Pipeline 50, 75 und 130
Anhang

Ascend Communications

Ascend Access Control, Dynamic Bandwidth Allocation, DSLPipe, MAX, MAX TNT, Multiband, Multiband MAX, MultiDSL, Pipeline und Secure Access Firewall sind Warenzeichen von Ascend Communications, Inc. Ascend und das Ascend-Logo sind eingetragene Warenzeichen und alle Ascend-Produktnamen sind Warenzeichen von Ascend Communications, Inc. Andere in dieser Publikation erwähnte Warenzeichen und Handelsnamen sind Eigentum ihrer jeweiligen Inhaber.

Copyright © 1997, Ascend Communications, Inc. Alle Rechte vorbehalten.

Dieses Dokument enthält Informationen, die Eigentum von Ascend Communications, Inc sind. Dieses Dokument darf nicht vervielfältigt, reproduziert, auf ein elektronisches Medium oder in maschinenlesbare Form übertragen oder anderweitig dupliziert werden, und die hierin enthaltenen Informationen dürfen weder verwendet, verbreitet oder anderweitig offengelegt werden, es sei denn, es liegt eine vorherige schriftliche Genehmigung von Ascend Communications, Inc. vor.

Januar 28, 1998 Teile-Nr. 0000-0000-000 Preliminary

Inhaltsverzeichnis

Kapitel 1 Konfiguration 1-1

Lesen Sie dies zuerst 1-2
Pipelines können Sprachrufe annehmen oder ablehnen 1-3
Konfigurieren mit einem Tastentelefon 1-5
Automatische SPID-Erkennung (nur Nordamerika) 1-8
„Data Usage“ für weitere Vermittlungsstellentypen 1-9
Anzeigen des Load-Namens 1-10
Alternative Anschlußnummern für Pipeline 130 1-12
Unterstützung langer Benutzernamen 1-14
Längere ausgehende Telefonnummern 1-14

Kapitel 2 WAN-Konfiguration 2-1

Parameter „Max Channel Count“ geändert 2-2
Schnittstellenunterstützung für MP-Rufverwaltung 2-2
BACP-Unterstützung über MP hinzugefügt 2-3
Pipeline MPP zieht neuesten Kanal zuerst ab 2-3
Inverse ARP für Frame Relay 2-4
Pipeline 50 und 130 als lokaler ATMP-Agent 2-4
Serieller WAN-V.35-Anschluß für Pipeline 130 2-7
FDL für T1-Leitungen hinzugefügt 2-12
Interner Taktgebermodus für Pipeline 130 T1 2-14
Flexibler Start für DS0-Ursprung in „Nailed T1“ 2-15

Kapitel 3 IP-Routing 3-1

IP-Sicherheit 3-2
Entfernen unterbrochener Hostverbindungen 3-25
Netzwerkübersichten für Adreß-Pools 3-28

Standard-Routen pro Benutzer angeben 3-28
Unterstützung von mehreren IP-Routing-Protokollen 3-30
Änderungen an der Routing-Tabelle und am Diagnosemodus 3-37
Routing auf Schnittstellenbasis 3-40
Multicast-Weiterleitung und IGMP-Funktion 3-45

Kapitel 4 IP-Adreßverwaltung 4-1

Network Address Translation (NAT) für ein LAN 4-2
BOOTP Relay 4-26
Erweiterte DHCP-Dienste 4-30
Erweiterte DNS-Liste 4-49
Benutzerdefinierbares Timeout für TCP-Verbindung 4-51
DNS-Server für Einwählbenutzer 4-54
Option für lokale DNS-Tabelle mit Host-Adressen 4-60

Kapitel 5 IPX-Routing 5-1

Unterstützen der Verbreitung von IPX Type 20-Paketen 5-2
Neues Maximum für Server- und Routeneinträge 5-3
Mehr standardmäßige IPX-SAP-Proxy-Server 5-4
Unterstützung für IPX ohne Festlegen eines IPX-Servers 5-4
Optimierter Zugang für anwählende NetWare-Clients 5-5
IPX-Filter 5-6
SPX-Spoofing für IPX hinzugefügt 5-8

Kapitel 6 Sicherheit 6-1

Unterstützung von Secure Access 6-2
Filterbeständigkeit 6-10
BACP-Unterstützung über MP hinzugefügt 6-12
Unterstützung von MS-CHAP 6-13
Unterstützung von „Called Number Authentication“ 6-15
Unterbrechungsursachencode für „CLID auth“ 6-17
„Expect Callback“ hinzugefügt 6-18
SNMP-Schreibsicherheit als Standard deaktiviert 6-19
SNMP-Anforderungsauthentifizierung hinzugefügt 6-21
Aufrufen von MPP-Sitzungsstatistiken mit „SNMP Get“ 6-25
SNMP hilft, einen Ruf einem Gerät zuzuordnen 6-27
SNMP-Erweiterungen 6-28

Feste Schnittstellen erscheinen in SNMP IfTable zuerst 6-29

Kapitel 7 Administration 7-1

Anzeigen unerwünschter Wählpakete 7-2
Rufblockierung bei gescheiterten Verbindungen 7-8
Befehl „Traceroute“ zum Terminal-Server hinzugefügt 7-9
Neue Option „-a“ im Befehl „tsave“ 7-12
Neue Option „-m“ im Befehl „tsave“ 7-13
Größere Ausführungsdateien 7-15
Neue SNMP Traps für gescheiterte Telnet-Kennwortüberprüfungen 7-20
Befehl zum Anzeigen der Systemversion hinzugefügt 7-21
Mehr Informationen im Protokoll „Fatal Error“ 7-22
Benutzerdefinierbarer Anschluß für Syslog-Meldungen 7-24
Terminal-Server und Diagnosefunktionen 7-25
Einstellen der Systemuhr mit SNMP 7-26
Beenden von PPP-Rufen bei Authentifizierungs-Timeout 7-26
Konfigurieren eines Anschlusses für Syslog-Meldungen 7-27
TFTP prüft Kompatibilität geladener Dateien 7-28

Anhang A Pipeline 75 Sprachfunktionen A-1

Statusanzeige für Sprachrufe A-2
WAN LED leuchtet bei Sprachrufen A-2
Unterstützt einen 2-Kanalruf auf einem SPID A-3
Konferenzschaltung A-4
CallerID unterstützt A-5
IDSL-Unterstützung für Sprachrufe von Pipeline 75 oder TA A-5
Unterstützung für ausgehende 3,1K-Audiorufe hinzugefügt A-9

Anhang B Pipeline 130 Fehlersuche und -beseitigung B-1

Timer-Unterbrechung von Reserveverbindung B-2
T1-Prüfschleife für die Pipeline 130 ..... B-2
Manuelle Prüfschleife für Pipeline 130 ..... B-4
Unterstützung der Inband-Prüfschleife für T1 ..... B-6
Manuelle T1-Prüfschleife mit dem Leitungs-Transceiver B-7
SNMP Traps für BRI linkUp und linkDown B-8

Konfiguration

1

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise auf die Art aus, wie Sie Ihr Gerät konfigurieren:

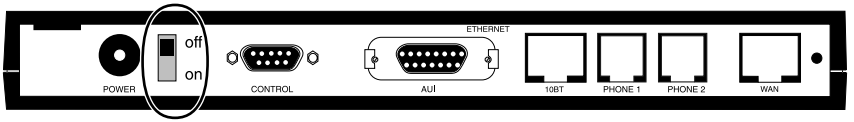
Lesen Sie dies zuerst 1-2
Pipelines können Sprachrufe annehmen oder ablehnen 1-3
Konfigurieren mit einem Tastentelefon 1-5
Automatische SPID-Erkennung (nur Nordamerika) 1-8
„Data Usage“ für weitere Vermittlungsstellentypen 1-9
Anzeigen des Load-Namens 1-10
Alternative Anschlußnummern für Pipeline 130 1-12
Unterstützung langer Benutzernamen 1-14
Längere ausgehende Telefonnummern 1-14

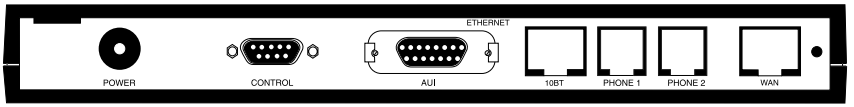
Lesen Sie dies zuerst

Die Auslieferung der neuen Einheiten Pipeline 50 oder 75 hat begonnen. Sie unterscheiden sich in der Rückansicht und können nur mit dem Softwarerelease 5.0B oder neuer betrieben werden. Die Version U ist bereits verfügbar, die Version S/T wird ab dem dritten Quartal des Jahres 1997 erhältlich sein.

Warning: Verwenden Sie keine ältere Softwareversion mit der neuen Pipeline 50 oder 75. Falls Sie eine ältere Softwareversion mit der Pipeline 50 oder 75 verwenden, funktioniert die Einheit nicht, und Sie müssen sie zum Austausch an Ascend zurücksenden. Sie können eine alte oder neue Einheit deaktivieren, wenn Sie eine ältere Softwareversion laden.

Die ältere Pipeline 75 weist einen Schalter auf

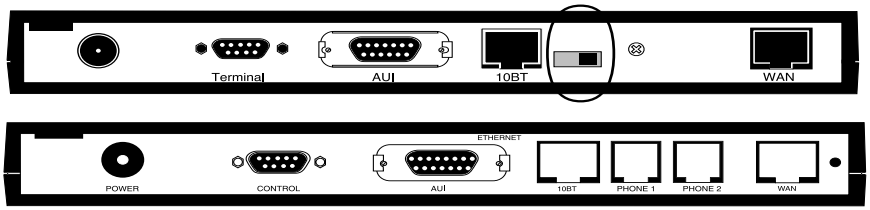




Die neuere Pipeline 75 weist keinen Schalter auf

Falls Sie alte und neue Pipeline 50 oder 75-Einheiten kombinieren, können Sie anhand dieser Abbildungen feststellen, welche Einheiten neu sind. Nur die alten Einheiten weisen auf der Rückseite einen Schalter auf.

Die ältere Pipeline 50 weist einen Schalter auf



Die neuere Pipeline 50 weist keinen Schalter auf

Die Pipeline 50 und 75 weisen jetzt identische Rückseiten auf.

Pipelines können Sprachrufe annehmen oder ablehnen

Dank des neuen Parameters „Ans Voice Call“ können Sie eine Pipeline so konfigurieren, daß sie Sprachrufe annimmt oder ablehnt.

Bisher lehnten die Pipeline 50 und 130 Sprachrufe ab, einschließlich von DOV-Rufen (Data Over Voice), bei denen der Anruf über ein Modem erfolgt, das an eine herkömmliche Telefonleitung angeschlossen ist; ein solcher Vorgang wurde auch nicht protokolliert. Die Pipeline 75 nahm Sprachrufe immer an und leitete sie an die POTS-Anschlüsse. Daher konnten Sie die Einheit nicht für Datenrufe dedizieren.

Mit dem Parameter „Ans Voice Call“ können Sie eine Pipeline 50 oder 130 so einrichten, daß sie Sprachrufe beantworten. Wenn Sie für den Parameter den Wert „No“ festlegen, können Sie darüber hinaus eine Liste der Nummern anzeigen, deren Anrufe abgelehnt wurden. Wenn Sie bei einer Pipeline 75 für den Parameter „Ans Voice Call“ den Wert „Yes“ festlegen, funktioniert die Einheit wie bisher. Falls Sie sich für den Parameter „No“ festlegen, beantwortet die Einheit den Ruf, leitet ihn aber nicht an einen POTS-Anschluß weiter.

Der Parameter „Ans Voice Call“ befindet sich im Menü „Configure“.

```
Configure...
   Switch Type=
   Chan Usage=
   My Num A=
   My Num B=
   SPID 1=
   SPID 2=
  >Ans Voice Call=Yes
```

Der Standardwert ist „Yes“, d. h. Sprachrufe werden angenommen. Wenn Sie „Ans Voice Call=No“ festlegen, können Sie die Telefonnummern abgelehnter Anrufe auflisten, indem Sie den Befehl „Show ISDN“ an der Eingabeaufforderung des Terminalservers eingeben. Beispiel:

```
ascend% show isdn

NL: CALL REJECTED/OTHER DEST: 5551010
```

Von der aufgelisteten Telefonnummer 5551010 ging ein Anruf ein, der nicht von der Pipeline beantwortet wurde.

Ans Voice Call

Beschreibung: Eingehende Sprachrufe werden bei einer ISDN Pipeline angenommen oder abgelehnt.

Verwendung: Geben Sie den Wert „Yes“ ein, um eingehende Sprachrufe anzunehmen; mit „No“ werden Sie abgelehnt.

Abhängigkeiten: Keine.

Parameter-Ort: Menü „Configure“.

Konfigurieren mit einem Tastentelefon

Gilt nur für die Pipeline 75. Dank dieser Funktion können Sie die ISDN-Telefonnummer einer Pipeline-Einheit über ein Tastentelefon eingeben. Mit dieser und zwei weiteren Funktionen (Automatische Vermittlungsstellenkennung und Remote Konfiguration durch eine Konfigurationszentrale) kann eine Pipeline, die installiert wird, auch schnell konfiguriert werden, ohne sie an einen Computer anzuschließen.

Überblick

Dieses Verfahren ist in erster Linie für Telefoninstallateure oder andere professionelle Installateure gedacht. Es ermöglicht, die Pipeline gleichzeitig zu installieren und zu konfigurieren. Es ist zwar nicht erforderlich, einen Computer an die Pipeline anzuschließen, um das Verfahren durchzuführen, aber es muß eine Konfigurationszentrale geben, die die Pipeline anrufen und die Konfiguration abschließen kann, nachdem die Pipeline eine Verbindung zur ISDN-Leitung hergestellt hat.

Hinweis: Wenn die Pipeline an eine japanische Vermittlungsstelle NTT INS-64 angeschlossen ist, arbeitet diese Funktion nicht.

Erforderliche Teile und Informationen

Um eine Pipeline mit einem Tastentelefon zu konfigurieren, benötigen Sie folgendes:

- Eine neue Pipeline 75 mit der Softwareversion 5.0B oder neuer.
  Das hier beschriebene Verfahren gilt für eine Pipeline mit werkseitig eingestellten Standardwerten. Wenn Sie das Verfahren mit einer bereits konfigurierten Pipeline verwenden wollen, müssen Sie die Softwareversion 5.0B oder neuer installieren, falls dies noch nicht erfolgt ist. Rufen Sie dann den Terminalserver auf, und geben Sie die Befehle `nvram` und `fclear` ein, um die werkseitig eingestellten Standardwerten wiederherzustellen.
- Ein Kabel, um die Pipeline mit der ISDN-Telefonleitung zu verbinden.
  Dieses Kabel (Teile-Nr. 2510-0122-001) wird mit der Pipeline geliefert.
- Ein Tastentelefon und ein modulares Telefonkabel, um es an die Pipeline anzuschließen.

- Die Telefonnummern der ISDN-Telefonleitung, die von der Pipeline verwendet werden.
- Die Telefonnummer der Konfigurationszentrale, die die Konfiguration abschließen wird.

Installieren der Pipeline

Gehen Sie bei der Installation folgendermaßen vor:

1 Schließen Sie die Pipeline mit dem mitgelieferten Kabel an die ISDN-Telefonleitung an.

2 Schließen Sie ein Tastentelefon an den Anschluß „Phone 1“ oder „Phone 2“ auf der Rückseite der Pipeline an.

Konfigurieren der Pipeline

Geben Sie die Telefonnummern für die ISDN-Telefonleitung folgendermaßen ein:

1 Nehmen Sie den Hörer des Tastfernsprechers ab.

Mit Ausnahme einiger älterer Geräte werden Sie bei allen Pipelines einen Fehlerton hören. Dieser Ton ist anders als ein Besetztzeichen.

2 Drücken Sie auf dem Telefon die Taste `*`.

Falls Sie nach Schritt 1 einen Fehlerton gehört haben, sollte er jetzt nicht mehr zu hören sein.

3 Drücken Sie auf dem Telefon die Taste `*` noch zweimal.

4 Drücken Sie auf dem Telefon die Taste `1`.

Damit kündigen Sie an, daß Sie die erste der Telefonnummern für die ISDN-Leitung eingeben werden.

5 Geben Sie die erste Telefonnummer für die ISDN-Leitung ein.

6 Drücken Sie auf dem Telefon die Taste `*`.

Hinweis: Falls Sie nach Schritt 2 einen Fehlerton hören, haben Sie die Telefonnummer nicht erfolgreich eingegeben. In diesem Fall müssen Sie den Hörer auflegen und erneut mit Schritt 1 beginnen.

Wenn Sie die erste Telefonnummer erfolgreich eingegeben haben, hören Sie jetzt ein Besetztzeichen. In diesem Fall können Sie die zweite Telefonnummer eingeben:

7 Drücken Sie auf dem Telefon die Taste *.

8 Drücken Sie auf dem Telefon die Taste * noch zweimal.

9 Drücken Sie auf dem Telefon die Taste 2.

Damit kündigen Sie an, daß Sie die zweite der Telefonnummern für die ISDN-Leitung eingeben werden.

10 Geben Sie die zweiteTelefonnummer für die ISDN-Leitung ein.

11 Drücken Sie auf dem Telefon die Taste *.

Wenn Sie die zweite Telefonnummer erfolgreich eingegeben haben, hören Sie jetzt ein Besetztzeichen.

Nachdem Sie die ISDN-Telefonnummern eingegeben haben, identifiziert die Pipeline den Typ der Vermittlungsstelle, an die sie angeschlossen ist:

1 Legen Sie den Hörer auf.

Die Pipeline identifiziert den Typ der Vermittlungsstelle und legt in der Einstellung „Switch Type“ den entsprechenden Wert fest. Falls der ISDN-Telefonserviceanbieter SPIDs (Service Profile Identifiers) verwendet, identifiziert die Pipeline auch diese automatisch und legt die entsprechenden Werte für die SPID-Einstellungen fest. Die automatische Kennung dauert in der Regel 1 bis 3 Minuten. (SPIDs nicht in Deutschland)

2 Warten Sie, bis die WAN-Statusleuchte aufhört zu blinken.

Wenn die Leuchte aufhört zu blinken, ist die automatische Kennung abgeschlossen. Sie können jetzt mit dem an der Pipeline angeschlossenen Telefon abgehende Telefonanrufe vornehmen. Die Pipeline kann nun auch eingehende Anrufe annehmen.

Schließen Sie die Pipeline-Konfiguration folgendermaßen ab:

1 Rufen Sie die Konfigurationszentrale an.

Sie können dazu das an der Pipeline angeschlossene Telefon verwenden.

2 Teilen Sie der Konfigurationszentrale die ISDN-Telefonnummern für die Pipeline mit.

3 Lassen Sie sie die Pipeline anrufen, um die verbleibenden Konfigurationseinstellungen vorzunehmen.

Automatische SPID-Erkennung (nur Nordamerika)

Gilt nur für die Pipeline-Einheiten 50 und 75, die in Nordamerika installiert werden. Diese Funktion fügt einen Parameter hinzu, mit dem Sie die Pipeline so konfigurieren können, daß beim Anschluß der Basisanschlußleitung eine automatische Auswahl der entsprechenden Vermittlungsstelle erfolgt. Falls es sich bei der Vermittlungsstelle nicht um AT&T P-to-P handelt, erkennt die Pipeline die SPIDs anhand der angegebenen Telefonnummern.

Konfigurieren von AutoSPID

Um die automatische Vermittlungsstellenauswahl auf der Pipeline zu konfigurieren, gehen Sie folgendermaßen vor:

1. Falls bereits eine Konfiguration vorhanden ist (nicht die Standardkonfiguration), empfiehlt es sich, diese Konfiguration speichern, bevor Sie fortfahren.
2. Öffnen Sie das Menü „BRI...“.

```
Configure
>Switch Type=AUTO SPID
 My Num A=
 My Num B=
 SPID A=N/A
 SPID B=N/A
 Data Usage=N/A
 Phone 1 Usage=N/A
 Phone 2 Usage=N/A
 Phone Num Binding=N/A
```

3. Wählen Sie „Switch Type=AUTO SPID“.
4. Geben Sie die vollständigen zehnstelligen Telefonnummern in „My Num A“ und „My Num B“ ein.

   Sie müssen beide Telefonnummern mit den Vorwahlnummern eingeben. Falls diese Nummern falsch sind, kann die Funktion nicht die korrekte SPID erhalten.

Dieser Vorgang kann mehrere Minuten beanspruchen. In diesem Zeitraum dürfen Sie weder die Konfiguration erneut eingeben noch die Verbindung zum Basisanschluß unterbrechen.

Sobald der Vermittlungsstellentyp erkannt wurde, wird die Verbindung vollständig initialisiert und im Fenster „VT-100 Line Status“ erscheint ein „D“. Falls ein „M“ erscheint, wurden die Telefonnummern u. U. falsch eingegeben, der Auto-SPID-Vorgang ist gescheitert oder der BRI-Anbieter hat die Leitung falsch bereitgestellt. Geben Sie in diesem Fall die Telefonnummern korrekt ein oder konfigurieren Sie „Switch Type“ sowie „SPID1“ und „SPID2“ manuell.

Hinweis: Falls es sich bei Ihrem Service um AT&T Point-To-Point handelt, gibt es bei Ihrem Service keine SPIDs.

5 Speichern Sie die Konfiguration, wenn Sie dazu aufgefordert werden (nachdem der Vermittlungsstellentyp korrekt erkannt wurde). Dadurch verlassen Sie das Menü „BRI“.

