranetwork SVCs and intranetwork and internetwork PVCs, including point-to-point and point-to-multipoint circuits. Recording can be flexibly enabled at the originating end of a point-to-point circuit, at the terminating end of a point-to-point circuit, and at the terminating end of a point-to-multipoint circuit.
Support for both time-based and usage-based billing	The management parameters can be configured to support billing based on elapsed time of a circuit and/or on usage-based counts.
Support for near-realtime SVC billing	Billing records are produced within 15 minutes of the end of an SVC call or the occurrence of an unsuccessful call.
Management flexibility	Control over what is billed, when it is billed and how much information is recorded, including measurement of the following: • Cell counts on a switch-wide and per UNI basis for CBR circuits • Separate cell counts for CLP = 0 and CLP = 0+1 • OAM cell counts from reported cell counts • Unsuccessful SVC attempts (including the failure reason) at the originating and terminating ends • End-system subaddresses (ATM AESA private addresses) for both the calling and called party of SVC calls • Provide a default billing number or default ATM address for the UNI
Standards-based data output	Bellcore AMA Format (BAF) records, packaged into Bellcore Standard AMA files and comma-delimited ASCII format

Standby Server

The NavisXtend Standby Server application provides a warm standby for network management data created by the NavisCore application to maximize network uptime on IP, Frame Relay, SMDS, and ATM networks. The application protects the valuable data assets to allow service providers to provide continuous network operations. This high level of data integrity allows service providers to implement internal disaster recovery plans and to provide high-uptime service level agreements.

The Standby Server provides the following benefits:

- **Redundancy for the NavisCore primary database** – Standby Server protects data by replicating the primary database to a remote standby data server.
- **Recovery programs for primary database and all standby server components restoration** – If database systems fail, database administrators can use the Standby Server scripts and procedures to restore these components.
- **Improved database availability** – Third-party and Ascend applications can access the standby database in read-only mode, thus reducing traffic to the primary database.

The Ascend Standby Server is based on an OEM of the Standby Server from Sybase, with extensive customization by Ascend to make the product applicable for the service provider market. Customization includes the following:

- Procedures for setting up, installing, and managing the Standby Server environment and for performing database recoveries when systems fail.
- Scripts to install all the Sybase components and to configure these components for the Standby Server environment.
- Standby Server scripts to manage the standby environment and to recover database information in various failure scenarios. These scripts enable the service provider to switch databases, recover database information, monitor Standby Server components, run the warm standby in stand-alone mode, and stop replication.

Once the Standby Server is installed on the backup server (a separate server is required), the following processes transpire when updates are made to the primary database:

- The operator enters information into the primary database via NavisCore.
- The Log Transfer Manager for the active database retrieves the new transactions from the active database's transaction log for replication.
- The Log Transfer Manager forwards the transaction to the warm standby server, which writes them into a stable queue.
- The Standby Server submits transactions to the warm standby server.
- The warm standby server executes the transactions received from the Standby Server to update the warm standby database.

Upon failure of the primary database, the warm standby database is ready for operations, with minimal data loss.

The complete Standby Server system consists of the following components:

- Standby Server
- Active Log Transfer Manager used to read the transaction log and forward new data to the warm standby server
- Active Data Server
- Warm Standby Data Server
- Standby Server Manager Server used to monitor the status of the replication system via a graphical user interface
- Server hardware equipment at both sites

All software components are provided in conjunction with the product.

In addition, services are available from Ascend to ease Standby Server installation and configuration through the Professional Services group.

7. Summary

The NavisXtend applications deliver the next-generation management solutions to the service providers who are looking for scalable, distributed management that can reduce operational costs and increase new service revenues.

The NavisXtend applications can be deployed independently or together to meet the specific demands of the service provider network. Each NavisXtend application addresses a specific network management functional area, to allow service providers to divide management tasks and align management with business operations.

Although the specifics of each product differ, the NavisXtend applications all share a common architecture based on the following:

- Adherence to industry standards for data transport to the network and interface with existing service provider network management infrastructures
- Client/server architectures that are highly scalable, supporting the distribution of access, geographical location, and management function
- Movement toward Web-based interfaces to reduce client access costs and training issues
- Use of increased automation and use of intelligence to ease operational costs
- Support for delivery of new services to both internal and external customers.

NavisXtend is ready for the new service provider competitive environment, providing a strategic set of business tools for the business of networking.

Worldwide and North American Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

European Headquarters
Rosemount House
Rosemount Avenue
West Byfleet
Surrey KT14 6NP, United Kingdom
Tel: +44 (0) 1932.350.115
Fax: +44 (0) 1932.350.199

Japan Headquarters
Level 19 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07, Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Asia-Pacific Headquarters
Suite 1419, Central Building
1 Pedder Street
Central, Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2669

ASCEND

15-12-AG
09/97