„Data Usage“ für weitere Vermittlungsstellentypen

Gilt nur für die Pipeline 75. Der Parameter „Data Usage“ kann jetzt festgelegt werden, wenn es sich beim Wert des Parameters „Switch Type“ um „France“, „U.K.“, „NET 3“, „Japan“, „Belgium“, „Australia“, „Swiss“, „German“ oder „MP German“ handelt.

Parameterangaben

Data Usage

Beschreibung: Gibt an, welche der ISDN-Telefonnummern für eingehende Datenrufe verwendet werden sollen. Falls Ihr ISDN-Service Datenrufe nur auf einer Telefonnummer gestattet, können Sie mit diesem Parameter die zu verwendende Telefonnummer angeben.

Verwendung: Betätigen Sie die Eingabetaste, um die Optionen durchzugehen.

- „A“ gestattet eingehende Datenanrufe zur Telefonnummer, die im Parameter „My Num A“ festgelegt wurde.
- „B“ gestattet eingehende Datenanrufe zur Telefonnummer, die im Parameter „My Num B“ festgelegt wurde.
- „A + B“ “ gestattet eingehende Datenanrufe zu Telefonnummern, die in den Parametern „My Num A“ oder „My Num B“festgelegt wurden.

Abhängigkeiten: Falls der Wert des Parameters „Switch Type“ „AT&T/P-T-P“ lautet, erscheint beim Parameter „Data Usage“ der Wert „N/A“. Es gibt nur eine Nummer für diesen ISDN-Servicetyp, die für alle Datenrufe verwendet wird.

Parameter-Ort: Configure-Profil, BRI

Siehe auch: My Num A, My Num B, Switch Type

Anzeigen des Load-Namens

Ein Softwarerelease von Ascend wird als *Load* vertrieben. Dabei handelt es sich um binäre Dateien, die Sie auf ein lokales Gerät kopieren und auf die Pipeline laden. Die Loads unterscheiden sich je nach Funktion und Zielplattform. Der Name einer Load wird im Statusfenster „Sys Options“ und in Meldungen unkorrigierbarer Abbruchfehler angezeigt. Der Load-Name ist ein wichtiges Hilfsmittel bei der Behebung von Fehlerbedingungen.

Der Name einer Load-Datei hat das Format *Funktion.Modell*. Das Präfix gibt die Netzwerkschnittstelle an und wie die Einheit funktionieren soll. Folgende Abkürzungen werden dabei verwendet:

t	T1
e	E1
b	ISDN BRI
52	Switched-56 2-Draht
54	Switched-56 4-Draht

i	nur IP
p	nur IPX
x	X.25
1	alte Hardware (z. B. b1.p50)
2	neue Hardware (z. B. b2.p75)

Beispiel:

b.p50 steht für die Pipeline 50 BRI

52.p50 steht für die Pipeline 50 Switched-56 4-Draht

Die Pipeline-Modelle 50, 75 und 130 werden als p50, p75 bzw. p13 abgekürzt.

Hinweis: Wenn Sie die neueste Softwareversion vom Ascend FTP-Site (ftp.ascend.com/pub/Software-Releases) laden, müssen Sie zunächst über die README-Datei des jeweiligen Unterverzeichnisses feststellen, welche Datei Sie laden müssen.

Auf Ihrer Pipeline erscheint die aktuelle Load im Statusfenster „Sys Options“. Beispiel:

```
00-100 Sys Option
>Access Router          ^
 Load: b.p75
 Switched Installed     v
```

Siehe auch „TFTP prüft Kompatibilität geladener Dateien“ auf Seite 7-28.

Alternative Anschlußnummern für Pipeline 130

Sie können jetzt bis zu drei alternative Wählnummern in einem Anschlußprofil einer Pipeline 130 hinzufügen. Diese alternativen Nummern werden erprobt, bevor ein designiertes Sekundärprofil aufgerufen wird.

Verwenden der alternativen Nummern

Bisher enthielt ein Anschlußprofil nur eine Nummer, über die eine Bridge, ein Router oder eine Node am anderen Ende der Verbindung angewählt werden konnte. Falls mit dieser Nummer keine Verbindung hergestellt werden konnte, wurde ein weiterer Versuch mit Informationen in einem Sekundärprofil (mit „Session Options“ festgelegt) durchgeführt. Falls jetzt mit der Wählnummer keine Verbindung hergestellt werden kann, werden zunächst die alternativen Wählnummern verwendet, bevor das Sekundärprofil benutzt wird.

Konfigurieren alternativer Wählnummern

Sie können einem Anschlußprofil drei alternative Nummern zuweisen. Sie werden der Reihe nach verwendet oder bis ein Feld für eine alternative Nummer leer ist (d. h. falls Sie im ersten und dritten Feld eine Nummer eingegeben, das zweite Feld aber leer gelassen haben, wird die Nummer im dritten Feld nie verwendet). Falls mit keiner der alternativen Nummern eine Verbindung mit der Gegenstelle hergestellt werden kann, wird das designierte Sekundärprofil verwendet, falls eines in „Session Options“ festgelegt wurde.

Die Parameter der alternativen Wählnummern (Alt Dial) erscheinen wie folgt:

```
Ethernet > Connections > profile
    Station=name
    Active=Yes
    Encaps=MPP
    Dial#=5551111
    Alt Dial#1=5551112
    Alt Dial#2=5551113
    Alt Dial#3=5551114
    Calling#=
```

```
Route IP=Yes
Bridge=No
Dial Brdcast=N/A
Encaps Options...
IP Options...
IPX Options...
Session Options...
Telco Options...
```

Falls Sie zwei alternative Nummern hinzufügen, müssen Sie darauf achten, „Alt Dial#1“ und „Alt Dial#2“ zu verwenden. Ein leeres Feld gibt an, daß das Ende der Informationen zu alternativen Wählnummern erreicht ist.

Alt Dial#n

Beschreibung: Sie können in einem Anschlußprofil einer Pipeline 130 bis zu drei alternative Wählnummer eingeben. Belegen Sie die Felder für alternative Wählnummern der Reihe nach. Ein leeres Feld gibt an, daß das Ende der alternativen Wählnummern erreicht ist. (Falls „Alt Dial#2“ leer ist, wird „Alt Dial#3“ nicht verwendet, selbst wenn es eine Nummer enthält.)

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen und um eine Telefonnummer einzugeben. Betätigen Sie die Eingabetaste, um das Textfeld zu schließen. In einem Feld können Sie bis zu 37 Zeichen eingeben; folgende Zeichen sind gültig:

```
1234567890()[]!z-*#|
```

Nur die numerischen Zeichen werden gesendet.

Als Standardwert ist das Feld leer.

Beispiel: Alt Dial#1=5551112

Abhängigkeiten: Eine alternative Nummer wird nur verwendet, falls mit der Nummer in „Dial#“ keine Verbindung hergestellt werden kann, und falls ein vorhergehendes Feld für eine alternative Nummer nicht leer ist.

Parameter-Ort: Ethernet > Connections > Profile.

Unterstützung langer Benutzernamen

Der Parameter „My Name=“ kann jetzt lange Namen mit bis zu 72 Zeichen aufnehmen.

Längere ausgehende Telefonnummern

```
Die maximale Länge von Telefonnummern wurde auf 24 Stellen gest
```

Die folgenden Telefonnummernfelder weisen jetzt eine Länge von 24 Stellen auf:

„Configure“-Profil > My Num A

„Configure“-Profil > My Num B

Ethernet > Connections > *Profile* > Dial #

Ethernet > Connections > *Profile* > Telco Options > Bill #

WAN-Konfiguration

2

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise auf die Art aus, wie Sie Ihre Einheit konfigurieren:

Parameter „Max Channel Count“ geändert 2-2
Schnittstellenunterstützung für MP-Rufverwaltung 2-2
BACP-Unterstützung über MP hinzugefügt 2-3
Pipeline MPP zieht neuesten Kanal zuerst ab 2-3
Inverse ARP für Frame Relay 2-4
Pipeline 50 und 130 als lokaler ATMP-Agent 2-4
Serieller WAN-V.35-Anschluß für Pipeline 130 2-7
FDL für T1-Leitungen hinzugefügt 2-12
Interner Taktgebermodus für Pipeline 130 T1 2-14
Flexibler Start für DS0-Ursprung in „Nailed T1“ 2-15

Parameter „Max Channel Count“ geändert

Sie können nur die im Parameter „Max Ch Count” festgelegten, unterstützten Werte als Höchstzahl der Kanäle, die für einen MP+-Ruf verwendet werden sollen, angeben. Beispiel: Für den Parameter „Max Ch Cnt“ können Sie auf der Pipeline 50 den Höchstwert 2 festlegen.

Bisher konnte ein Wert von 0 bis 32 eingegeben werden, gleichgültig, ob die Einheit 32 Kanäle unterstützte oder nicht.

Sie finden den Parameter „Max Ch Count“ in Ethernet > Answer > *Profile* > PPP options, und Ethernet > Connections > *Profile* > Encaps options.

Schnittstellenunterstützung für MP-Rufverwaltung

PPP-Verbindungen verwenden für Einkanalrufe das PPP-Einkapselungsverfahren. Sowohl MP- als auch MP+ sind Erweiterungen von PPP, um Mehrkanalrufe zu unterstützen. In bisherigen Versionen forderte die Pipeline zuerst MP+ an, falls eine Verbindung für „MPP“ eingerichtet worden war. Konnte die Verbindung nicht mit MP+ aufgebaut werden, verwendete die Pipeline statt dessen das Protokoll MP. Falls dieses Protokoll ebenfalls abgelehnt wurde, wurde PPP verwendet.

Sie können ausdrücklich die Option „RFC 1717 MP“ konfigurieren. MP unterstützt Mehrkanalrufe, jedoch nicht die Dynamic Bandwidth Allocation (DBA). Der „Base-Channel Count“ wird verwendet, um die Anzahl der durchzuführenden Rufe festzulegen, und die Anzahl der Kanäle, die für diese Verbindung verwendet werden, bleibt unverändert. Außerdem müssen für eine MP-Verbindung alle Kanäle in der Verbindung dieselbe Telefonnummer nutzen (d. h., daß sich die Kanäle auf der antwortenden Seite der Verbindung in einer Mehrfach-Weiterschaltungsgruppe befinden müssen).

Es folgen die neuen Parameter, die Sie zur Konfigurierung von MP-Verbindungen verwenden können:

```
Ethernet > Connection > Profil > Encaps=MP
Ethernet > Answer > Encaps > Profil > MP=Yes
```

BACP-Unterstützung über MP hinzugefügt

Beim Bandwidth Allocation Control Protocol (BACP) handelt es sich um den Internet-Standard, der Ascend Multilink Protocol Plus (MP+) entspricht.

Funktionsweise des BACP

BACP läuft über MP und gestattet es einem Gerät, das MP unterstützt (unabhängig von dessen Hersteller), je nach Bedarf eine Bandbreite hinzuzufügen oder zu entfernen. BACP funktioniert ähnlich wie MP+ und verwendet die gleichen Menüelemente wie MP+.

Da BACP nicht „Idle Percent“ unterstützt, wurde das Feld aus dem Menü Ethernet > Connection profile > Encaps entfernt.

Konfigurieren von BACP

Wenn Sie eine Pipeline konfigurieren wollen, um mit BACP zu senden und zu empfangen, müssen Sie den Parameter „BACP“ im Verbindungs- oder Antwortprofil folgendermaßen festlegen:

- Für die Sendung legen Sie den Wert Ethernet > Connection profile > Encaps > BACP=Yes
  fest (der Standardwert ist „No“).

  Hinweis: Das Feld „Idle Percent“ wurde aus diesem Menü entfernt, da es bei MP immer den Wert „N/A“ hat und nicht von BACP unterstützt wird.
- Für den Empfang legen Sie den Wert Ethernet > Answer > PPP BACP=Yes fest (der Standardwert ist „No“).

Dieser Parameter ist nur verfügbar, falls „Encaps=MP“ festgelegt wurde.

Pipeline MPP zieht neuesten Kanal zuerst ab

Die Reihenfolge, in der MPP Kanäle bei der Verringerung der Bandbreite abzieht, wurde geändert. MPP zieht zuerst den zuletzt hinzugefügten Kanal ab.

Inverse ARP für Frame Relay

Mit dem Inverse Address Resolution Protocol (InARP) kann ein Gerät die Protokolladresse eines anderen Geräts auflösen, wenn die Hardware-Adresse bekannt ist. Im Falle von Frame Relay lautet die Hardware-Adresse „DLCI“. Die Ascend-Implementierung von Inverse ARP reagiert nur auf Anforderungen von Frame Relay und IP Inverse ARP.

Inverse ARP-Anforderungen *müssen* vom folgenden Typ sein:

- der ARP-Protokolltyp von IP (0x8000)
- der ARP-Hardwareadreßtyp ist die 2-Byte Q.922-Adresse

Alle anderen Typen werden ignoriert.

Die Inverse ARP-Antwort liefert folgende Daten:

- die ARP-Quellprotokolladresse ist die IP-Adresse der Pipeline. Sie finden sie im Parameter „Mod Config, Ether Options, IP Adrs“.
- die ARP-Quellhardwareadresse ist die Q.922-Adresse des lokalen DLCI.

Hinweis: Die Pipeline gibt keine Inverse ARP-Anforderungen aus.

Näheres zu Inverse ARP finden Sie unter RFCs 1293 und 1490.

Pipeline 50 und 130 als lokaler ATMP-Agent

Virtuelle private Netzwerke können eine Pipeline 50 oder 130 jetzt als Endpunkt eines lokalen ATMP-Agenten enthalten. In einer solchen Implementierung arbeitet die Pipeline nur im Router-Modus.

Verwendung einer Pipeline in einem virtuellen privaten Netzwerk

Virtuelle private Netzwerke bieten kostengünstigen, remoten Zugriff auf private LANs über das Internet. Der Tunnel zum privaten Unternehmensnetzwerk kann von einem ISP ausgehen, wodurch mobile Nodes ein Unternehmensnetzwerk anwählen können. Der Tunnel kann sich aber auch zwischen zwei Unternehmensnetzwerken befinden, die aufeinander über eine kostengünstige Internet-Verbindung zugreifen.

Mit einer UDP/IP-Sitzung baut das Ascend Tunnel Management Protocol (ATMP) zwischen zwei Einheiten einen Tunnel für verkapselte Pakete auf. Die Verkapselung der Pakete erfolgt mit der standardmäßigen Generic Routing Encapsulation (GRE), wie in RFC 1701 beschrieben. Im wesentlichen bietet der Tunnel direkten Zugriff auf ein lokales Netzwerk. Die Pakete müssen geroutet sein (IPX oder IP).

Entfernte und lokale Agenten

ATMP-Tunnel funktionieren zwischen zwei Ascend-Einheiten. Eine der Einheiten tritt als entfernter Agent (in der Regel ein lokaler ISP) auf und die andere als lokaler Agent (der Zugriff auf das lokale Netzwerk hat). Eine mobile Node stellt eine Einwählverbindung mit dem entfernten Agenten her und damit eine IP-Sitzung über Internet mit dem lokalen Agenten. Der entfernte Agent fordert dann einen ATMP-Tunnel auf der IP-Sitzung an. Der entfernte Agent muß RADIUS verwenden, um Einwählverbindungen mobiler Nodes zu authentifizieren.

Der lokale Agent bildet den Abschluß des Tunnels, an dem sich der Großteil der ATMP-Informationen befindet. Dieser Agent muß in der Lage sein, mit dem lokalen Netzwerk (dem Zielnetzwerk für mobile Nodes) kommunizieren zu können, und zwar entweder über eine direkte Verbindung, einen anderen Router oder über eine feste Verbindung.

Der lokale Agent kann mit dem lokalen Netzwerk über eine direkte Verbindung, einen anderen Router oder über eine feste Verbindung kommunizieren. Er arbeitet im Router-Modus, wenn das lokale Netzwerk über Paket-Routing erreicht wird. Er arbeitet im Gateway-Modus, wenn zum lokalen Netzwerk eine feste Verbindung besteht.

Bei einem lokalen Agenten kann es sich um eine Ascend MAX-Einheit oder eine Pipeline 50 oder 130 handeln. Wenn eine Pipeline als Endpunkt eines lokalen Agenten verwendet wird, wird nur das Routing unterstützt.

Konfigurieren eines lokalen Agenten im Router-Modus

Nachdem der ATMP-Tunnel zwischen dem lokalen und dem entfernten Agenten eingerichtet wurde, empfängt der lokale Agent IP-Pakete über diesen Tunnel, entfernt die GRE-Verkapselung und leitet die Pakete an seine Bridge/Router-Software weiter. Außerdem fügt er der Routing-Tabelle eine Host-Route zur mobilen Node hinzu.

Unten sehen Sie die Parameter, mit denen Sie einen lokalen Agenten im Router-Modus konfigurieren können. Die Parameter für das IPX-Routing im Ethernet-Profil sind nur erforderlich, falls die Pipeline ein IPX-Routing vornimmt.

```
Ethernet
  Mod Config
   IPX Routing=Yes
   Ether options…
    IP Adrs=10.1.2.3/24
      IPX Frame=802.2
      IPX Enet #=00000000
    ATMP options...
      Password=private
      UDP Port=5150
```

Mit `Password` wird der ATMP-Tunnel authentifiziert. Es muß mit dem Kennwort übereinstimmen, das mit dem Attribut „Ascend-Home-Agent-Password“ im RADIUS-Profil der mobilen Node festgelegt wurde. (Alle mobilen Nodes verwenden dasselbe Kennwort für dieses Attribut.)

ATMP verwendet den UDP-Anschluß 5150 für ATMP-Meldungen zwischen den entfernten und lokalen Agenten. Falls Sie eine andere UDP-Anschlußnummer angeben, müssen Sie sicherstellen, daß es keine Konflikte mit der restlichen ATMP-Konfiguration gibt.

Unten sehen Sie die Parameter für einen IP-Routing-Anschluß mit dem entfernten Agenten, der wie üblich authentifiziert und hergestellt wird:

```
Ethernet
  Connections
    Station=foreign-agent
    Active=Yes
    Encaps=MPP
    Dial #=555-1213
    Route IP=Yes
    Encaps options...
      Send Auth=CHAP
      Recv PW=foreign-pw
      Send PW=home-pw
    IP options...
      LAN Adrs=10.65.212.226/24
```

Serieller WAN-V.35-Anschluß für Pipeline 130

Das Pipeline-Modell P130-1UBRI-V35 bietet zusätzlich zu einem ISDN BRI- oder Switched 56-Anschluß einen seriellen WAN-V.35-Anschluß. In den folgenden Abschnitten wird beschrieben, wie der Anschluß konfiguriert und überwacht wird.

Konfigurieren des seriellen WAN-V.35-Anschlusses

Die serielle WAN-Übertragungsgeschwindigkeit wird durch die über die Verbindung empfangene Taktgeberrate bestimmt. Die maximal annehmbare Taktgeberrate ist 1,56 Mbit/s. Die Taktgeberrate des seriellen WAN-Anschlusses wirkt sich nicht auf die Bandbreite anderer WAN-Schnittstellen in der Pipeline aus.

Nachdem der serielle WAN-V.35-Anschluß aktiviert wurde, werden die Verbindungsprofile alle 10 Sekunden überprüft. Falls ein Verbindungsprofil oder ein Frame-Relay-Profil für den Betrieb mit einer Mietleitung konfiguriert wurde und für den Parameter „Group“ im Anschluß- oder Frame-Relay-Profil der gleiche Wert festgelegt wurde wie für den Parameter „Group“ im V.35-Mod-Config-Profil, ist der V.35-Anschluß auf synchronen HDLC-Modus eingerichtet, und es wird versucht, die Verbindung an diesem Anschluß herzustellen.

Bevor Sie das Serial-WAN-Profil konfigurieren, müssen Sie entscheiden, welche Frame-Relay-Verbindung oder andere Verbindung den seriellen WAN-V.35-Anschluß verwenden soll. Legen Sie dann für den Parameter „Group“ den gleichen Wert wie für den Parameter „Group“ im V.35-Mod-Config-Profil fest:

- Für Verbindungsprofile müssen Sie den Parameter „Group“ im Untermenü „Connections/Telco options“ festlegen.
- Für ein Frame-Relay-Profil müssen Sie den Parameter „Nailed Grp“ festlegen.

Konfigurieren des seriellen WAN-V.35-Anschlusses:

1 Öffnen Sie das Serial-WAN-Profil.

```
30-000 Serial WAN
 Mod Config...
```

2 Öffnen Sie das Mod-Config-Profil.

```
20-B00 Mod Config...
  Module Enabled-Yes
  Group=3
  Activation=Static
```

3 Legen Sie für „Module Enabled“ den Wert „Yes“ fest.

4 Wählen Sie für „Group“ eine Nummer, die dem Parameter „Group“ in einem Verbindungsprofil oder dem Parameter „Nailed Grp“ in einem Frame-Relay-Profil entspricht.

5 Legen Sie den passenden Wert für „Activation“ fest.

Damit werden die Signale am seriellen WAN-Anschluß festgelegt, mit denen angegeben wird, daß das DCE (Data Circuit-Terminating Equipment) anschlußbereit ist.

6 Schließen Sie das Serial-WAN-Profil, und speichern Sie die Änderungen.

Parameterangaben

In diesem Abschnitt werden die neuen Parameter beschrieben, die der Pipeline zur Unterstützung des seriellen WAN-V.35-Anschlusses hinzugefügt wurden.

Module Enabled

Beschreibung: Aktiviert den seriellen WAN-V.35-Anschluß der Pipeline.

Verwendung: Betätigen Sie die Eingabetaste, um die Optionen durchzugehen:

- „Yes“ aktiviert den seriellen WAN-Anschluß.
  „Yes“ ist der Standardwert.
- „No“ deaktiviert den seriellen WAN-Anschluß.

Parameter-Ort: V.35 > Serial WAN > Mod Config

Activation

Beschreibung: Dieser Parameter legt die Signale am seriellen WAN-Anschluß fest, mit denen angegeben wird, daß das DCE (Data Circuit-Terminating Equipment) anschlußbereit ist.

Die Flußsteuerung erfolgt immer mit dem Signal „CTS“ (Clear To Send).

Verwendung: Betätigen Sie die Eingabetaste, um die Optionen durchzugehen:

- „Static“ gibt an, daß die Pipeline keine Flußsteuerungssignale verwendet, weil das DCE immer angeschlossen ist.
- „DPR“ (Call Digit or Tone) gibt an, daß das DCE das DPR-Signal auslöst, wenn es bereit ist.
- „CRQ“ (Call Request) gibt an, daß das DCE das CRQ-Signal auslöst, wenn es bereit ist.
- „RTS“ (Request to Send) gibt an, daß das DCE das RTS-Signal auslöst, wenn es bereit ist.
- „CRQ+RTS“ gibt an, daß das DCE das CRQ- und RTS-Signal auslöst, wenn es bereit ist.
- „DPR+CRQ+RTS“ gibt an, daß das DCE das DPR-, CRQ-und RTS-Signal auslöst, wenn es bereit ist.
- „Disabled“ gibt an, daß der serielle WAN-V.35-Anschluß deaktiviert ist. Mit dieser Einstellung wird eine aktive Sitzung beendet und weitere Versuche, eine Verbindung herzustellen, werden verhindert.
- Serial-WAN-Profil: Serial WAN/Mod Config

Parameter-Ort: V.35 > Serial WAN > Mod Config

Group

Beschreibung: Weist den festen Kanälen des seriellen WANs eine Gruppennummer zu. Wenn der Parameter „Group“ in einem Verbindungsprofil oder der Parameter „Nailed Grp“ in einem Frame-Relay-Profil den gleichen Wert

aufweist wie der Parameter „Group“ im Serial-WAN-Profil, verwendet das Anschluß- oder Frame-Relay-Profil den seriellen WAN-Anschluß.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie eine Zahl zwischen 1 und 60 ein. Der Standardwert ist 3.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen.

Abhängigkeiten: Denken Sie an diese zusätzlichen Informationen:

- Falls Sie dem Parameter „Group“ Kanäle hinzufügen und diese Änderungen speichern, fügt die Pipeline diese zusätzlichen Kanäle jeder Online-Verbindung hinzu, die diese Gruppe verwendet.
- Weisen Sie einer Gruppe nicht mehr als ein aktives Verbindungsprofil zu.
- Weisen Sie einer Gruppe, die ein Frame-Relay-Profil verwendet, kein Verbindungsprofil zu.

Parameter-Ort: V.35 > Serial WAN > Mod Config

Siehe auch: Group, Nailed Grp

Neues Leitungsstatusfeld

Das Leitungsstatusfenster „10-100“ enthält jetzt ein Feld neben dem Feld „Link“, in dem die Anwesenheit und der Status des V.35-Anschlusses angezeigt werden. Die Pipeline überwacht die CTS- und DTR-Signale, um die Verbindungsintegrität zu bestimmen.

Falls der V.35-Anschluß vorhanden aber nicht aktiv ist, erscheint ein Leitungsstatusfenster, das dem folgenden ähnelt:

```
10-100 1
Link   D   V.35
B1     *.....
B2     *.....
```

Falls der V.35-Anschluß vorhanden und aktiv ist, erscheint ein Leitungsstatusfenster, das dem folgenden ähnelt:

```
10-100 1
Link   D   V.35
B1     *....*
B2     *.....
```

Physische Spezifikationen der Pipeline 130 V.35

Die Pipeline wiegt 563 g und hat die Abmessungen 3,28 cm x 22,1 cm x 15,9 cm. Sie weist folgende physische Schnittstellen auf:

Anschlüsse	Funktion oder Betrieb
Netzanschluß	Für 18 VDC Stromzufuhr.
Terminal-(Steuerungs-)Anschluß, Typ DE-9.	Für Systemverwaltung und Einrichtung. 9600 Bit/s (Standard), 8 Bits/Zeichen, keine Prüfbits, keine Flußsteuerung und 1 Stopbit.
Ein BRI-Anschluß, Typ RJ-45, gekennzeichnet WAN 1.	Anschluß rechts außen: für BRI-Zugriff auf WAN. Werksoptionen: U-Schnittstelle oder S-Schnittstelle.
Ein V.35-Anschluß, Typ DB-44, gekennzeichnet WAN 2.	Anschluß neben rechts außen: für V.35-Zugriff auf WAN. Hinweise zu Beschränkungen der Kanalverwendung finden Sie in der Benutzerdokumentation zur Pipeline.
Zwei Ethernet-Anschlüsse, Typ DA-15 (gekennzeichnet AUI) und Typ RJ-45 (gekennzeichnet UTP (10 BaseT)).	Eine Ethernet-Schnittstelle, die beim Anschluß automatisch von der Software gewählt wird.

In der folgenden Tabelle werden die Pins der V.35-Schnittstelle einer Pipeline dargestellt:

V.35-Signal	Kupplung DB-44
FGND RI	1 8
SD+ SD-	39 40
RD+ RD-	30 29

V.35-Signal	Kupplung DB-44
ST+ ST-	41 42
RT+ RT-	32 31
TT+ TT-	38 37
DTR DSR	6 11
DCD SGND	9 25
CTS RTS	7 36

FDL für T1-Leitungen hinzugefügt

Diese Funktion verleiht der Pipeline 130 T1 vollständige CSU-Fähigkeit (Channel Service Unit).

Funktionsweise von FDL

Bei einer FDL (Facilities Data Link) handelt es sich um einen 4 Kbit/s Systemdatenkanal, der verfügbar ist, wenn Sie das Format T1 ESF (Extended Super Frame) verwenden. FDL leitet in regelmäßigen Abständen Informationen an die Wartungsgeräte des Trägers. Dadurch kann der Telefonserviceanbieter über das FDL-Protokoll die Qualität und Leistung von T1-Leitungen überwachen. Wenn Sie FDL aktivieren, verfügt die Pipeline 130 T1 über vollständige CSU-Funktionalität.

Diese Funktion fügt dem Profil „Nailed T1 > Mod Config“ den Parameter „FDL“ hinzu. Der Parameter „FDL“ gibt an, welchen FDL-Protokolltyp die Pipeline verwendet. Der Träger kann Ihnen mitteilen, welches FDL-Protokoll Sie angeben müssen.

Denken Sie an diese zusätzlichen Informationen:

- Der Parameter „FDL“ gilt nicht für D4-framed T1-Leitungen.
- Es werden auch dann Daten zu den D4- und ESF-Leistungen im Fenster „FDL Stats“ gesammelt, wenn Sie nicht das FDL-Protokoll wählen.
  - D4 steht für das D4-Format, auch Superframe-Format genannt, mit dem Daten auf physischer Ebene in Datenübertragungsblocks unterteilt werden.

    Dieses Format besteht aus 12 aufeinanderfolgenden Rahmen, die durch Rahmenbits getrennt werden.
  - ESF steht für das Extended-Superframe-Format, mit dem Daten auf physischer Ebene in Datenübertragungsblocks unterteilt werden.

    Dieses Format besteht aus 24 aufeinanderfolgenden Rahmen, die durch Rahmenbits getrennt werden.

Konfigurieren von FDL

Dem Menü „Nailed T1 > Mod Config“ wurde das Feld „FDL“ hinzugefügt.

FDL wird folgendermaßen aktiviert:

1 Öffnen Sie das Nailed-T1-Profil.

2 Öffnen Sie das Mod-Config-Menü.

```
90-B00 Mod Config
Nailed T1 Group=3
Activation=Enabled
Framing Mode=ESP
Encoding=B8ZS
>FDL=None
First DSO=1
Last DSO=6
Loop Back=Normal
```

3 Wählen Sie den entsprechenden FDL-Modus. Betätigen Sie die Eingabetaste, um die Optionen durchzugehen. Ihr Träger kann Ihnen mitteilen, welcher Modus Ihnen zur Verfügung steht.

Die Optionen für das Feld „FDL“ lauten:

Option	Beschreibung
ANSI	ANSI FDL implementiert
ATT	ATT FDL implementiert
Sprint	Sprint FDL implementiert
None	FDL nicht implementiert Dies ist der Standardwert.

Interner Taktgebermodus für Pipeline 130 T1

Sie können jetzt angeben, ob die Pipeline die T1-Übertragungstaktgeberrate lokal generieren oder über die Empfangstaktgeberrate eine Synchronisierung mit dem Netzwerk durchführen sollte. Bisher erzeugte die Pipeline keine T1-Übertragungstaktgeberrate mit ihrem internen Oszillator.

Funktionsweise von „Clock Source“

Der Parameter „Clock Source“ befindet sich im Untermenü „Nailed T1 > Mod Config“. Der Standardwert ist „No“. Dabei handelt es sich um die Einstellung, die normalerweise verwendet wird, wenn die Pipeline an eine vom Telefonserviceanbieter bereitgestellte T1-Schnittstelle angeschlossen wird.

Wenn Sie zwei Pipeline 130-Geräte zusammen an eine private Twin-Shielded Twisted-Pair-Verbindung anschließen, müssen Sie für den Parameter „Clock Source“ der einen Pipeline den Wert „Yes“ und für den Parameter „Clock Source“ der anderen Pipeline den Wert „No“ festlegen.

Konfigurieren der T1-Übertragungstaktgeberrate

Wenn Sie die Pipeline so konfigurieren wollen, daß die T1-Übertragungstaktgeberrate vom internen Oszillator der Einheit generiert wird, müssen Sie „Clock Source=Yes“ festlegen.

```
30-100 Mod Config
   Nailed T1 Group=3
   Activation=Enabled
   Framing Mode=ESF
   Encoding=B8ZS
   First DSO=1
   Last DSO=24
  >Clock Source=No
   Loop Back=Normal
```

Flexibler Start für DS0-Ursprung in „Nailed T1“

Gilt nur für Pipeline 130. Bisher war es bei der Nailed-T1-Konfiguration erforderlich, daß die Daten mit dem ersten DS0 der T1-Leitung begannen. Wurde eine Pipeline 130 mit Nailed-T1 zu einer vorhandenen T1-Leitung hinzugefügt, konnte es zu einem Konflikt kommen, wenn die erste Position bereits belegt war. Sie können jetzt einen anderen Kanal als den ersten T1-Kanal als Ursprung für das erste DS0 wählen.

Einstellen des DS0-Ursprungs

Konfigurieren von DS0-Kanälen für „Nailed-T1“

Sie können den ersten und letzten DS0-Kanal im Untermenü „Nailed T1 > Mod Config“ angeben. Wieviele Kanäle Sie angeben können, hängt davon ab, welchen Kodierungsmodus Sie der Leitung zugewiesen haben. Falls es sich beim Kodierungsmodus um AMI handelt, können Sie maximal sechs DS0-Kanäle festlegen. Der Wert des Parameters „Last DS0“ muß gleich dem (bei einem Kanal) oder größer als der des Parameters „First DS0“ sein.

Konfigurieren der DS0-Kanäle für „Nailed-T1“ auf der Pipeline 130:

1 Öffnen Sie das Nailed-T1-Profil.

Betätigen Sie, falls erforderlich, die Escape-Taste, bis das Hauptbearbeitungsmenü angezeigt wird, wählen Sie dann „Nailed T1“, und betätigen Sie die Eingabetaste.

2 Wählen Sie „Mod Config“.

Das Untermenü „Nailed T1 > Mod Config“ erscheint. Es folgen Beispielwerte, die Sie in diesem Menü eingeben können.

```
Mod Config
 Nailed Grp=1
 Activation=Enabled
 Framing Mode=ESF
 Encoding=B8ZS
>First DS0=1
 Last DS0=6
 Loop Back=Normal
```

3 Wählen Sie „First DS0“.

Legen Sie den Startkanal fest.

4 Wählen Sie „Last DS0“.

Legen Sie einen Endkanal fest. Mit diesem Wert legen Sie die Höchstzahl an DS0-Kanälen fest, und er muß gleich dem oder größer als der des Parameters „First DS0“ sein. Beispiel: Wenn Sie „First DS0=2“ und „Last DS0=7“ festlegen, haben Sie damit einen Bereich mit sechs Kanälen angegeben, wobei 2 der erste Kanal ist. Falls Sie „First DS0=2“ und „Last DS0=2“ festlegen, haben Sie angegeben, daß nur ein DS0-Kanal (Kanal 2) benutzt wird.

Falls der Wert für „First DS0“ größer ist als der Wert für „Last DS0“, erscheint die folgenden Meldung:

```
Message #224: First DS0 value must be less than or equal to
Last DS0.
```

Hinweis: Falls Sie den Modus „AMI“ (Alternative Mark Inversion) wählen, dürfen Sie nicht mehr als sechs DS0-Kanäle festlegen. Der Modus „B8ZS“ gestattet maximal 24 Kanäle.

Falls Sie versuchen, das Nailed-T1-Profil mit mehr als sechs Kanälen zu speichern, erscheint die folgende Fehlermeldung und Sie können das Profil nicht speichern:

```
Invalid channel count.
Maximum channel count may not exceed 6
```

5 Wählen Sie „Save“, und betätigen Sie dann die Eingabetaste, um die Änderungen zu speichern.

IP-Routing

3

Überblick

Die folgenden neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie das IP-Routing auf Ihrer Einheit einrichten:

IP-Sicherheit 3-2
Entfernen unterbrochener Hostverbindungen 3-25
Netzwerkübersichten für Adreß-Pools 3-28
Standard-Routen pro Benutzer angeben 3-28
Unterstützung von mehreren IP-Routing-Protokollen 3-30
Änderungen an der Routing-Tabelle und am Diagnosemodus 3-37
Routing auf Schnittstellenbasis 3-40
Multicast-Weiterleitung und IGMP-Funktion 3-45

IP-Sicherheit

Gilt nur für die Pipeline 50 und 75. Die Pipeline kann Pakete mit Verschlüsselungs- und Authentifizierungskopfzeilen, wie in den RFCs 1826, 1827, 1828, 1829, 1851 und 1852 beschrieben, verkapseln und entkapseln. Sie können die IP-Sicherheit über die VT100-Menüs einrichten und steuern.

Überblick über IP-Sicherheit

In der folgenden Tabelle werden die neuen Begriffe und Konzepte in IP-Sicherheit erläutert.

Konzept	Beschreibung
Security Association (SA)	Eine Sammlung von Parametern und Statusvariablen, die von einer Sicherheitsumwandlung bei der Datenübertragung zwischen zwei Systemen verwendet wird. Eine Security Association wird eindeutig mit einem Security Parameter Index (SPI) und einer Ziel-IP-Adresse angegeben. Sie enthält sowohl geheime Informationen zur Verschlüsselung, Entschlüsselung oder Authentifizierung als auch andere Informationen zur Umwandlung. Eine Security Association beschreibt nur eine Verkapselung für eine Richtung (z. B. ausgehende ESP/DES-CBC an eine bestimmte IP-Adresse).
Security Parameter Index (SPI)	Ein ganzzahliger 32 Bit-Wert, den die Pipeline zusammen mit der Zieladresse verwendet, um eine Security Association zu wählen.

Konzept	Beschreibung
Security scheme	Eine Vorlage, die die IP-Adresse der Gegenstelle eines Tunnels, vier SAs und ihre zugehörigen SPIs, Schlüssel und andere umwandlungsspezifische Parameter enthält. Sie können diese Vorlage mit einem Satz neuer Parameter in der VT100-Schnittstelle einrichten. Sie müssen nicht alle SAs konfigurieren, aber zumindest eines pro aktivem Schema. Die Pipeline kann nur die von Ihnen angegebenen SAs verwenden, um die zu übertragenden Pakete zu verkapseln oder um empfangene Pakete zu überprüfen.
Transform	Ein Verfahren, mit dem das Ergebnis der Zuweisung eines Sicherheitsalgorithmus zu einem Benutzerpaket, einschließlich der erforderlichen Schlüssel, Geheimnisse oder Parameter verkapselt wird. Eine AH-Authentifizierungsumwandlung (IP Authentication Header, RFC 1826) führt die Benutzerauthentifizierung durch. Die Pipeline unterstützt die Authentifizierungsumwandlung AH-MD5 (RFC 1828) und AH-SHA (RFC 1852). Eine ESP-Verschlüsselungsumwandlung (IP Encapsulating Security Payload, RFC 1827) führt die Verschlüsselung von Daten durch. Die Pipeline unterstützt die Verschlüsselungsumwandlungen ESP-DES-CBC (RFC 1829) und ESP-3DES-EDE-CBC (RFC 1851).
Tunnel	Sie richten einen IP-Sicherheitstunnel mit dem lokalen Router als einem Endpunkt und dem entfernten System als anderem Endpunkt ein. Das System am entfernten Ende des Tunnels überprüft und entschlüsselt die verkapselten Pakete, die von der Pipeline ausgesandt wurden. Nach der Entkapselung des Pakets leitet der entfernte Tunnelendpunkt das entschlüsselte und entauthentifizierte Paket an sein Endziel weiter.

Konzept	Beschreibung
Static scheme	Ein Sicherheitsschema mit einer festen, entfernten Tunnel-IP-Adresse.
Mobile scheme	Ein Sicherheitsschema ohne konfigurierte, entfernte Tunnel-IP-Adresse. Die Pipeline entnimmt die Adresse eines entfernten Tunnelendpunkts dem ersten Paket, das in einer Sitzung von diesem entfernten Ende eingeht. Ein mobiles Schema ist von Vorteil, falls es sich bei dem entfernten System um den Kunden eines ISP handelt, das den Einwählverbindungen der Kunden dynamisch IP-Adressen zuweist.
Scheme database SA database	Beim Systemstart überprüft die Pipeline alle Schemata und trägt sie in der Scheme-Datenbank ein. Außerdem trägt die Pipeline alle vier SAs zusammen mit den von Ihnen festgelegten Parametern in die SA-Datenbank ein. Wenn Sie ein Schema über die VT100-Schnittstelle hinzufügen, löschen oder ändern, aktualisiert die Pipeline die beiden Datenbanken entsprechend. Konflikte führen zu einer Fehlermeldung und fehlerhafte Schemata werden nicht gespeichert.

Einrichten von IP Security

Sie können IP Security anhand der folgenden Schritte einrichten. Vollständige Informationen zu den Parametern finden Sie im Abschnitt „Neue Parameter“ auf Seite 3-8.

1 Wenn Sie die Funktion IP-Sicherheit einrichten wollen, müssen Sie den korrekten Code für den Parameter „IP Security“ im Menü „System > Feature Codes“ angeben.

Beispiel: Ihre Spezifikation könnte folgendermaßen aussehen:

```
20-400 Feature Codes
 >IP Security=ips-yg38-t22b-r+
```

2 Öffnen Sie das Menü „Ethernet > IP Security“, das eine Reihe von konfigurierbaren Sicherheitsschemata enthält.
Beispiel:

```
20-600 IP Security
 >20-601 Harrison
  20-602 Jackson
  20-603 Anderson
  20-604
  20-605
```

3 Öffnen Sie ein neues Schema.
Beispiel:

```
20-604
 >Name=
  Active=No
  Mobile=No
  Tunnel Address=0.0.0.0
  Received Auth...
  Transmitted Auth...
  Received Crypt...
  Transmitted Crypt...
```

4 Geben Sie für den Parameter „Name“ den Namen des Schemas, der bis zu 16 Zeichen lang sein kann, ein. Als Standardwert wird dieses Feld leer gelassen.

5 Legen Sie „Active=Yes“ fest.

6 Geben Sie für den Parameter „Mobile“ an, ob es im Schema „Security“ eine feste IP-Adresse für den entfernten Endpunkt des Tunnels gibt.

Falls es im Schema „Security“ eine feste IP-Adresse gibt, legen Sie „Mobile=No“ fest. Falls es im Schema „Security“ keine feste IP-Adresse gibt, legen Sie „Mobile=Yes“ fest. Der Standardwert ist „No“.

7 Geben Sie für den Parameter „Tunnel Address“ die IP-Adresse des entfernten Systems an, das die von der Pipeline ausgehenden, sicherheitsverkapselten Pakete überprüft und entschlüsselt.

Nach der Entkapselung des Pakets leitet der entfernte Tunnelendpunkt das entschlüsselte und entauthentifizierte Paket an sein Endziel weiter. Sie richten einen IP-Sicherheitstunnel mit dem lokalen Router als einem Endpunkt und dem entfernten System als anderem Endpunkt ein.

8 Wenn Sie Parameter zur Authentifizierung empfangener Pakete angeben wollen, müssen sie den Eintrag „Received Auth“ öffnen.
Beispiel:

```
20-604 Easthampton
  Received Auth...
  >SPI=1
  Transform=None
  MD5 Key=N/A
  SHA-1 Key=N/A
```

Die Werte, die Sie im Menü „Received Auth“ festlegen, müssen den Werten entsprechen, die am entfernten Ende des IP-Security-Tunnels für die gleichen Parameter im Menü „Transmitted Auth“ festgelegt wurden.

9 Legen Sie für den Parameter „SPI“ den von der Pipeline verwendeten Security Parameters Index (SPI) zusammen mit der Zieladresse fest, um eine Security Association (SA) auszuwählen.

Geben Sie eine ganze Zahl zwischen 1 und 4294967295 ein. Der Standardwert ist 1. Der hier angegebene Wert muß sich von jedem anderen auf dem Router konfigurierten SPI unterscheiden.

10 Legen Sie für den Parameter „Transform“ eine Authentifizierungsumwandlung fest.

MD5 steht für die Authentifizierungsumwandlung „AH-MD5“ (RFC 1828). SHA-1 steht für die Authentifizierungsumwandlung „AH-SHA-1“ (RFC 1852). „None“ deaktiviert „Security Association (SA)“. Der Standardwert ist „None“.

11 Falls „Transform=MD5“ ist, stellen Sie den Parameter „MD5 Key“ ein.

12 Falls „Transform=SHA-1“ ist, stellen Sie den Parameter „SHA-1 Key“ ein.

13 Wenn Sie Parameter für die Authentifizierung übertragener Pakete angeben wollen, müssen Sie zum Menü „Security Scheme“ zurückkehren und den Eintrag „Transmitted Auth“ wählen.
Beispiel:

```
20-604 Easthampton
  Transmitted Auth...
  >SPI=1
  Transform=None
  MD5 Key=N/A
  SHA-1 Key=N/A.
```

14 Stellen Sie einen Wert für die Parameter „SPI“ und „Transform“ sowie für „MD5 Key“ oder „SHA-1 Key“ ein. Die Werte, die Sie im Menü „Transmitted Auth“ einstellen, müssen den Werten entsprechen, die am entfernten Ende des IP-Security-Tunnels für die gleichen Parameter im Menü „Received Auth“ festgelegt wurden.

15 Wenn Sie Parameter für die Verschlüsselung von empfangenen Paketen festlegen wollen, müssen Sie zum Menü „Security Scheme“ zurückkehren und den Eintrag „Received Crypt“ wählen.
Beispiel:

```
20-604 Easthampton
  Received Crypt...
  >SPI=1
  Transform=None
  DES Key=N/A
  DES IV Length=N/A
  3DES Key 1=N/A
  3DES Key 2=N/A
  3DES Key 3=N/A
  3DES IV Length=N/A
```

Die Werte, die Sie im Menü „Received Crypt“ festlegen, müssen den Werten entsprechen, die am entfernten Ende des IP-Security-Tunnels für die gleichen Parameter im Menü „Transmitted Crypt“ festgelegt wurden.

16 Stellen Sie den Parameter „SPI“ ein.

17 Stellen Sie für den Parameter „Transform“ eine Verschlüsselungsumwandlung ein.

DES-CBC steht für die Verschlüsselungsumwandlung „ESP-DES-CBC“ (RFC 1829). 3DES-CBC steht für die Verschlüsselungsumwandlung „ESP-3DES-EDE-CBC“ (RFC 1851). „None“ deaktiviert „Security Association (SA)“. Der Standardwert ist „None“.

18 Falls „Transform=DES-CBC“ ist, legen Sie die Parameter „DES Key“ und „DES IV Length“ fest.

19 Falls „Transform=3DES-CBC“ ist, legen Sie die Parameter „3DES Key“ und „3DES IV Length“ fest.

20 Wenn Sie Parameter für die Verschlüsselung übertragener Pakete festlegen wollen, müssen Sie zum Menü „Security Scheme“ zurückkehren und den Eintrag „Transmitted Crypt“ wählen.
Beispiel:

```
20-604 Easthampton
  Transmitted Crypt...
  >SPI=1
  Transform=None
  DES Key=N/A
  DES IV Length=N/A
  3DES Key 1=N/A
  3DES Key 2=N/A
  3DES Key 3=N/A
  3DES IV Length=N/A
```

21 Legen Sie für jeden Parameter einen Wert fest.
Die Werte, die Sie im Menü „Transmitted Crypt“ festlegen, müssen den Werten entsprechen, die am entfernten Ende des IP-Security-Tunnels für die gleichen Parameter im Menü „Received Crypt“ festgelegt wurden.

22 Speichern Sie die Änderungen.

Neue Parameter

3DES IV Length

Beschreibung: Gibt die Bit-Anzahl im Initialisierungsvektor an.

Wenn das System eine Blockchiffrierung (wie DES) in Modus „Cipher Block Chaining“ (CBC) verwendet, wird ein Block unter Verwendung des vorhergehenden Blocks verschlüsselt. Da es für den ersten Block in einem Paket keinen vorhergehenden Block gibt, fügt das System jedem Paket einen Initialisierungsvektor hinzu, um den Vorgang zu starten.

Verwendung: Sie können 32 oder 64 Bit angeben. Der Standardwert ist 32.

Abhängigkeiten: Wenn Sie den Parameter „3DES IV Length“ zuweisen wollen, müssen Sie die Verschlüsselungsumwandlung „ESP-3DES-EDE-CBC“ angeben, indem Sie „Transform=3DES-CBC“ eingeben.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Crypt und Ethernet > IP Security > *Schema* > Transmitted Crypt

Siehe auch: Transform

3DES Key *n*

Beschreibung: Gibt „3DES Key“, ein von Tunnelendpunkten gemeinsam benutztes Geheimnis, an.

Verwendung: Geben Sie einen 64 Bit-hexadezimalen Wert an. Ein Byte muß sieben Bit für den Schlüssel und ein Bit (das Bit 01) für ungerade Parität enthalten. Falls Sie einen Schlüssel mit ungültiger Parität eingeben und speichern, erscheint eine Warnung, und die Pipeline berichtigt die Parität, speichert das Profil aber nicht. Erst wenn Sie die Speichertaste erneut betätigen, wird es gespeichert.

Abhängigkeiten: Wenn Sie den Parameter „3DES Key“ zuweisen wollen, müssen Sie die Verschlüsselungsumwandlung „ESP-3DES-EDE-CBC“ angeben, indem Sie „Transform=3DES-CBC“ festlegen.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Crypt und Ethernet > IP Security > *Schema* > Transmitted Crypt

Siehe auch: Transform

Active

Beschreibung: Gibt an, ob das Schema „IP Security“ aktiviert ist.

Verwendung: Geben Sie eine der folgenden Einstellungen an:

- „Yes“ aktiviert das Schema.
- „No“ deaktiviert das Schema.
  Der Standardwert ist „No“. Wenn Sie diesen Wert wählen, erscheint der Name des Schemas mit einem Bindestrich und einer vorausgehenden Leerstelle im Menü „Ethernet > IP Security“.

Parameter-Ort: Ethernet > IP Security > *Schema*

Siehe auch: Mobile, Name, Tunnel Address

DES IV Length

Beschreibung: Gibt die Bit-Anzahl im Initialisierungsvektor an.

Verwendung: Sie können 32 oder 64 Bit angeben. Der Standardwert ist 32.

Abhängigkeiten: Wenn Sie den Parameter „DES IV Length“ zuweisen wollen, müssen Sie die Verschlüsselungsumwandlung „ESP-DES-CBC“ angeben, indem Sie „Transform=DES-CBC“ einstellen.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Crypt und Ethernet > IP Security > *Schema* > Transmitted Crypt

Siehe auch: Transform

DES Key

Beschreibung: Gibt „3DES Key“, ein von Tunnelendpunkten gemeinsam benutztes Geheimnis, an.

Verwendung: Geben Sie einen 64 Bit-hexadezimalen Wert an. Ein Byte muß sieben Bit für den Schlüssel und ein Bit (das Bit 01) für ungerade Parität enthalten. Falls Sie einen Schlüssel mit ungültiger Parität eingeben und speichern, erscheint eine Warnung, und die Pipeline berichtigt die Parität, speichert das Profil aber nicht. Erst wenn Sie die Speichertaste erneut betätigen, wird es gespeichert.

Abhängigkeiten: Wenn Sie den Parameter „DES Key“ zuweisen wollen, müssen Sie die Verschlüsselungsumwandlung „ESP-DES-CBC“ angeben, indem Sie „Transform=DES-CBC“ einstellen.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Crypt und Ethernet > IP Security > *Schema* > Transmitted Crypt

Siehe auch: DES IV Length, Transform

IP Security

Beschreibung: Gibt den Funktionscode „IP Security“ an - eine Zeichenfolge, mit der die Funktion IP-Sicherheit auf der Pipeline aktiviert wird. Sie erhalten den Funktionscode, wenn Sie das Produkt erwerben. Nachdem Sie ihn für den Parameter „IP Security“ eingegeben und die Pipeline erneut gestartet haben, ist die Funktion aktiviert.

Verwendung: Geben Sie den Funktionscode „IP Security“ an. Ein korrekter Code aktiviert eine von drei Stufen in „IP Security“. Der Status von „IP Security“ wird auf der Pipeline im Menü „Sys Option“ angezeigt. Je nachdem, welchen Funktionscode Sie eingeben, erscheint eine der folgenden Optionen:

- IPsec Not Inst - „IP Security“ nicht installiert
- IPsec Inst 40 Bit - „IP Security“ mit bis zu 40 Bit-Verschlüsselung installiert
- IPsec Inst 56 Bit - „IP Security“ mit bis zu 56 Bit-Verschlüsselung installiert
- IPsec Unlimited - „IP Security“ mit Verschlüsselung willkürlicher Länge installiert

Parameter-Ort: System > Feature Codes

MD5 Key

Beschreibung: Gibt „MD5 Key“, ein von Tunnelendpunkten gemeinsam benutztes Geheimnis, an.

Verwendung: Geben Sie eine Bit-Folge mit einer geraden Anzahl hexadezimaler Zahlen an. Sie müssen mindestens zwei Zahlen angeben, aber nicht mehr als 32. Als Standardwert bleibt das Feld leer.

Abhängigkeiten: Wenn Sie den Parameter „MD5 Key“ zuweisen wollen, müssen Sie die Authentifizierungsumwandlung „AH-MD5“ angeben, indem Sie „Transform=MD5“ einstellen.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Auth und Ethernet > IP Security > *Schema* > Transmitted Auth

Siehe auch: SHA-1 Key, SPI, Transform

Mobile

Beschreibung: Gibt an, ob es im Security-Schema eine feste IP-Adresse für den entfernten Endpunkt des Tunnels gibt. Gibt es keine, ist das Schema mobile.

Die Pipeline trägt zunächst kein mobiles Schema in die Schema-Datenbank ein. Wenn die Pipeline ein Paket empfängt, das sie authentifizieren kann, markiert die Pipeline das ursprüngliche, mobile Schema als besetzt. Anschließend trägt sie eine Kopie des Schemas in die Schema-Datenbank ein, indem Sie die im empfangenen Paket enthaltene Tunneladresse in das neu erstellte Schema kopiert. Durch dieses Verfahren kann die Pipeline mit dem neu erstellten Schema übertragene Antwortpakete verkapseln und weitere, von dem selben entfernten System empfangene Pakete abstimmen.

Wenn es zu einem mobilen Schema keinen Eintrag in der Schema-Datenbank gibt, verfügt es nicht über einen zugehörigen Tunnel und die Pipeline kann es daher nicht verwenden, um übertragene Pakete zu verkapseln. Falls ein Paket empfangen wird und auf eine Weise authentifiziert wird, so daß ein mobiles Schema mit einer anderen IP-Adresse als Tunnelendpunkt verbunden wird, ändert die Pipeline die Eintragung in der Datenbank, um auf die neue Tunneladresse zu verweisen. Daher kann die Pipeline ein mobiles Schema immer nur für je ein entferntes System verwenden.

Verwendung: Geben Sie eine der folgenden Einstellungen an:

- „Yes“ gibt an, daß das Schema mobil ist.
- „No“ gibt an, daß das Schema nicht mobil ist.
  Der Standardwert ist „No“.

Abhängigkeiten: Wenn „Mobile=No“ ist, ist „Tunnel Address“ nicht zutreffend.

Parameter-Ort: Ethernet > IP Security > *Schema*

Siehe auch: Active, Name, Tunnel Address

Name

Beschreibung: Gibt den Namen des IP Security-Schemas an.

Verwendung: Geben Sie einen aus bis zu 16 Zeichen bestehenden Namen an. Als Standardwert bleibt dieses Feld leer.

Die Pipeline indiziert ein Schema mit ganzen Zahlen: 1 (eins) für das erste Schema, 2 (zwei) für das zweite Schema usw. Die Pipeline kann Sicherheitsschemata dynamisch zuweisen, d. h. sie wählt die gleiche Zahl und läßt ausreichenden Platz für alle möglichen statischen Schemata.

Parameter-Ort: Ethernet > IP Security > *Schema*

Siehe auch: Active, Mobile, Tunnel Address

SHA-1 Key

Beschreibung: Gibt „SHA-1 Key“, ein von Tunnelendpunkten gemeinsam benutztes Geheimnis, an.

Verwendung: Geben Sie eine Bit-Folge mit einer geraden Anzahl hexadezimaler Zahlen an. Sie müssen mindestens zwei Zahlen angeben, aber nicht mehr als 40. Als Standardwert bleibt das Feld leer.

Abhängigkeiten: Wenn Sie den Parameter „SHA-1 Key“ zuweisen wollen, müssen Sie die Authentifizierungsumwandlung „AH-SHA-1“ angeben, indem Sie „Transform=SHA-1“ einstellen.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Auth und Ethernet > IP Security > *Schema* > Transmitted Auth

Siehe auch: MD5 Key, SPI, Transform

SPI

Beschreibung: Gibt den von der Pipeline verwendeten Security Parameters Index (SPI) zusammen mit der Zieladresse an, um eine Security Association (SA) auszuwählen.

Verwendung: Geben Sie eine ganze Zahl zwischen 1 und 4294967295 ein. Der Standardwert ist „1“. Der hier angegebene Wert muß sich von jedem anderen auf dem Router konfigurierten SPI unterscheiden.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Auth,
Ethernet > IP Security > *Schema* > Transmitted Auth,
Ethernet > IP Security > *Schema* > Received Crypt und
Ethernet > IP Security > *Schema* > Transmitted Crypt

Siehe auch: MD5 Key, SHA-1 Key, Transform

Transform

Beschreibung: Gibt ein Verfahren an, mit dem das Ergebnis der Zuweisung eines Sicherheitsalgorithmus zu einem Benutzerpaket, einschließlich der erforderlichen Schlüssel, Geheimnisse oder Parameter verkapselt wird.

Verwendung: In den Menüs „Received Auth“ und „Transmitted Auth“ können Sie eine Authentifizierungsumwandlung angeben. Wählen Sie einen dieser Werte:

- „MD5“ steht für die Authentifizierungsumwandlung AH-MD5 (RFC 1828).
- DES-CBC (40 Bit)
- „SHA-1“ steht für die Authentifizierungsumwandlung AH-SHA-1 (RFC 1852).
- „None“ deaktiviert „Security Association“.
  Der Standardwert ist „None“.

In den Menüs „Received Crypt“ und „Transmitted Crypt“ können Sie eine Verschlüsselungsumwandlung angeben. Wählen Sie einen dieser Werte:

- „DES-CBC“ steht für die Verschlüsselungsumwandlung ESP-DES-CBC (RFC 1829).

- „3DES-CBC“ steht für die Verschlüsselungsumwandlung ESP-3DES-EDE-CBC (RFC 1851).
- „None“ deaktiviert „Security Association“.

  Der Standardwert ist „None“.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Wenn „Transform=MD5“ ist, müssen Sie einen Wert für den Parameter „MD5 Key“ festlegen. Der Parameter „SHA-1 Key“ ist nicht zutreffend.
- Wenn „Transform=SHA-1“ ist, müssen Sie einen Wert für den Parameter „SHA-1 Key“ festlegen. Der Parameter „MD5 Key“ ist nicht zutreffend.
- Wenn „Transform=DES-CBC“ ist, müssen Sie einen Wert für den Parameter „DES Key“ festlegen. Die Parameter „3DES Key“ und „3DES IV Length“ sind nicht zutreffend.
- Wenn „Transform=3DES-CBC“ ist, müssen Sie mindestens einen Wert für den Parameter „DES Key“ festlegen. Die Parameter „DES Key“ und „DES IV Length“ sind nicht zutreffend.

Parameter-Ort: Ethernet > IP Security > *Schema* > Received Auth,
Ethernet > IP Security > *Schema* > Transmitted Auth,
Ethernet > IP Security > *Schema* > Received Crypt und
Ethernet > IP Security > *Schema* > Received Auth

Siehe auch: 3DES Key, 3DES IV Length, DES Key, DES IV Length, MD5 Key, SHA-1 Key

Tunnel Address

Beschreibung: Gibt die IP-Adresse des entfernten Systems an, das die von der Pipeline ausgesandten, verkapselten Pakete überprüft und entschlüsselt. Nach der Entkapselung des Pakets leitet der entfernte Tunnelendpunkt das entschlüsselte und entauthentifizierte Paket an sein Endziel weiter.

Sie richten einen IP-Sicherheitstunnel mit dem lokalen Router als einem Endpunkt und dem entfernten System als anderem Endpunkt ein.

Verwendung: Geben Sie eine IP-Adresse in punktierter Dezimalschreibweise an. Der Standardwert ist 0.0.0.0.

Parameter-Ort: Ethernet > IP Security > *Schema*

Siehe auch: Active, Mobile, Name

Neue Diagnosebefehle

In diesem Abschnitt werden neue Diagnosebefehle beschrieben, die zur Unterstützung der Funktion IP-Sicherheit hinzugefügt wurden.

IPsecSADump

Mit diesem Befehl werden alle Security Associations angezeigt, die sich zur Zeit in der Datenbank befinden. Geben Sie den Befehl ohne optionale Argumente ein:

>IPsecSADump

Die angezeigten Informationen können folgendermaßen aussehen:

```
SA at 0x2c3f90 (scheme 1):
  flags=21 <ACTIVE,ESP,MOBILE>
  SPI=2, dst=Mobile(Unset), ESP type=DES3_CBC IV Size=64,
IV=0x26575d3ea7478374
SA at 0x2c3ed0 (scheme 1):
  flags=21 <ACTIVE,ESP,MOBILE>
  SPI=2, dst=Localhost, ESP type=DES_CBC IV Size=32,
IV=0x57f00cb6a80ff349
SA at 0x2c3e10 (scheme 1):
  flags=22 <ACTIVE,AH,MOBILE>
  SPI=1, dst=Mobile(Unset), AH type=SHA1
SA at 0x2c3d50 (scheme 1):
  flags=22 <ACTIVE,AH,MOBILE>
  SPI=1, dst=Localhost, AH type=MD5
```

In der folgenden Tabelle werden die Informationselement beschrieben.

Element	Beschreibung
`flags`	Gibt den Status und die Merkmale der Security Association an. In diesem Feld kann einer der folgenden Werte erscheinen: `ACTIVE` - Die Security Association ist aktiv. `INACTIVE` - Sie is nicht aktiv. `ESP` - Sie verwendet eine ESP-Verschlüsselungsumwandlung (IP Encapsulating Security Payload, RFC 1827). `AH` - Sie verwendet eine AH-Authentifizierungsumwandlung (IP Authentication Header, RFC 1826). `MOBILE` - Sie ist Teil eines mobilen IP Security-Schemas. `LOCKED` - Sie ist Teil eines statischen IP Security-Schemas.
`SPI`	Gibt den von der Pipeline verwendeten SPI zusammen mit der Zieladresse an, um die Security Association zu wählen.
`dst`	Gibt die mit der Security Association verbundene Zieladresse an. In diesem Feld kann einer der folgenden Werte erscheinen: *`local_hostname`* - Gibt den Namen des lokalen Routers an. *`dest_ipaddr`* - Gibt den Namen des Ziel-Hosts an. `Mobile (Unset)`- Gibt eine nicht initialisierte, mobile Security Association an.

Element	Beschreibung
`type`	Gibt den verwendeten Umwandlungstyp an: MD5 - Steht für die Authentifizierungsumwandlung „AH-MD5“ (RFC 1828). SHA1 - Steht für die Authentifizierungsumwandlung „AH-SHA-1“ (RFC 1852). DES_CBC - Steht für die Verschlüsselungsumwandlung „ESP-DES-CBC“ (RFC 1829). DES3_CBC - Steht für die Verschlüsselungsumwandlung „ESP-3DES-EDE-CBC“ (RFC 1851).
`IV size`	Gibt die Bit-Anzahl im Initialisierungsvektor der Verschlüsselungsumwandlung „ESP-3DES-EDE-CBC“ an.
`IV`	Gibt den „3DES key“ an.

IPsecSchemeDump

Mit diesem Befehl wird ein IP Security-Schema oder alle IP Security-Schemata angezeigt, die sich zur Zeit in der Datenbank befinden. Geben Sie den Befehl mit folgender Syntax ein:

>**IPsecSchemeDump** ***integer***

Falls Sie das Argument ***integer*** bei der Eingabe des Befehls angeben, zeigt die Pipeline das der Zahl zugehörige Schema an. Falls Sie dieses Argument nicht angeben, werden mit diesem Befehl alle in der Datenbank enthaltenen Schemata angezeigt.

Wenn Sie den Befehl eingeben, können die angezeigten Informationen folgendermaßen aussehen:

```
SCHEME 1 at 0x2c3d10:

   flags=1 <ACTIVE>

   dst=Unset(Mobile)
```

```
Incoming AH SA at 0x2c3d50, Outgoing AH SA at 0x2c3e10

Incoming ESP SA at 0x2c3ed0, Outgoing ESP SA at 0x2c3f90
```

In der folgenden Tabelle werden die Informationselemente beschrieben.

Element	Beschreibung
`flags`	Gibt den Status des Schemas an. In diesem Feld kann einer der folgenden Werte erscheinen: `ACTIVE` - Das Schema ist aktiv. `INACTIVE` - Das Schema ist nicht aktiv.
`dst`	Gibt die zum Schema gehörige Zieladresse an. In diesem Feld kann einer der folgenden Werte erscheinen: *`dest_ipaddr`* - Gibt den Namen des Ziel-Hosts an. `Mobile (Unset)`- Gibt eine nicht initialisierte, mobile Security Association an.
`Incoming...`	Gibt sowohl die Security Associations an, die der Router empfängt, als auch die interne Router-Speicheradresse, unter der die Daten gespeichert werden. ESP weist darauf hin, daß die Security Association eine ESP-Verschlüsselungsumwandlung (IP Encapsulating Security Payload, RFC 1827) verwendet. AH weist darauf hin, daß sie eine AH-Authentifizierungsumwandlung (IP Authentication Header, RFC 1826) verwendet.
`Outgoing...`	Gibt sowohl die Security Associations an, die der Router überträgt, als auch die interne Router-Speicheradresse, unter der die Daten gespeichert werden.

IPsecdblog

Mit diesem Befehl schalten Sie zwischen den Diagnosestatusmeldungen für IP-Sicherheit hin und her. Geben Sie den Befehl mit folgender Syntax ein:

```
> IPsecdblog d|s y|n
```

In der folgenden Tabelle werden die Informationselemente beschrieben.

Argument	Beschreibung
d y	Gibt an, daß die Pipeline die Diagnosemeldungen der IP-Sicherheit auf dem Diagnosemonitor anzeigt.
d n	Gibt an, daß die Pipeline die Diagnosemeldungen der IP-Sicherheit nicht auf dem Diagnosemonitor anzeigt.
s y	Gibt an, daß die Pipeline die Diagnosemeldungen der IP-Sicherheit im Syslog speichert.
s n	Gibt an, daß die Pipeline die Diagnosemeldungen der IP-Sicherheit nicht im Syslog speichert.

Syslog und Diagnosemeldungen in IP-Sicherheit

Diese Version enthält die folgenden neuen Meldungen, die im Syslog oder auf dem Diagnosemonitor erscheinen können.

Message	Beschreibung
`IPSEC: Scheme` *num*`: Expected remote` *x.x.x.x*`, got` *y.y.y.y*`.`	Der Router hat ein Paket mit SPIs empfangen, die Schema *num* entsprechen, jedoch ging das Paket von *x.x.x.x* ein, und nicht von der für Schema *num* konfigurierten Tunneladresse *y.y.y.y.*
`IPSEC: Scheme` *num1*`: Expecting SPI` *num2*`, got SPI` *num3*	Der Router hat ein Paket mit AH- und ESP-Verschlüsselungen empfangen, aber die beiden SPIs stimmen nicht überein.

Message	Beschreibung
`IPSEC: Scheme` *num1*`: Expecting no encryption, got SPI` *num2*`.`	Der Router hat ein Paket mit SPI *num2*, AH außen und ESP innen, empfangen, aber für Schema *num1* wurde keine Verschlüsselung konfiguriert.
`IPSEC: Failed encap on inactive scheme` *num*	Der Router hat ein Paket für Schema *num* empfangen, während das Schema in der VT100-Schnittstelle aktualisiert wurde. Diese Meldung weist auf einen vorübergehenden Zustand hin.
`IPSEC: Scheme` *num*`: Bogus ICMP Destination Unreachable: Source Route Failed`	Beim Host der Gegenstelle liegt eine Fehlerbedingung vor. Der Router sendet keine quellgerouteten IPSEC-Pakete, daher sollte er diese ICMP-Fehlermeldung nicht erhalten.
`IPSEC: SHA1: Received invalid AH: SPI` *num x.x.x.x -> y.y.y.y*	Der Router hat ein AH-SHA-Paket empfangen, aber die Authentifizierung entsprach nicht derjenigen, die in der VT100-Schnittstelle konfiguriert wurde.
`IPSEC: Received unknown SPI` *num, x.x.x.x -> y.y.y.y*	Ein AH- oder ESP-verkapseltes Paket wurde empfangen, aber SPI *num* wurde auf dieser Pipeline nicht konfiguriert.
`IPSEC: Scheme` *num1*`: Expecting no authentication, got SPI` *num2*	Der Router hat ein Paket mit SPI *num2*, AH außen und ESP innen, empfangen, aber für Schema *num1* wurde keine Authentifizierung konfiguriert.
`IPSEC: Scheme` *num*`: Received packet encapsulation does not match scheme`	Schema *num* wurde zur Verwendung von AH- und ESP-Verkapselung konfiguriert, aber das Paket hat nur einen Verkapselungstyp verwendet.
`IPSEC: Scheme` *num*`: Bogus ICMP Destination Unreachable: Port Unreachable`	Beim Host der Gegenstelle liegt eine Fehlerbedingung vor. Die ICMP-Meldung verweist auf falsche TCP- oder UDP-Anschlußnummern, aber der Router sendet AH- und ESP-Pakete, die keine Anschlußnummern enthalten.

Message	Beschreibung
`IPSEC: MD5: Received invalid AH: SPI` *num x.x.x.x -> y.y.y.y*	Der Router hat ein AH-MD5-Paket empfangen, aber die Authentifizierung entsprach nicht derjenigen, die in der VT100-Schnittstelle konfiguriert wurde.
`IPSEC: Scheme` *num1*`: SPI` *num2* `is not AH,` *x.x.x.x -> y.y.y.y*	Der Router hat ein SPI *num2* AH-Paket empfangen, aber SPI *num2* wurde für ESP konfiguriert.
`IPSEC: Scheme` *num1*`: SPI` *num2* `is not ESP,` *x.x.x.x -> y.y.y.y*	Der Router hat ein SPI *num2* ESP-Paket empfangen, aber SPI *num2* wurde für AH konfiguriert.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `is > 64 hops away`	Sie haben das Schema falsch konfiguriert; es verweist auf einen Tunnelendpunkt, den der Router nicht finden kann.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `doesn't speak AH`	Sie haben das Schema falsch konfiguriert; es verweist auf einen Tunnelendpunkt, der keine AH-Verkapselung verarbeiten kann.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `doesn't speak ESP`	Sie haben das Schema falsch konfiguriert; es verweist auf einen Tunnelendpunkt, der keine ESP-Verkapselung verarbeiten kann.
`IPSEC: Scheme` *num*`: Tunnel endpoint` *x.x.x.x* `is unreachable`	Sie haben das Schema falsch konfiguriert; es verweist auf einen Tunnelendpunkt, den der Router nicht erreichen kann.

Änderungen an der Firewall

In diesem Abschnitt werden Änderungen an der Ascend-Firewall beschrieben.

Diagnosebefehl „FWALLversion“ geändert

Der Diagnosebefehl „FWALLversion“ liefert jetzt eine räumlich begrenzte Liste aller Firewall-Versionen, die der Router akzeptiert. Falls Sie „IP Security“ aktiviert haben, folgt auf die Informationen zur Version der Buchstabe *i*. Ein aktueller Router zeigt z. B. folgende Informationen an:

```
> FWALLversion

FWversion: 1 2 i
```

Der Router akzeptiert Firewall Version 1 oder 2. IP-Sicherheit kann für beide aktiviert sein.

Versionsänderungen

Die Firewall-Versionsnummer lautet jetzt 2, obwohl die Pipeline auch Firewalls der Version 1 akzeptiert und sie korrekt funktionieren.

Sprachänderungen

Die Firewall-Sprache, die von SAM (Programm „Secure Access Manager“ für Windows) in Dateien mit der Erweiterung „.fw“ gespeichert wird, verfügt über vier neue Schlüsselwörter. Mit diesen Schlüsselwörtern können Sie steuern, wie die Pipeline ein- und ausgehenden Paketen IP Security-Umwandlungen zuweist.

In der folgenden Tabelle werden die einzelnen Schlüsselwörter beschrieben.

Schlüsselwort	Beschreibung
scheme=[*Schema*]	Verkapseln übertragener Pakete mit den in *scheme* enthaltenen Informationen. Beim Empfang wird das eingegangene Paket mit den Parametern in *scheme* verglichen und nur dann akzeptiert, wenn alle Parameter übereinstimmen. Falls kein Schema-Argument erscheint, verwendet die Pipeline ein mit der dynamischen Auslöseregel erinnertes Schema. Verwenden Sie dieses Schlüsselwort nur in dynamischen Regelschablonen ohne das Argument *scheme*.
auth	Weisen Sie nur empfangene Pakete zu, die erfolgreich authentifiziert wurden.
crypt	Weisen Sie nur empfangene Pakete zu, die erfolgreich entschlüsselt wurden.

Änderungen in Syslog-Meldungen des Firewalls

Die einzeiligen Meldungsübersichtszeilen, die angezeigt werden, wenn ein Firewall ein Paket protokolliert, können jetzt spezifische Informationen zur IP-Sicherheit anzeigen:

- Protokollierte IP-Pakete mit einem Protokollfeld 50 werden als *esp* und nicht als *50* angezeigt.
- Protokollierte IP-Pakete mit einem Protokollfeld 51 werden als *ah* und nicht als *51* angezeigt.
- Bei empfangenen IP-Paketen, die erfolgreich authentifiziert wurden, wird am Ende der protokollierten Meldung die Folge *auth* angehängt.
- Bei empfangenen IP-Paketen, die erfolgreich entschlüsselt wurden, wird am Ende der protokollierten Meldung die Folge *crypt* angehängt.

Entfernen unterbrochener Hostverbindungen

In vorhergehenden Versionen wurden die Routen, die mit Verbindungsprofilen verbunden waren, immer bekanntgemacht und der Routing-Tabelle der Pipeline hinzugefügt, selbst wenn die Verbindung unterbrochen war. Dies stellte in einigen Situationen ein Problem dar, insbesondere für Benutzer von festen Leitungen, denn diese Benutzer wollten Routen nicht bekanntmachen, wenn die Verbindung unterbrochen war. In der vorliegenden Version können Sie die Pipeline anweisen, Routen aus der Routing-Tabelle zu entfernen, wenn die zugehörige Verbindung offline ist, und diese Routen nicht bekanntzumachen.

Überblick

Die Pipeline macht Adressen, die Verbindungsprofilen zugeordnet sind, bekannt als Routen, mit denen sie eine Verbindung herstellen kann. Als Standard werden diese Adressen bekanntgemacht, selbst wenn die Verbindung unterbrochen ist, da sie für Verbindungen, die die Pipeline bei Bedarf herstellt, erforderlich sind.

Es gibt jedoch einige Situationen, in denen diese Bekanntmachung Probleme verursacht. Bei einer festen Leitung geht man davon aus, daß die Verbindung immer steht. Wenn sie jedoch unterbrochen ist, sind die Routen zu dieser Verbindung erst wieder erforderlich, wenn sie wieder hergestellt wird. Das folgende Beispiel illustriert dieses Problem:

Pipeline1 und Pipeline2 befinden sich auf demselben lokalen LAN.

- Pipeline1 verfügt über eine feste Leitung zu einer entfernten Stelle. Die Adresse der Gegenstelle enthält den Parameter „Metric=4“.
- Pipeline2 ist eine Reserveverbindung. Die Adresse ihrer Gegenstelle enthält den Parameter „Metric=7“.

Der Verkehr läuft aufgrund der niedrigeren Metrik über Pipeline1. Falls die feste Verbindung von Pipeline1 unterbrochen wird, wird ihre Route zum entfernten Netzwerk als Standard weiterhin bekanntgemacht. Daher erscheint die in Pipeline2 angegebene Verbindung nie.

Über den Parameter „Temporary“ können Sie festlegen, daß die Pipeline die Route zu einer inaktiven Verbindungsadresse entfernt. Sie finden diesen Parameter im Untermenü „IP Options“ des Verbindungsprofils.

Änderungen an der Benutzerschnittstelle

Temporary

Beschreibung: Gibt an, ob die Pipeline die Bekanntmachung einer Route zur Adresse in diesem Verbindungsprofil beendet, wenn die Verbindung unterbrochen wird, und ob die Pipeline diese Route und alle auf dieser Verbindung dynamisch erlernten Routen aus der Routing-Tabelle entfernt.

Verwendung: Sie können eine der folgenden Einstellungen angeben:

- Mit „Yes“ wird eine Route zu einer Verbindung aus der Routing-Tabelle entfernt (dies gilt auch für Routen, die dynamisch auf dieser Verbindung erlernt wurden), wenn die Verbindung offline ist, und macht die Route nicht weiter bekannt.

  Nachdem die Verbindung wiederhergestellt ist, wird die Route wieder bekanntgemacht, und sie erscheint wieder in der Routing-Tabelle.
- Mit „No“ wird weiterhin die in den Parametern „LAN Adrs“ und „WAN Alias“ angegebene Route zu einer Verbindung bekanntgemacht, selbst wenn die Verbindung offline ist.

  Die Route erscheint zusammen mit allen Routen, die dynamisch auf dieser Verbindung erlernt wurden, in der Routing-Tabelle der Pipeline. Alle Routen altern normal. Der Standardwert ist „No“.

Beispiel: Pipeline1 verfügt über eine feste Verbindung mit der Adresse 128.50.69.69. Pipeline1 macht diese Adresse bekannt, wenn die Verbindung steht. Pipeline1 erfährt über RIP, daß die Gegenstelle 198.5.248.72 bekanntmacht. Falls die Verbindung unterbrochen wird und „Temporary=Yes“ festgelegt wurde, entfernt die Pipeline 128.50.69.69 und 198.5.248.72 aus ihrer Routing-Tabelle und macht sie nicht mehr bekannt. Falls die Verbindung unterbrochen wird und „Temporary=No“ festgelegt wurde, bleibt 128.50.69.69 in der Routing-Tabelle (mit dem Hinweis „wanidle“ für die ruhende Verbindung) und gestattet es 198.5.248.72 normal zu altern.

Abhängigkeiten: Bei einer Frame Relay-Verbindung handelt es sich um eine feste Verbindung, die in einem Verbindungsprofil definiert wurde. Eine Frame Relay-Verbindung kann auch über ein zugewiesenes Reserve-Verbindungsprofil verfügen; falls die Verbindung unterbrochen wird, stellt die Pipeline die Verbindung mit dem Reserveprofil her. Sie können das Reserveprofil mit dem Parameter „Backup“ angeben. Bei Frame Relay-Verbindungen wirkt sich der Parameter „Temporary“ unterschiedlich aus, je nachdem, ob es für die Verbindung ein Reserveprofil gibt oder nicht:

- Falls eine Frame Relay-Verbindung, für die es ein Reserveprofil gibt, unterbrochen wird, ignoriert die Pipeline die Einstellung „Temporary=Yes“. Die Pipeline entfernt keine Routen aus der Routing-Tabelle, wenn die Frame Relay-Verbindung unterbrochen wird.
- Falls eine Frame Relay-Verbindung, für die es kein Reserveprofil gibt, unterbrochen wird, folgt die Pipeline der Einstellung „Temporary=Yes“. Die Pipeline entfernt Routen aus der Routing-Tabelle, wenn die Frame Relay-Verbindung unterbrochen wird.

Parameter-Ort: Connection profile > IP Options > Temporary.

Änderung in der IP Routing-Anzeige

In der IP Routing-Anzeige wird eine temporäre Route jetzt mit „T“ markiert. Im folgenden Beispiel werden durch die Verwendung des Befehls „Show IP Routes“ zwei temporäre Routen angezeigt:

```
ascend% show ip routes
Destination          Gateway          IF      Flg   Pref   Met   Use   Age
192.168.252.0/30     192.168.252.1    wan10   rGT   60     7     0     7
192.168.252.1/32     192.168.252.1    wan10   rT    60     7     1     7
```

Netzwerkübersichten für Adreß-Pools

Die beiden folgenden Schnittstellen wurden den Routing-Tabellen hinzugefügt:

- Die Schnittstelle „Reject“ (rj0)

  Die Schnittstelle „Reject“ hat die IP-Adresse 127.0.0.2. Pakete mit einer Route zu dieser Schnittstelle werden mit einer ICMP-Meldung “host unreachable” an die Quelladresse zurückgesandt.
- Die Schnittstelle „black-hole“ (bh0)

  Die Schnittstelle „black-hole“ hat die IP-Adresse 127.0.0.3. Pakete, mit einer Route zu dieser Schnittstelle werden ohne Hinweise vernichtet.

Standard-Routen pro Benutzer angeben

In einem Verbindungsprofil können Sie jetzt Standard-Routen pro Benutzer angeben. Falls ein Bediener einen bestimmten Service verwendet, können Sie die `Pipeline` veranlassen, Datenverkehr an den vom Service verwendeten Router zu senden, selbst, wenn es sich bei dem Router nicht um den Standard-Gateway, der in der systemumfassenden Routing-Tabelle angezeigt wird, handelt.

Überblick

Falls Sie eine Standardroute in einem Verbindungsprofil angeben, routet die Pipeline IP-Pakete folgendermaßen:

1 Die Pipeline sucht in der Routing-Tabelle nach der Adresse des nächsten Routers.

2 Falls es sich beim nächsten Router um die Standardroute des Systems (Ziel 0.0.0.0) handelt, verwendet die Pipeline die pro Benutzer festgelegte Standardadresse als nächsten Router anstelle der systemumfassenden Standardroute.

Die Pipeline verwendet die pro Benutzer festgelegte Standardadresse auch dann, falls die normale Routing-Logik scheitert und es keine systemumfassenden Standardroute gibt.

Diese Funktion gilt für das Routing aller Pakete, die von einer Schnittstelle mit einem gegebenen Profil empfangen wurden, und ist unabhängig von der spezifischen IP-Quelladresse; daher können Sie diese Funktion verwenden, wenn das Profil zu einem anderen Zugangs-Router gehört und alle Hosts hinter diesem Router den Standard-Gateway verwenden. Während sich dies auf alle Pakete auswirkt, die bei der Schnittstelle mit dem gegebenen Profil eingehen, geht die Pipeline mit Paketen, die von anderen Benutzern oder vom Ethernet eingehen, wie üblich um. Außerdem ändert diese Funktion nicht die globale Routing-Tabelle.

Änderungen an der Konfigurationsschnittstelle

Wenn Sie eine Route pro Benutzer in der Konfigurationsschnittstelle der Pipeline konfigurieren wollen, müssen Sie den Parameter „Client Gateway“ im Menü „IP Options“ des Verbindungsprofils festlegen.

Client Gateway

Beschreibung: Gibt die Standardroute für IP-Pakete an, die von einem Benutzer über diese Verbindung eingehen.

Verwendung: Legen Sie die IP-Adresse für den nächsten Router in punktierter Dezimalnotation fest. Der Standardwert ist 0.0.0.0; falls Sie diesen Wert akzeptieren, leitet die Pipeline Pakete, wie in der Routing-Tabelle angegeben, über die systemumfassende Standardroute weiter, falls sie keine spezifischere Route finden kann.

Die Pipeline muß über eine direkte Route zur angegebenen Adresse verfügen. Die direkte Route kann über ein Profil oder eine Ethernet-Verbindung erfolgen. Falls die Pipeline über keine direkte Route verfügt, legt sie die Pakete auf der Verbindung ab. Wenn Sie eine Diagnose von Routing-Problemen an einem Profile, das diese Funktion verwendet, durchführen, ist ein Fehler in einer Gateway-Adresse auf Pro-Benutzer-Basis bei einer Inspektion der globalen Routing-Tabelle nicht erkennbar.

Beispiel: Falls Sie in einem Profil „Client Gateway=10.0.0.3“ festlegen, werden IP-Pakete des Benutzers mit Zielen über die Standardroute bei 10.0.0.3 über das Gateway geleitet.

Parameter-Ort: Verbindungsprofil: Ethernet > Connections > *Profile* >IP Options

Unterstützung von mehreren IP-Routing-Protokollen

Diese Softwareversion enthält Änderungen am IP-Router, die eine Unterstützung für mehrfache IP-Routing-Protokolle, wie RIP-v1 und RIP-v2, bieten.

Routenpräferenzen

Routenpräferenzen bieten eine zusätzliche Kontrolle darüber, welchen Routentypen der Vorzug vor anderen gewährt wird. Pro IP-Adresse und Netzmaske enthält die Routing-Tabelle eine Route je Protokoll, wobei die Protokolle folgendermaßen festgelegt sind:

- verbundene Routen, wie z. B. Ethernet: „Preference=0“
- über ICMP-Redirects erlernte Routen: „Preference=30“.
- Routen, die der Tabelle durch die SNMP-MIB II hinzugefügt wurden: „Preference=100“.
- von RIP erlernte Routen: „Preference=100“.

  Sie können den Standardwert im Untermenü „Route Preferences“ der Ethernet-Profile ändern.
- statisch konfigurierte IP-Route oder Verbindungsprofil: „Preference=100“.

  Sie können den Standardwert im Verbindungs- oder IP-Routenprofil ändern.

Bei der Bestimmung, welche Routen in die Routing-Tabelle aufgenommen werden sollen, vergleicht der Router zunächst die Präferenzwerte und wählt die niedrigere Nummer. Sind die Präferenzwerte gleich, vergleicht der Router als nächstes die Werte des Parameters „Metric“ und entscheidet sich für die Route mit der niedrigeren Metrik.

Gibt es für eine bestimmte Adresse und Netzmaske mehrere Routen, ist die Route mit dem geringeren Präferenzwert vorzuziehen. Wenn zwei Routen den gleichen Präferenzwert haben, wird der Route mit dem niedrigeren „Metric“-Wert der Vorzug gegeben. Der Router verwendet letztendlich die nach diesen Kriterien vorzuziehende Route. Die anderen Routen bleiben latent bzw. „verborgen“ und kommen zum Einsatz, wenn die jeweils beste Route nicht mehr verfügbar ist.

Die folgenden Parameter wurden zur Unterstützung der Routenpräferenzen hinzugefügt:

Ort	Parameter mit Standardwert
Ethernet > Connections > *Profile* IP options (Verbindungsprofil)	Preference=[]
Ethernet > Static Rtes > *Profile* (IP-Routenprofil)	Preference=[]
Ethernet > Mod Config > Route Ref (Ethernet-Profil)	Static Preference=100 Rip Preference=100

Preference

Beschreibung: Gibt den Präferenzwert für eine bestimmte, statisch konfigurierte IP-Route an, die in einem IP-Routen- oder Verbindungsprofil festgelegt werden kann. Bei der Bestimmung, welche Routen in die Routing-Tabelle aufgenommen werden sollen, vergleicht der Router zunächst die Präferenzwerte und wählt die niedrigere Nummer. Sind die Präferenzwerte gleich, vergleicht der Router als nächstes die Werte des Parameters „Metric“ und entscheidet sich für die Route mit der niedrigeren Metrik.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie eine Zahl zwischen 0 und 255 ein. Der Standardwert ist 100. „0“ ist der Standardwert für verbundene Routen (wie z. B. das Ethernet). „255“ bedeutet “Diese Route nicht verwenden” (gilt nur für Verbindungsprofile).

Die Standardwerte für andere Routentypen lauten:

- über ICMP-Redirects erlernte Routen: 30
- von RIP erlernte Routen: 100
- statische Routen (in einem IP-Routen- oder Verbindungsprofil konfiguriert): 100

Diese Präferenzwerte verleihen statischen Routen und RIP-Routen den gleichen Wert, wobei ICMP Redirects vor beiden den Vorrang erhält.

Parameter-Ort: Verbindungsprofil: Connections > *Profil* > IP Options
IP-Routenprofil: Static Rtes > Profile

Static Preference

Beschreibung: Gibt den Präferenzwert für statisch konfigurierte Routen an, die mit IP-Adreß-Pools und dem Terminal Server-Befehl IPROUTE ADD erstellt wurden. Bei der Bestimmung, welche Routen in die Routing-Tabelle aufgenommen werden sollen, vergleicht der Router zunächst die Präferenzwerte und wählt die niedrigere Nummer. Sind die Präferenzwerte gleich, vergleicht der Router als nächstes die Werte des Parameters „Metric“ und entscheidet sich für die Route mit der niedrigeren Metrik.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie eine Zahl zwischen 0 und 255 ein. Der Standardwert ist „100“. „0“ ist der Standardwert für verbundene Routen (wie z. B. das Ethernet). „255“ bedeutet “Diese Route nicht verwenden”.

Die Standardwerte für andere Routentypen lauten:

- über ICMP-Redirects erlernte Routen: 30
- von RIP erlernte Routen: 100
- statische Routen in einem IP-Routen- oder Verbindungsprofil: 100

Parameter-Ort: Ethernet-Profil: Ethernet > Mod Config > Route Pref

Rip Preference

Beschreibung: Gibt den Präferenzwert für Routen an, die über das RIP-Protokoll erlernt wurden. Bei der Bestimmung, welche Routen in die Routing-Tabelle aufgenommen werden sollen, vergleicht der Router zunächst die Präferenzwerte und wählt die niedrigere Nummer. Sind die Präferenzwerte gleich, vergleicht der Router als nächstes die Werte des Parameters „Metric“ und entscheidet sich für die Route mit der niedrigeren Metrik.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie eine Zahl zwischen 0 und 255 ein. Der Standardwert ist „100“. „0“ ist der Standardwert für verbundene Routen (wie z. B. das Ethernet). „255“ bedeutet “Diese Route nicht verwenden”.

Die Standardwerte für andere Routentypen lauten:

- über ICMP-Redirects erlernte Routen: 30
- statische Routen über IP-Adreß-Pools, RADIUS-Authentifizierung und den Terminal Server-Befehl IPROUTE ADD: 100
- statische Routen in einem IP-Routen- oder Verbindungsprofil: 100

Parameter-Ort: Ethernet-Profil: Ethernet > Mod Config > Route Pref

Änderungen an der Anzeige der Routing-Tabelle

Der Terminal-Server-Befehl „IPROUTE SHOW“ wurde leicht geändert, um mehr Informationen, die für mehrere IP-Routing-Protokolle relevant sind, aufzunehmen. Sie können sich die IP-Routing-Tabelle anzeigen lassen, indem Sie die Terminal-Server-Schnittstelle aufrufen und an der Eingabeaufforderung den folgenden Befehl eingeben:

```
iproute show
```

Daraufhin erscheint auf dem Bildschirm eine Tabelle, die der folgenden ähnelt:

```
Destination        Gateway        IF       Flg Pref  Met   Use   Age
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
10.207.76.1/32     10.207.76.1    wanidle0 S    100   7     2     20887
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
127.0.0.1/32       -              lo0      CP   0     0     0     20887
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
10.0.0.100/32      10.0.0.100     wan0     S    100   1     153   20887
10.1.2.0/24        -              ie0      C    0     0     19775 20887
10.1.2.1/32        -              lo0      CP   0     0     389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

Diese Tabelle enthält die folgenden Routen:

- `0.0.0.0/0  10.0.0.100   wan0   SG   1     1     0     20887`
  Dies ist die Standard-Route; sie weist durch das aktive Verbindungsprofil. Im IP-Routenprofil für die Standard-Route ist ein „Preference“-Wert von 1 festgelegt, so daß dieser Route gegenüber dynamisch erlernten Routen der Vorzug gegeben wird.
- `10.207.76.0/24 10.207.76.1 wanidle0 SG 100 7  0 20887`
  `10.207.76.1/32 10.207.76.1 wanidle0 S  100 7  2 20887`

  Diese Routen sind in einem Verbindungsprofil festgelegt. Beachten Sie, daß es sich um zwei Routen handelt – eine direkte Route zum Gateway und eine Route zum größeren Netzwerk.

  `10.207.77.0/24 10.207.76.1 wanidle0 SG 100 8  0  20887`
  Dies ist eine statische Route, die durch ein inaktives Gateway weist.
- `127.0.0.1/32    -       lo0      CP   0     0     0   20887`
  Dies ist eine Prüfschleifen-Route, die bewirkt, daß Pakete an diese spezielle Adresse intern bearbeitet werden. Das Flag „C“ gibt an, daß es sich um eine verbundene Route („Connected“) handelt, während mit dem Flag „P“ („Private“) angegeben wird, daß der Router diese Route nicht bekanntmacht.
- `10.0.0.0/24 10.0.0.100 wan0  SG  100  1   21387 20887`
  `10.0.0.100/32 10.0.0.100  wan0   S   100   1   153   20887`

Diese Routen werden durch ein gegenwärtig aktives Verbindungsprofil angelegt. Sie sind den oben gezeigten 10.207.76.0-Routen ähnlich, weisen aber durch eine aktive Schnittstelle.

- `10.1.2.0/24 - ie0 C 0 0 19775 20887`
  Diese Route beschreibt die Verbindung zur Ethernet-Schnittstelle. Es handelt sich bei ihr um eine direkt verbundene Route mit einem „Preference“- und einem „Metric“-Wert von jeweils 0.
- `10.1.2.1/32 - lo0 CP 0 0 389 20887`
  Dies ist eine weitere Prüfschleifen-Route, und zwar eine Host-Route mit unserer Ethernet-Adresse. Da sie eine private Route ist, wird sie nicht bekanntgemacht.
- `255.255.255.255/32 - ie0 CP 0 0 0 20887`
  Dies ist eine private Route zur Broadcast-Adresse. Diese Route wird dann verwendet, wenn der Router ein Broadcast-Paket senden will, aber sonst nicht konfiguriert ist. Ein typisches Einsatzgebiet für eine solche Route ist die Suche nach einem Server auf einem Client-Computer, der Abfragen für eine Token-Sicherheitskarte bearbeitet.

Beschreibung der Felder in der Routing-Tabelle

Die Spalten in der Routing-Tabelle zeigen die folgenden Informationen an:

- „Destination“
  Die Spalte „Destination“ gibt die Zieladresse der Route an. Um ein Paket an diese Adresse zu senden, verwendet die Pipeline diese Route. Dabei ist zu beachten, daß der Router die am meisten spezifizierte Route (die Route mit der größten Netzmaske) verwendet, die dem angegebenen Ziel entspricht.
- „Gateway“
  In der Spalte „Gateway“ wird die Adresse des nächsten Routers angegeben, der Pakete an ein bestimmtes Ziel weiterleiten kann. Für direkte Routen (ohne Gateway) wird in der Spalte „Gateway“ kein Gateway mehr angezeigt.
- „IF“
  Die Spalte „IF“ („Interface“) zeigt den Namen der Schnittstelle an, durch die ein Paket mit dieser Adresse gesendet wird.
  - „ie0“ ist die Ethernet-Schnittstelle
  - „lo0“ ist die Prüfschleifen-Schnittstelle
  - „wanN“ gibt die Nummer der aktiven WAN-Schnittstelle an

  - „wanidle0“ ist die inaktive Schnittstelle (die spezielle Schnittstelle, auf die alle Routen gerichtet sind, wenn ihre WAN-Verbindungen „down“ sind).

- „Flg“

  Die Spalte „Flg“ („Flag“) kann die folgenden Flag-Werte enthalten:

  - C – „Connected“ (direkt verbundene Route, z. B. das Ethernet)
  - I – ICMP (dynamische ICMP-Redirect-Route)
  - N – „NetMgt“ (über SNMP-MIB II in die Tabelle aufgenommen)
  - R – RIP (dynamische RIP-Route)
  - S – „Static“ (lokal in einem IP-Routen- oder Verbindungsprofil konfigurierte Route)
  - ? – Unbekannt (Route mit unbekanntem Fehler; zeigt einen Fehler an)
  - G – „Gateway“ (diese Route kann nur über ein Gateway erreicht werden)
  - P – „Private“ (diese Route wird nicht über RIP oder OSPF bekanntgemacht)
  - T – „Temporary“ (diese Route wird vernichtet, wenn ihre Schnittstelle nicht mehr verfügbar ist)
  - * – verborgen (Wenn eine Route verborgen ist, heißt das, daß es eine bessere Route in der Tabelle gibt, so daß diese Route „hinter“ der besseren Route verborgen ist. Ist die bessere Route nicht mehr verfügbar, kann statt dessen diese Route verwendet werden.)

  Beachten Sie, daß das Flag „H“ (Host Route) entfernt wurde, da es aufgrund der /32-Netzmaske in der Zielspalte überflüssig war. Das Flag „U“ (Up) wurde ebenfalls entfernt. Physische Schnittstellen werden als „up“ betrachtet, nachdem sie im Ascend Enterprise MIB installiert wurden; daher war das Flag „U“ widersprüchlich. Das Flag „D“ (dynamic route) wurde durch die neuen Flags „I“ (ICMP Redirect) und „R“ (RIP) ersetzt.

- „Pref“

  Die Spalte „Pref“ („Preference“) enthält den Präferenzwert der Route. Alle Routen, die über RIP in die Tabelle aufgenommen werden, haben einen festen Präferenzwert von 100. Der Präferenzwert der statischen Routen kann dagegen unabhängig festgesetzt werden.

- „Metric“

  In der Spalte „Metric“ wird die in RIP-Form angegebene Metrik für die Route angezeigt, wobei der gültige Bereich von 0 bis 16 geht.

- „Use“

  In dieser Spalte wird angezeigt, wie häufig die Route seit ihrer Erstellung verwendet wurde. (Viele dieser Verwendungen sind intern, so daß sich aus dieser Zahl nicht die Anzahl der Pakete erkennen läßt, die über diese Route gesendet wurden.)

  Hinweis: Für Routen, die nicht benutzt wurden, wird in der Spalte „Use“ der Wert 0 angezeigt. Sie wurden bisher durch den Wert 1 in der Spalte „Use“ angezeigt.

- „Age“

  In dieser Spalte wird das Alter der Route in Sekunden angezeigt. Anhand dieses Wertes lassen sich Probleme erkennen, wenn Routen sich schnell ändern oder „flattern“.

Änderungen an der Routing-Tabelle und am Diagnosemodus

Am IP-Routing-Stapel der Pipeline wurden Änderungen vorgenommen, die die Leistung verbessern und zusätzliche Unterstützung für Multicast-Routing bieten. Unter anderem gibt es:

- Änderungen an Benutzerschnittstellen
- Änderungen am Diagnosemodus
- Änderungen am Betrieb von Secure Access Firewall

Außerdem entsprechen Pipelines jetzt genauer RFC1812 (Anforderungen an Router), Abschnitt 5.

Änderungen an Benutzerschnittstellen

Die Ausgabe nach Verwendung des Befehles `iproute show` wurde geändert.

Aus Netzwerk 127 wurde der Blackhole-Schnittstelle eine Route hinzugefügt:

```
127.0.0.0/8   -    bh0    CP    0   0       0      59593
```

Pakete, die an die Blackhole-Schnittstelle geleitet werden, werden ohne weiteren Hinweis vernichtet.

Routen, die auf lokale Geräte gerichtet sind, werden jetzt als „local“ markiert. Dazu gehören die folgenden Routen:

```
127.0.0.1/32   -     local    CP  0   0      0      59593
224.0.0.1/32   -     local    CP  0   0      0      59593
224.0.0.2/32   -     local    CP  0   0      0      59593
w.x.y.z/32     -     local    CP  0   0      0      59593
```

Es gibt eine w.x.y.z-Route pro lokaler IP-Adresse.

Beachten Sie, daß es sich bei den Routen zu 224.0.0.1 und 224.0.0.2 um neue Routen handelt. Sie stellen die Multicast-Adressen für alle Systeme im lokalen Subnetz bzw. alle Router auf dem lokalen Subnetz und werden nie weitergeleitet.

Einer virtuellen Schnittstelle wurde eine neue Route, „mcast“ genannt, hinzugefügt. Alle Multicast-Adressen (mit Ausnahme spezieller Adressen wie 224.0.0.1/32 und 224.0.0.2/32) sind auf die Schnittstelle „mcast“ gerichtet:

```
224.0.0.0/4    -     mcast    CP   0   0     0      59593
```

Änderungen am Diagnosemodus

Die Diagnoseausgabe des Befehls Ippacket wurde geändert.

Geänderte Diagnosemeldungen

Bei folgenden Fehlermeldungen wurde die Formulierung geändert:

IP: no ip address for this port	IP: received packet on unconfigured interface
IP: options: calling icmp_send(): type = %d code = %d	IP: options: sending icmp to %s, type = %d code = %d
IP: passed pkt length is short	IP: received frame too small to hold any IP header
IP: short IP header	IP: received packet with header size < 20 bytes
IP: version check failed	IP: received unknown IP version %d

IP: bootp packet	IP: received BOOTP packet
IP: NAT packet	IP: received NAT packet
IP: checksum failed	IP: received bad checksum
IP: no memory	IP: no memory, dropping packet

Neue Diagnosemeldungen

Die folgenden Meldungen wurden hinzugefügt:

- IP: received packet too small to hold its IP header
- IP: received truncated IP packet
- IP: received 0 ttl

Gelöschte Diagnosemeldungen

Die folgenden Meldungen wurden gelöscht:

- IP: passed pkt length is short
- IP: (pkt <MIN_ETHER_LEN) length check failed
- IP: (pkt >MAX_ETHER_LEN) length check failed
- IP: (pkt <=MAX_ETHER_LEN) length check failed
- IP: (pkt <=MAX_ETHER_LEN) is padded
- IP: short length check failed
- IP: IF wants gateway %s, but no route
- IP: route to gateway %s isn't direct
- IP: (next hop to it is %s)
- IP: no route to %s.
- IP: not forwarding
- IP: bad incoming ttl of zero!!!
- IP: ttl expired
- Bad checksum pkt at 0x%p
- IP: parse: not bcast

- IP: parse: source & dest if different
- IP: NAT Session not active
- IP: reassembly error
- IP: not joined
- IP: unused Pool address.

Änderungen am Betrieb von Secure Access Firewall

Die Art, in der Secure Access Firewall mit gerichteten Broadcasts umgeht, wurde geringfügig geändert. Ein gerichteter Broadcast, der als ein Unicast empfangen wird, wird nicht lokal ausgeliefert, falls der Firewall auf der ausgehenden Schnittstelle dieses Paket blockieren würde. Wenn der Firewall auf der ausgehenden Schnittstelle eingerichtet wurde, um dieses Paket zu blockieren, wird es nirgendwo empfangen werden, auch nicht auf der Pipeline. Bisher hätte die Pipeline das Paket an die ausgehende Schnittstelle geleitet, wo der Firewall es abgelegt hätte.

Routing auf Schnittstellenbasis

Alle Pipelines implementieren Routing auf System- oder Boxbasis. Beim Routing auf Systembasis gibt es für die gesamte Box eine IP-Adresse. Für Systeme, die eine Backbone-Verbindung haben, ist das Routing auf Systembasis vom Standpunkt der Konfiguration und der Fehlersuche bei weitem die einfachste Routing-Art. Die Alternative hierzu ist das Routing auf Schnittstellenbasis. Beim Routing auf Schnittstellenbasis verfügt jede physische oder logische Schnittstelle der Box über eine eigene IP-Adresse.

Es gibt mittlerweile jedoch einige Programme, die mit der Pipeline verwendet werden, bei denen es von Vorteil wäre, einige Schnittstellen zu numerieren, d. h. die Pipeline funktioniert teilweise als Router auf Systembasis und teilweise als Router auf Schnittstellenbasis. Mögliche Gründe, um numerierte Schnittstellen zu verwenden, sind beispielsweise die Fehlersuche auf Punkt-zu-Punkt Mietverbindungen und die Erzwingung einer Routing-Entscheidung zugunsten einer Verbindung, wenn es zwei zum selben Ziel gibt. Allgemeiner gesprochen kann die Pipeline auf Wunsch mit dem Routing auf Schnittstellenbasis eher wie ein Multi-Home-Internet-Host funktionieren.

Mit dieser Funktion kann der Benutzer eine Verbindung als numeriert (Schnittstellenbasis) oder nicht numeriert (Systembasis) konfigurieren. Wenn keine Schnittstellen als numeriert angegeben wurden, arbeitet die Einheit genau wie früher. Sie können die Schnittstellennumerierung über das Verbindungsprofil vornehmen.

Systemverhalten mit einer numerierten Schnittstelle

Falls eine Pipeline eine numerierte Schnittstelle verwendet, müssen Sie die folgenden Unterschiede beim Betrieb im Vergleich zum nicht numerierten Routing (Systembasis) beachten:

- IP-Pakete, die in der Pipeline generiert und an die entfernte Adresse gesandt wurden, verfügen über eine IP-Quelladresse, die der numerierten Schnittstelle und nicht der Standard (Ethernet)-Adresse der Pipeline entspricht.
- Während der Authentifizierung eines Rufs von einer Pipeline, die eine numerierte Schnittstelle verwendet, gibt die Pipeline die Adresse der Schnittstelle als ihre IP-Adresse durch.
- Die Pipeline fügt ihrer Routing-Tabelle alle numerierten Schnittstellen, die in den Anschlußprofilen aufgelistet sind, als Host-Routen hinzu.
- Die Pipeline wird IP-Pakete, bei deren Zieladresse es sich um eine numerierte, in einem Verbindungsprofil aufgelistete Schnittstelle handelt, annehmen, da sie sie als an die Pipeline gerichtet betrachtet. (Das Paket kann tatsächlich über eine beliebige Schnittstelle eingehen, und die numerierte Schnittstelle, die der Zieladresse des Pakets entspricht, muß nicht aktiv sein.)

Parameter „Interface IP Address“ (IF Adrs)

Die Konfigurierung einer numerierten Verbindung erfolgt im Verbindungsprofil unter dem Submenü „IP Options“. Ein neuer Parameter „IF Adrs“ gibt die IP-Adresse der Schnittstelle an. Wenn Sie den Standardwert (0.0.0.0/0) nicht ändern, wird die Schnittstelle als nicht numeriert betrachtet.

Es folgt ein Beispiel für ein typisches Profil einer nicht numerierten Schnittstelle. Das neue Feld „IF Adrs“ wird bei einer nicht numerierten Schnittstelle nicht verwendet.

```
90-103
  Ip options...
  LAN Adrs=192.168.6.29/24
  WAN Alias=0.0.0.0/0
  IF Adrs=0.0.0.0/0
  Metric=0
  reference=2
  Private=No
  IP=Off
  Pool=0
```

Im folgenden Profil sehen Sie die Einstellungen für eine numerierte Schnittstelle. Als Parameter „WAN Alias“ wurde die Adresse des entfernten Endes der Verbindung eingegeben. Der neue Parameter „IF Adrs“ zeigt die Nummer der Schnittstelle am lokalen Ende der Verbindung.

```
90-103
 Ip options...
 LAN Adrs=192.168.6.29/24
 WAN Alias=192.1.1.17
 IF Adrs=192.1.1.8/30
 Metric=0
 Preference=2
 Private=No
 RIP=Off
 Pool=0
```

IF Adrs

Beschreibung: Gibt die IP-Adresse der Schnittstelle am lokalen Ende der Verbindung an.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie dann die IP-Adresse der numerierten Schnittstelle ein.

Eine IP-Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Falls auf dem Netzwerk eine Netzmaske verwendet wird, müssen Sie dies angeben. Trennen Sie die Netzmaske von der IP-Adresse durch einen Schrägstrich. Der Standardwert ist 0.0.0.0/0.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen.

Beispiel: `200.207.23.7/24`

Abhängigkeiten: Der Parameter „IF Adrs“ ist nicht zutreffend, falls die Pipeline nicht IP („Route IP=No“) unterstützt.

Parameter-Ort: Verbindungsprofil: Ethernet > Connections > IP options

Siehe auch: WAN Alias, Route IP

Angeben der entfernten Schnittstellenadresse

Dieser Abschnitt enthält einige Richtlinien, um das Routing auf Schnittstellenbasis zu verwenden.

Falls die System- und Schnittstellenadressen bekannt sind

Falls Sie das Routing auf Schnittstellenbasis zu einem System hinzufügen, das bereits eingerichtet wurde, um das Routing auf Systembasis zu verwenden, können Sie die entfernte Schnittstellenadresse am einfachsten über den Parameter „WAN Alias“ im Verbindungsprofil angeben. „WAN Alias“ wird verwendet, um das entfernte Ende einer Verbindung zu identifizieren. Wenn Sie den Parameter „WAN Alias“ festlegen, geschieht folgendes:

- Sowohl für „Lan Adrs“ als auch für „WAN Alias“ werden Host-Routen erstellt; der Wert in „WAN Alias“ wird in der Routing-Tabelle als ein Gateway (nächster Router) zu „Lan Adrs“ aufgelistet.
- Zum Subnet des entfernten Systems wird eine Route erstellt, die „WAN Alias“ als nächsten Router anzeigt.
- Eingehende PPP/MPP-Rufe müssen ihre IP-Adresse als Wert für „WAN Alias“ (nicht als Wert für „Lan Adrs“) angeben. Das bedeutet, der Anrufer muß eine numerierte Schnittstelle verwenden, und die Schnittstellenadresse muß mit dem Wert für „WAN Alias“ auf der Empfangsseite übereinstimmen.

Falls Sie statische Routen zu Hosts am entfernten Ende erstellen wollen, können Sie die „WAN Alias“-Adresse als Feld für den “nächsten Router” (Gateway) verwenden. (Die „Lan Adrs“-Adresse wird auch funktionieren, und zwar so, als würde sie für das Routing auf Systembasis verwendet werden.)

Falls nur die Schnittstellenadresse bekannt ist

Es ist auch gestattet, die Systemadresse der Gegenstelle nicht in das Profil einzugeben und nur das Routing auf Schnittstellenbasis zu verwenden. Dieses Verfahren bietet sich an, wenn sich das entfernte System z. B. auf einem Backbone-Netzwerk befindet, das von den Verwaltern regelmäßig neu konfiguriert wird, und Sie auf das entfernte System nur mit der gemeinsam beschlossenen Schnittstellenadresse verweisen wollen.

In diesem Fall müssen Sie die Schnittstellenadresse im Parameter „Lan Adrs“ eingegeben und den Standardwert (0.0.0.0) des Parameters „WAN Alias“ unverändert beibehalten. Beachten Sie, daß für „Lan Adrs“ immer ein Eintrag vorgenommen werden muß. Wenn also nur die Schnittstellenadresse bekannt ist, müssen Sie sie als Wert für den Parameter „Lan Adrs“ und nicht für den Parameter „WAN Alias“ eingeben.

Wenn Sie die Adresse der entfernten Schnittstelle als Wert für den Parameter „Lan Adrs“ eingeben, geschieht folgendes:

- Eine Host-Route zur „Lan Adrs“ (Schnittstellen)-Adresse wird erstellt.
- Eine Netzwerk-Route zum Subnetz der entfernten Schnittstelle wird erstellt.
- Eingehende PPP/MPP-Rufe müssen ihre IP-Adresse als Wert für „Lan Adrs“ (Schnittstellen)-Adresse angeben.

Falls die Adresse der entfernten Schnittstelle nicht angegeben wurde

Falls Sie das Routing auf Schnittstellenbasis verwenden und die lokale Schnittstelle numeriert ist, ist die Adresse der Gegenstelle im allgemeinen bekannt (in der Praxis muß das Subnet von den Verwaltern beider Stellen gemeinsam beschlossen werden.) Es ist möglich, jedoch wird es nicht empfohlen, die lokale Schnittstelle zu numerieren, die Schnittstellenadresse der Gegenstelle auszulassen und nur deren System- oder LAN-Adresse zu verwenden. Verwenden Sie in diesem Falle nicht die (angeblich unbekannte) Adresse der entfernten Schnittstelle in einer statischen Route.

Wenn eine lokale Schnittstelle numeriert ist, aber keine korrespondierende Adresse einer entfernten Schnittstelle festgelegt wurde, muß die entfernte Schnittstelle über eine Adresse auf dem gleichen Subnetz wie die lokale, numerierte Schnittstelle verfügen. Ein eingehendes PPP wird zurückgewiesen, falls die lokale Schnittstelle im Verbindungsprofil numeriert ist und der (entfernte) Anrufer eine Adresse angibt, die sich nicht auf demselben Subnetz befindet.

Multicast-Weiterleitung und IGMP-Funktion

Die Pipeline unterstützt jetzt das Internet Group Membership Protocol (IGMP) Version 1 und Version 2 sowie Konfigurationsoptionen, mit denen die Pipeline Multicast-Datenverkehr weiterleiten kann. Die Pipeline kommuniziert mit einem Multicast-Router über dessen Ethernet-Schnittstelle und leitet Multicast-Datenverkehr an Multicast-Clients mit Einwählverbindungen, die über Pipelines angeschlossen sind, weiter. Die Pipeline überträgt auf transparente Weise den Multicast-Datenverkehr zwischen dem Multicast-Router und seinen Clients.

Konfigurieren der Pipeline für Multicast-Weiterleitung

Konfigurieren Sie die Pipeline folgendermaßen für die Multicast-Weiterleitung:

1. Wählen Sie Ethernet > Mod Config > Multicast.
2. Legen Sie für „Forwarding“ den Wert „Yes“ fest.
3. Geben Sie das Multicast-Profil an, mit dem der Anschluß an den Multicast-Router erfolgt.
4. Starten Sie die Pipeline erneut, um die Änderungen wirksam werden zu lassen.

Parameterangaben

Zwei neue Parameter wurden hinzugefügt, um die Multicast-Funktion zu unterstützen:

- Ethernet > Mod Config > Multicast Forwarding
- Ethernet > Mod Config > Multicast Profile

In diesem Abschnitt werden die neuen Parameter beschrieben.

Multicast Forwarding

Beschreibung: Aktiviert die Multicast-Weiterleitung in der Nur-IP-Version der Pipeline. Der Standardwert ist „No“.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen „Yes“ und „No“ umzuschalten.

- „Yes“ aktiviert die Multicast-Weiterleitung.
  Wenn Sie den Wert „Yes“ festlegen, hält ein Multicast-Router die Pipeline für einen Multicast-Client, der IGMP-Anfragen vom Router erhält und sie mit IGMP beantwortet. Ein Client mit Einwählverbindung hält sie für einen Multicast-Router, der IGMP-Anfragen aussendet und Multicast-Datenverkehr weiterleitet.
- „No“ deaktiviert die Multicast-Weiterleitung (Standard).

Parameter-Ort: Ethernet > Mod Config > Ethernet Profile

Abhängigkeiten: Verfügbar in der Nur-IP-Version für die Pipeline.

Siehe auch: Multicast-Profil

Multicast Profile

Beschreibung: Gibt den Namen eines Verbindungsprofils für eine WAN-Verbindung mit einem Multicast-Router in der Nur-IP-Version der Pipeline an. Falls Sie keinen Profilnamen angegeben haben und Multicast-Weiterleitung aktivieren, geht die Pipeline davon aus, daß ihr Ethernet die Multicast-Schnittstelle ist.

Das angegebene Verbindungsprofil muß resident sein.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie dann den Namen des Verbindungsprofils für die Multicast-Schnittstelle an. Falls Sie keinen Namen angeben, geht die Pipeline davon aus, daß es auf der Ethernet-Schnittstelle einen Multicast-Router gibt. Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen.

Parameter-Ort: Ethernet > Mod Config

Abhängigkeiten: Nur verfügbar in der Nur-IP-Version für die Pipeline. Nicht verfügbar, falls „Multicast Forwarding=No“ festgelegt wurde.

Siehe auch: Multicast Forwarding

Terminal-Server-Befehle für Multicast-Weiterleitung und IGMP

Die „Show“-Befehle, die in diesem Abschnitt beschrieben werden, wurden der Befehlszeile des Terminal-Servers hinzugefügt, um die Multicast-Funktion zu unterstützen. Wenn Sie sie verwenden wollen, müssen Sie zuerst die Terminal-Server-Schnittstelle (System > Sys Diag> Term Serv) aufrufen.

Wenn Sie alle aktiven Multicast-Gruppenadressen und die bei einer Gruppe registrierten Clients (Schnittstellen) anzeigen wollen, geben Sie folgendes ein:

```
ascend% show igmp groups
```

Daraufhin erscheint auf dem Bildschirm eine Tabelle, die der folgenden ähnelt:

```
IGMP Group address Routing Table Up Time: 0::0:22:17
 Hash      Group Address    Members    Expire time   Counts
  10       224.0.2.250
                             2           0:3:24     3211 :: 0 S5
                             1           0:3:21      145 :: 0 S5
                             0(Mbone)     ....     31901 :: 0 S5
```

Es folgt eine Erläuterung der einzelnen Spalten:

- „Hash“ ist ein Index einer Routing-Tabelle (wird nur für Diagnosezwecke angezeigt).
- „Group address“ ist die IP-Multicast-Adresse, die in diesem Paket verwendet wird.
- „Members“ gibt die Schnittstellen-ID an, an der sich die Mitgliedschaft befindet. „0“ steht für die Ethernet-Schnittstelle. Andere Zahlen stehen für WAN-Schnittstellen, die in der Reihenfolge numeriert werden, in der Sie aktiv wurden. Bei der Schnittstelle, die mit „Mbone“ gekennzeichnet wurde, handelt es sich um die Schnittstelle, auf der sich der Multicast-Router befindet.

- „Expire time“ gibt an, wann die Mitgliedschaft ausläuft. Die Pipeline sendet alle 60 Sekunden IGMP-Anfragen aus, d. h. daß die Mitgliedschaft im allgemeinen verlängert wird. Falls das Verfallsdatum erreicht wird, wird der Eintrag aus der Tabelle entfernt. Wenn dieses Feld Punkte enthält, bedeutet es, daß diese Mitgliedschaft nie ausläuft.
- „Counts“ zeigt die Anzahl Pakete an, die an den Clienten weitergeleitet wurden, die Anzahl Pakete, die aufgrund mangelnder Ressourcen vernichtet wurden, und den Status der Mitgliedschaft (der Status wird für Diagnosezwecke angezeigt).

Wenn Sie alle IGMP-Multicast-Clients anzeigen wollen, geben Sie folgendes ein:

```
ascend% show igmp clients
```

Daraufhin erscheint auf dem Bildschirm eine Tabelle, die der folgenden ähnelt:

```
IGMP Clients

 Client      Version  RecvCount  CLU      ALU
  0(Mbone)      1        0         0       0
  2             1       39        68       67
  1             1    33310        65       65
```

Es folgt eine Erläuterung der einzelnen Spalten:

- „Client“ gibt die Schnittstellen-ID an, an der sich der Client befindet. „0“ steht für die Ethernet-Schnittstelle. Andere Zahlen stehen für WAN-Schnittstellen, die in der Reihenfolge numeriert werden, in der Sie aktiv wurden. Bei der Schnittstelle, die mit „Mbone“ gekennzeichnet wurde, handelt es sich um die Schnittstelle, auf der sich der Multicast-Router befindet.
- „Version“ gibt die Version des verwendeten IGMP an.
- „RecvCount“ gibt an, wieviele IGMP-Meldungen über diese Schnittstelle empfangen wurden.
- „CLU“ (Current Line Utilization) und „ALU“ (Average Line Utilization) zeigen den Prozentsatz der Bandbreite, die auf der Schnittstelle verwendet wird, an. Wenn die Bandbreiten-Nutzung hoch ist, werden einige IGMP-Pakettypen nicht weitergeleitet.

Wenn Sie IGMP-Aktivitätsstatistiken anzeigen wollen, geben Sie folgendes ein:

```
ascend% show igmp stats
```

Die Anzahl gesandter und empfangener IGMP-Pakettypen wird im folgenden Format angezeigt:

```
46 packets received.
 0 bad checksum packets received.
 0 bad version packets received.
 0 query packets received.
46 response packets received.
 0 leave packets received.
51 packets transmitted.
47 query packets sent.
 4 response packets sent.
 0 leave packets sent.
```

IP-Adreßverwaltung

4

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie Benutzern auf dem LAN IP-Adressen zuweisen:

Network Address Translation (NAT) für ein LAN 4-2
BOOTP Relay 4-26
Erweiterte DHCP-Dienste 4-30
Erweiterte DNS-Liste 4-49
Benutzerdefinierbares Timeout für TCP-Verbindung 4-51
DNS-Server für Einwählbenutzer 4-54
Option für lokale DNS-Tabelle mit Host-Adressen 4-60

Network Address Translation (NAT) für ein LAN

Wenn ein Host eine Verbindung zum Internet oder einem anderen TCP/IP-Netzwerk herstellen soll, muß er über eine eindeutige IP-Adresse in diesem Netzwerk verfügen. Das Internet und andere große TCP/IP-Netzwerke garantieren die Eindeutigkeit von Adressen, indem offizielle IP-Adressen von zentralen Stellen zugewiesen werden. Viele lokale Netzwerke verwenden jedoch private IP-Adressen, die nur auf diesem lokalen Netzwerk eindeutig sind. Damit ein Host, der eine private Adresse hat, mit dem Internet oder einem anderen Netzwerk, das eine offizielle IP-Adresse erfordert, kommunizieren kann, ist eine Pipeline in der Lage, eine Netzwerkadressenübersetzung (Network Address Translation, NAT) durchzuführen. Das funktioniert folgendermaßen:

- Wenn der lokale Host Pakete an das entfernte Netzwerk sendet, übersetzt die Pipeline automatisch die Privatadresse des Hosts auf dem lokalen Netzwerk in eine offizielle Adresse auf dem entfernten Netzwerk.
- Wenn der lokale Host Pakete von einem entfernten Netzwerk empfängt, übersetzt die Pipeline automatisch die offizielle Adresse auf dem entfernten Netzwerk in die private Adresse des Hosts auf dem lokalen Netzwerk.

NAT kann implementiert werden, um eine oder mehrere Adressen zu verwenden. Bei der Verwendung mehrerer IP-Adressen sind eine entfernte MAX-Einheit, die als DHCP-Server konfiguriert wurde, und eine Pipeline 75 BRI Version 2 erforderlich.

NAT mit einer Adresse und Anschluß-Routing

Eine Pipeline 50, 75 oder 130 kann auf folgende Arten eine NAT mit einer Adresse durchführen:

- Für mehr als einen Host auf einem lokalen Netzwerk, ohne IP-Adressen von einem DHCP-Server auf dem entfernten Netzwerk zu leihen.
- Wenn das entfernte Netzwerk die Verbindung zur Pipeline initiiert.
- Wenn die Pipeline vom entfernten Netzwerk Pakete für bis zu 10 unterschiedliche TCP- oder UDP-Anschlüsse empfängt und sie an bestimmte Hosts und Anschlüsse auf dem lokalen Netzwerk „routet“.

Hinweis: Falls Sie über eine Pipeline 75 BRI Version 2 verfügen, können Sie die NAT mit einer Adresse verwenden, in dem Sie für den Parameter „Ethernet > NAT > Lan“ den Wert „Single IP Addr“ festlegen. Bei allen anderen Einheiten ist die NAT mit einer Adresse der Standard und der Parameter „LAN“ ist ausgeblendet.

Bei der NAT mit einer Adresse ist für das entfernte Netzwerk nur die Pipeline als einziger Host auf dem lokalen Netzwerk „sichtbar“.

- Bei ausgehenden Rufen kann die Pipeline eine NAT für mehrere Hosts auf dem lokalen Netzwerk durchführen, nachdem sie während der PPP-Verhandlungen eine IP-Adresse vom entfernten Netzwerk erhalten hat.

  Eine beliebige Anzahl von Hosts auf dem lokalen Netzwerk kann eine beliebige Anzahl gleichzeitiger Verbindungen mit Hosts auf dem entfernten Netzwerk herstellen. Die einzige Beschränkung dabei ist die Speicherbegrenzung der Pipeline. Die Übersetzungen zwischen dem lokalen Netzwerk und dem Internet oder dem entfernten Netzwerk erfolgen dynamisch und müssen im Gegensatz zu den eingehenden Verbindungen nicht im Voraus konfiguriert werden.

- Bei eingehenden Rufen kann die Pipeline eine NAT für mehrere Hosts auf dem lokalen Netzwerkmit ihrer eigenen IP-Adresse durchführen. Die Pipeline kann eingehende Pakete für bis zu 10 verschiedene TCP- oder UDP-Anschlüssen an bestimmte Server auf dem lokalen Netzwerk routen. Übersetzungen zwischen dem lokalen Netzwerk und dem Internet oder dem entfernten Netzwerk sind statisch und müssen zuvor konfiguriert werden. Sie müssen eine Liste der lokalen Server mit den jeweils zugehörigen UDP- und TCP-Anschlüssen festlegen. Sie können ebenfalls einen lokalen Standardserver festlegen, der mit den nicht aufgelisteten UDP- und TCP-Anschlüssen arbeitet.

  Sie können die Pipeline z. B. so konfigurieren, daß sie alle für TCP-Anschluß 80 (Standardanschluß für HTTP) eingehenden Pakete an den Anschluß 80 eines World Wide Web-Servers auf dem lokalen Netzwerk routet. Bei dem Anschluß, zu dem das Routing erfolgt, muß es sich nicht um denselben handeln, der in den eingehenden Paketen angegeben wurde. Sie können beispielsweise alle Pakete für TCP-Anschluß 119 (den bekannten Anschluß für Network News Transfer Protocol) an Anschluß 1119 eines Usenet News-Servers auf dem lokalen Netzwerk routen. Sie können auch einen Standard-Server angeben, der alle Pakete empfängt, die nicht an einen der gerouteten Anschlüsse gesandt wurden. Falls Sie keinen gerouteten Anschluß, aber einen Standard-Server angeben, empfängt der Standard-

Server alle Pakete, die vom entfernten Netzwerk an die Pipeline gesandt werden.

Wenn Sie die Pipeline so konfigurieren, daß sie für einen bestimmten TCP- oder UDP-Anschluß eingehende Pakete an einen bestimmten Server auf dem lokalen Netzwerk routen, können mehrere Hosts auf dem entfernten Netzwerk gleichzeitig eine Verbindung mit dem Server herstellen. Die Anzahl der Verbindungen wird nur durch die verfügbare Speicherkapazität der Pipeline begrenzt.

Hinweis: NAT schaltet RIP automatisch aus, so daß die Adresse der Pipeline nicht an das Internet oder entfernte Netzwerke weitergegeben wird.

Informationen zum NAT-Profil

Im NAT-Profil können Sie den Namen eines Verbindungsprofils angeben, für das die Pipeline eine Netzwerkadreßübersetzung an ein- und abgehenden Rufen durchführt. Hier können Sie auch andere Parameter, die von der NAT benötigt werden, eingeben.

Anschluß-Routing und Firewalls

Damit das Anschluß-Routing bei einer NAT mit einer Adresse funktioniert, müssen Sie Firewalls konfigurieren, damit die Pipeline in der Lage ist, Pakete für den gerouteten Anschluß zu empfangen.

Konfigurieren von NAT mit einer Adresse und Anschluß-Routing

Sie können eine Pipeline auf eine der folgenden Arten konfigurieren, um eine NAT für entfernte Hosts, die auf Dienste auf dem lokalen Netzwerk zugreifen wollen, durchzuführen:

- Alle von einem entfernten Netzwerk eingehenden Pakete an einen Server auf dem lokalen Netzwerk routen.
- Für bis zu 10 verschiedene TCP- oder UDP-Anschlüsse eingehende Pakete an bestimmte Server und Anschlüsse auf dem lokalen Netzwerk routen sowie, optional, verbleibende Pakete an einen Standard-Server routen.

In den folgenden Abschnitten werden die beiden Möglichkeiten schrittweise erläutert.

Routen aller eingehenden Pakete an einen Server

Wenn Sie die Pipeline so konfigurieren wollen, daß sie eine NAT durchführt und alle von einem entfernten Netzwerk eingehenden Pakete an einen Server auf dem lokalen Netzwerk routet, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Menü „Ethernet > NAT“.

2 Legen Sie für den Parameter „Routing“ den Wert „Yes“ fest.

3 Legen Sie für den Parameter „Profile“ den Namen eines vorhandenen Verbindungsprofils fest.

Die Pipeline wird eine NAT immer dann durchführen, wenn eine Verbindung mit diesem Verbindungsprofil hergestellt wird. Die Verbindung kann sowohl von der Pipeline als auch vom entfernten Netzwerk initiiert werden.

4 Falls Sie eine Pipeline 75 BRI Version 2 konfigurieren, müssen Sie für den Parameter „Lan“ den Wert „Single IP Addr“ festlegen.

5 Falls Sie die Pipeline zuvor so konfiguriert hatten, für bestimmte TCP- oder UDP-Anschlüsse eingehende Pakete zu routen (wie in „Routen für bestimmte Anschlüsse eingehender Pakete“ auf Seite 4-6 beschrieben) müssen Sie:

– jedes Menü „Ethernet > NAT > Static Mapping > Static Mapping *nn*“ öffnen (wobei *nn* eine Zahl zwischen 01 und 10 ist).

– in jedem Menü für den Parameter „Valid“ den Wert „No“ festlegen.

6 Legen Sie für den Parameter „Def Server“ die IP-Adresse des Servers auf dem lokalen Netzwerk fest, der alle vom entfernten Netzwerk eingehenden Pakete empfangen soll.

7 Betätigen Sie die ESC-Taste, um das Menü zu verlassen.

8 Speichern Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Die Änderungen werden wirksam, wenn eine Verbindung mit diesem NAT-Profil hergestellt wird. Wenn sie sofort wirksam werden sollen, müssen Sie die im Parameter „Profile“ angegebene Verbindung schließen und erneut öffnen.

Routen für bestimmte Anschlüsse eingehender Pakete

Wenn Sie für bis zu 10 verschiedene TCP- oder UDP-Anschlüsse eingehende Pakete an bestimmte Server und Anschlüsse auf dem lokalen Netzwerk routen wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Menü „Ethernet > NAT“.

2 Legen Sie für den Parameter „Routing“ den Wert „Yes“ fest.

3 Legen Sie für den Parameter „Profile“ den Namen eines vorhandenen Verbindungsprofils fest.

Die Pipeline wird eine NAT immer dann durchführen, wenn eine Verbindung mit diesem Verbindungsprofil hergestellt wird. Die Verbindung kann sowohl von der Pipeline als auch vom entfernten Netzwerk initiiert werden.

4 Falls Sie eine Pipeline 75 BRI Version 2 konfigurieren, müssen Sie für den Parameter „Lan“ den Wert „Single IP Addr“ festlegen.

5 Öffnen Sie das Menü „Ethernet > NAT > Static Mapping“.

6 Öffnen Sie ein Menü „Static Mapping *nn“*, wobei *nn* eine Zahl zwischen 01 und 10 ist.

Mit den Werten, die Sie für die Parameter in einem Menü „Static Mapping *nn*“ festlegen, geben Sie das Routing für eingehende Pakete an, die an einen bestimmten TCP- oder UDP-Anschluß gesandt werden.

7 Legen Sie für den Parameter „Valid“ den Wert „Yes“ fest.

Damit wird das Anschluß-Routing, daß mit den verbleibenden Parametern in diesem Menü festgelegt wurde, aktiviert. Wenn Sie für diesen Parameter den Wert „No“ festlegen, wird das Routing für den angegebenen Anschluß deaktiviert.

8 Legen Sie als Wert für den Parameter „Dst Port#“ die Nummer eines TCP- oder UDP-Anschlusses fest. Informationen dazu, wie Sie Anschlußnummern erfahren, finden Sie in „Bekannte Anschlüsse“ auf Seite 4-8.

Die Pipeline routet vom entfernten Netzwerk für diesen Anschluß eingehende Pakete an den lokalen Server und Anschluß, die Sie jetzt angeben.

9 Legen Sie für den Parameter „Protocol“ den Wert „TCP“ oder „UDP“ fest.

Dieser Parameter bestimmt, ob mit den Parametern „Dst Port#“ und „Local Port#“ TCP- oder UDP-Anschlüsse angegeben werden.

10 Geben Sie für den Parameter „Local Port#“ den Anschluß auf dem lokalen Server an, an den Pakete geroutet werden sollen.

11 Geben Sie für den Parameter „Local Adrs“ die Adresse des lokalen Servers an, an den Pakete geroutet werden sollen.

12 Betätigen Sie die ESC-Taste, um das Menü zu verlassen.

13 Speichern Sie die Änderungen, wenn Sie dazu aufgefordert werden.

14 Wiederholen Sie die Schritte 6 bis 13 für alle weiteren Anschlüsse, deren Pakete Sie an einen bestimmten Server und Anschluß auf dem lokalen Netzwerk routen wollen.

15 Öffnen Sie das Menü „Ethernet > NAT“.

16 Legen Sie für den Parameter „Def Server“ die IP-Adresse eines Servers auf dem lokalen Netzwerk fest, der alle verbleibenden, vom entfernten Netzwerk eingehenden Pakete empfangen soll, d. h. alle Pakete, die nicht für Anschlüsse bestimmt sind, die Sie in den Menüs „Static Mapping *nn*“ angegeben haben.

17 Betätigen Sie die ESC-Taste, um das Menü zu verlassen.

18 Speichern Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Die Änderungen werden wirksam, wenn eine Verbindung mit diesem NAT-Profil hergestellt wird. Wenn sie sofort wirksam werden sollen, müssen Sie die im Parameter „Profile“ angegebene Verbindung schließen und erneut öffnen.

Routing für bestimmte Anschlüsse deaktivieren

Wenn Sie das Routing von Paketen, die vom entfernten Netzwerk für bestimmte TCP- oder UDP-Anschlüsse deaktivieren wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Menü „Ethernet > NAT > Static Mapping“.

2 Öffnen Sie ein Menü „Static Mapping *nn*“, wobei *nn* eine Zahl zwischen 01 und 10 ist.

Die Parameter in einem Menü „Static Mapping *nn*“ legen das Routing für eingehende Pakete fest, die an einen bestimmten TCP- oder UDP-Anschluß gesandt werden.

3 Legen Sie für den Parameter „Valid“ den Wert „No“ fest.

Damit wird das Routing für den Anschluß, der in diesem Menü mit den Parametern „Dst Port# und „Protocol“ angegeben wurde, deaktiviert.

4 Betätigen Sie die ESC-Taste, um das Menü zu verlassen.

5 Speichern Sie die Änderungen, wenn Sie dazu aufgefordert werden.

6 Wiederholen Sie die Schritte 2 bis 5, um das Routing für weitere Anschlüsse zu deaktivieren.

7 Betätigen Sie die ESC-Taste, um das Menü zu verlassen.

8 Speichern Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Die Änderungen werden wirksam, wenn eine Verbindung mit diesem NAT-Profil hergestellt wird. Wenn sie sofort wirksam werden sollen, müssen Sie die im Parameter „Profile“ angegebene Verbindung schließen und erneut öffnen.

Bekannte Anschlüsse

TCP- und UDP-Anschlüsse mit den Nummern 0 - 1023 werden „Well Known Ports“ (Bekannte Anschlüsse) genannt. Diese Anschlüsse, zu denen die Anschlüsse für die am weitesten verbreiteten Services auf dem Internet gehören, werden von der Internet Assigned Numbers Authority (IANA) zugewiesen. In fast allen Fällen sind die TCP- und UDP-Anschlußnummern für einen Service gleich.

Sie können eine Aktuelle Liste der „Well Known Ports“ und „Registered Ports“ (Anschlüsse im Bereich 1024-4915, die bei der IANA registriert sind) über FTP von

`ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers`

erhalten.

NAT mit mehreren Adressen

Bei einer Pipeline 75 BRI Version 2 kann eine NAT mit mehreren Adressen durchgeführt werden, wenn für mehr als einen Host auf dem lokalen Netzwerk Adressen übersetzt werden. Zu diesem Zweck leiht die Pipeline eine offizielle IP-Adresse für einen Host von einem DHCP-Server (Dynamic Host Configuration Protocol) auf dem entfernten Netzwerk.

Die NAT mit mehrerer Adressen hat den Vorteil, daß Hosts auf dem entfernten Netzwerk eine Verbindung mit bestimmten Hosts und nicht nur mit bestimmten Services wie dem Web- oder FTP-Service auf dem lokalen Netzwerk herstellen können. Dies gilt jedoch nur, falls der DHCP-Server so konfiguriert wurde, daß er immer dieselbe Adresse zuweist, wenn ein bestimmter lokaler Host eine Adresse anfordert. Außerdem kann ein Netzwerk-Serviceanbieter eine NAT mit mehrerer Adressen für Netzwerke mit mehr als einem Host benötigen.

Wenn Sie die NAT mit mehrerer Adressen verwenden, können Hosts auf dem entfernten Netzwerk eine Verbindung mit jeder der offiziellen IP-Adressen, die die Pipeline vom DHCP-Server leiht, herstellen. Falls das lokale Netzwerk über mehr als eine IP-Adresse verfügen muß, die für das entfernte Netzwerk sichtbar sind, müssen Sie die NAT mit mehrerer Adressen verwenden. Falls Hosts auf dem entfernten Netzwerk eine Verbindung zu einem bestimmten Host auf dem lokalen Netzwerk herstellen müssen, können Sie den DHCP-Server so konfigurieren, daß er immer dieselbe Adresse zuweist, wenn ein bestimmter lokaler Host eine Adresse anfordert.

Wenn Sie die NAT mit mehrerer Adressen aktiviert haben, versucht die Pipeline, bei allen empfangenen Paketen eine IP-Adressenübersetzung durchzuführen. (Sie kann nicht zwischen offiziellen und privaten Adressen unterscheiden.)

Die Pipeline tritt für alle Hosts auf dem LAN als ein DHCP-Client auf und ist von der MAX-Einheit abhängig (die als DHCP-Server auftritt), die aus ihrem IP-Adreß-Pool für das entfernte Netzwerk geeignete Adressen liefern muß. Auf dem lokalen Netzwerk verfügen sowohl die Pipeline als auch die Hosts über “lokale” Adressen auf demselben Netzwerk, die nur für die lokale Kommunikation zwischen Hosts und der Pipeline über das Ethernet verwendet werden.

Wenn der erste Client auf dem LAN Zugang zum entfernten Netzwerk verlangt, erhält die Pipeline diese Adresse durch PPP-Verhandlungen. Wenn darauf folgende Clienten Zugang zum entfernten Netzwerk verlangen, fordert die Pipeline mit einem DHCP-Anforderungspaket eine IP-Adresse bei der MAX-Einheit an. Die MAX-Einheit sendet dann eine Adresse aus seinem IP-Adreß-Pool an die Pipeline. Die Pipeline verwendet die dynamischen Adressen, die sie von der MAX-Einheit erhält, um IP-Adressen im Namen von lokalen Clients zu übersetzten.

Wenn das LAN Pakete empfängt, bestimmt die Pipeline, ob der ursprünglichen IP-Adresse eine übersetzt Adresse zugewiesen wurde. Ist dies der Fall, wird das Paket übersetzt und aus dem WAN weitergeleitet. Falls keine Übersetzung zugewiesen wurde (und nicht ansteht), ergeht für diese IP-Adresse eine neue DHCP-Anfrage. Während darauf gewartet wird, daß die MAX-Einheit eine IP-Adresse anbietet, werden korrespondierende Quellpakete vernichtet. Wenn vom WAN gesandte Pakete eingehen, prüft die Pipeline die Zieladresse anhand ihrer Tabelle mit übersetzten Adressen. Falls die Zieladresse vorhanden und aktiv ist, leitet die Pipeline das Paket weiter. Falls die Zieladresse nicht vorhanden oder nicht aktiv ist, wird das Paket vernichtet.

IP-Adressen werden im allgemeinen von der MAX-Einheit nur für eine begrenzte Dauer angeboten, aber die Pipeline erneuert automatisch die Gültigkeit für solche Adressen. Falls die Verbindung zum entfernten Server unterbrochen wird, werden all diese Adressen als widerrufen betrachtet. Daher bestehen TCP-Verbindungen nicht über einen Anruf hinaus.

Die Pipeline selbst verfügt über keine eigene Adresse auf dem entfernte Netzwerk. Das bedeutet, daß ein Zugriff auf die Pipeline nur vom lokalen Netzwerk, aber nicht vom WAN erfolgen kann.

Bei einigen Installationen geht die MAX-Einheit sowohl mit NAT DHCP-Anforderungen als auch mit normalen DHCP-Anforderungen um. In dieser Situation, falls die normalen DHCP-Clients eine Verbindung mit der MAX-Einheit über einen Non-Bridged-Verbindung herstellen, müssen Sie über einen separaten DHCP-Server verfügen, um die normalen DHCP-Anforderungen zu behandeln; die MAX-Einheit wird nur die NAT DHCP-Anforderungen behandeln.

Konfigurieren von NAT mit mehreren Adressen

Wenn Sie eine NAT mit mehreren Adressen konfigurieren wollen, ist es erforderlich, sowohl die Pipeline als auch die MAX-Einheit, an die sie angeschlossen ist, zu konfigurieren.

Um die NAT auf der Pipeline zu konfigurieren, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Menü „Ethernet > NAT“.

2 Legen Sie für „Profile“ wie unten beschrieben den Namen des Verbindungsprofils fest, mit dem die Verbindung zum MAX (dem DHCP-Server) hergestellt wird.

3 Legen Sie „Routing=Yes“ und „Lan=Multiple“ fest.

Dadurch kommen Sie der Möglichkeit zuvor, daß eine Standard-Route vom ISP die NAT-Route überschreibt.

4 Verlassen Sie das Menü „Mod Config“, und speichern Sie Ihre Änderungen.

Hinweis: Detailliertere oder aktuellere Informationen finden Sie in der MAX-Dokumentation im Abschnitt zur Konfigurierung der MAX-Einheit als DHCP-Server.

Wo NAT konfiguriert wird:

- Falls Sie die Verbindung mit Einstellungen im Antwortprofil herstellen und den Parameter „Use Answer“ als Standard verwenden (für RADIUS), oder falls Sie Namens-/Kennwortprofile verwenden, müssen Sie die NAT im Antwortprofil konfigurieren.
- Falls Sie Verbindungsprofile für Benutzer oder falls Sie den Parameter „Template Connection #“ (für Namens-/Kennwortprofile) verwenden, müssen Sie die NAT in einem Verbindungsprofil konfigurieren.
- Falls Sie RADIUS verwenden, müssen Sie die NAT in einem RADIUS-Profil konfigurieren.

Um die NAT zu konfigurieren, gehen Sie folgendermaßen vor:

1 Wählen Sie aus dem Hauptbearbeitungsmenü:

– Ethernet > Answer > DHCP options *oder*

– Ethernet > Connections > *NAT Connection Profile* > DHCP options

2 Legen Sie „Reply Enabled=Yes“ fest.

3 Legen Sie für „Pool Number“ den IP-Adreß-Pool fest, mit dem NAT-Clients IP-Adressen zugewiesen werden. Wenn Sie „Pool Number=0“ festlegen, kann ein beliebiger Pool verwendet werden.

4 Legen Sie in „MAX Leases“ die Anzahl der Adressen fest, die der Pipeline gegeben werden sollen.

5 Falls Sie RADIUS verwenden, um Benutzer zu authentifizieren und Sie Benutzer, die DHCP anfordern, nicht authentifizieren, müssen Sie im Antwortprofil für den Parameter „Use Answer as Defaults“ den Wert „Yes“ festlegen. Anderfalls wird der MAX nicht als ein DHCP-Server für diese Clients handeln.

NAT-Menüs

Das Menü „Ethernet“ enthält das neue Untermenü „NAT“.

```
20-000 Ethernet
   20-100 Connections
   20-200 Bridge Adrs
   20-300 Static Rtes
   20-400 Filters
   20-500 Frame Relay
   20-600 Answer
   20-700 SNMP Traps
   20-800 IPX Routes
   20-900 IPX SAP Filters
   20-A00 NAT
   20-B00 Mod Config
```

Das Menü „NAT“ enthält zwei neue Parameter („Lan“ und „Def Server“), zwei Parameter, die zuvor im Menü „Configure“ zu finden waren („Routing“ und „Profile“) sowie ein neues Untermenü („Static Mapping“).

```
20-A00 NAT
   Routing=Yes
   Profile=max4
   Lan=Single IP addr
   Static Mapping...
   Def Server=181.81.8.1
```

Das Menü „Static Mappings“ enthält 10 Untermenüs „Static Mapping *nn*“, wobei *nn* ein Wert zwischen 01 und 10 ist. Jedes dieser Untermenüs enthält Parameter, mit denen das Routing von Paketen von einem entfernten Netzwerk zu einem bestimmten TCP- oder UDP-Anschluß gesteuert werden kann:

```
20-A00 NAT
      Static Mapping 01
      Static Mapping 02
      Static Mapping 03
      Static Mapping 04
      Static Mapping 05
      Static Mapping 06
      Static Mapping 07
      Static Mapping 08
```

```
Static Mapping 09
Static Mapping 10
```

Ein Menü „Static Mapping *nn*“ enthält die folgenden Parameter:

```
20-A00 NAT
   Static Mapping 01
      Valid=Yes
      Dst Port#=21
      Protocol=TCP
      Loc Port#=21
      Loc Adrs=181.100.100.102
```

NAT für Frame Relay

Die Implementierung von NAT für ein IP-Adresse wurde erweitert, um eine Verwendung mit Frame Relay zu ermöglichen. Eine Pipeline 50, 75 oder 130, die die Frame Relay-Verkapselung verwendet, kann jetzt mit einer IP-Adresse eine lokale Adressen in eine offizielle Adresse für den Netzwerkbetrieb über das WAN und den Zugang zum Internet übersetzen.

Definieren der Frame Relay-Adresse im Menü „NAT“

Wenn Sie Frame Relay verwenden, ändert sich das Menü „Ethernet > NAT“ folgendermaßen:

```
20-A00 NAT
   Routing=Yes
   Profile=max4
   FR address=
   Static Mapping...
   Def Server=181.81.8.1
```

Wenn „Routing=Yes“ ist und Sie eine gültige, offizielle IP-Adresse für „FR address“ eingeben, ist NAT für Frame Relay-Verbindungen aktiviert.

Parameterangaben

Def Server

Beschreibung: Wenn die Pipeline konfiguriert wurde, um die NAT durchzuführen, kann sie Pakete, die von einem entfernten Netzwerk für bis zu 10 verschiedene TCP- oder UDP-Anschlüsse eingehen, an bestimmte Server und Anschlüsse auf dem lokalen Netzwerk routen. Dieser Parameter legt einen lokalen Server fest, an den die Pipeline alle eingehenden Pakete routet, die *nicht* an einen bestimmten Server oder Anschluß geroutet sind.

Hinweis: Falls Sie den Wert dieses Parameters ändern, wird die Änderung erst bei der nächsten Verbindung, die mit dem im NAT-Profil angegebenen entfernten Netzwerk hergestellt wird, wirksam. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung mit dem entfernten Netzwerk unterbrechen und dann erneut herstellen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann die IP-Adresse ein.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Geben Sie „0.0.0.0“ ein, wenn Sie das Routing von Paketen an einen Standard-Server deaktivieren wollen.

Der Standardwert ist 0.0.0.0.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Damit Pakete von einem entfernten Netzwerk geroutet werden können, müssen Sie im Menü „NAT“ die Parameter „Routing=Yes“ und „Lan=Single IP Addr“ festlegen. Mit Parametern in den Menüs „Static Mapping *NN*“ (wobei *NN* eine Zahl zwischen 01 und 10 ist) steuern Sie, ob die Pipeline Pakete, die von einem entfernten Netzwerk für bis zu 10 verschiedene TCP- oder UDP-Anschlüsse eingehen, an bestimmte Server und Anschlüsse auf dem lokalen Netzwerk routen kann.
  - Für die Parameter „Dst Port#“ und „Loc Port#“ müssen Sie einen anderen Wert als „0“ festlegen.
  - Die Adresse darf nicht „0“ sein.
- Falls Ihr lokales Netzwerk nur über einen Server verfügt, der alle eingehenden Pakete verarbeitet, können Sie den Server folgendermaßen festlegen:
  - legen Sie für diesen Parameter die Adresse des Servers fest.
  - legen Sie für den Parameter „Valid“ in den Menüs „Static Mapping *nn*“ den Wert „No“ fest, wodurch das Routing von eingehenden Paketen anhand ihrer Zielanschlüsse deaktiviert wird.
- Falls im Menü „NAT“ der Parameter „Routing=No“ oder der Parameter „Lan=Multi IP Addr“ festgelegt wurde, ist dieser Parameter nicht zutreffend.

Parameter-Ort: Ethernet > NAT

Siehe auch: Dst Port#, Loc Adrs, Loc Port#, Lan, Routing, Protocol, Valid

---

Dst Port#

Beschreibung: Dieser Parameter gibt einen TCP- oder UDP-Anschluß auf der Pipeline an, an den das entfernte Netzwerk Pakete sendet. Die Pipeline kann Pakete für diesen Anschluß an einen bestimmten Server und Anschluß auf dem lokalen Netzwerk routen. Dieses Routing, das nur im Zusammenhang mit der NAT erfolgt, wird durch die Parameter im selben Menü „Static Mapping *nn*“ (wobei nn eine Zahl zwischen 01 und 10 ist) gesteuert.

Hinweis: Falls Sie den Wert dieses Parameters oder eines anderen Parameters in einem Menü „Static Mapping nn“ ändern, wird die Änderung erst bei der nächsten Verbindung, die mit dem im NAT-Profil angegebenen entfernten Netzwerk hergestellt wird, wirksam. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung mit dem entfernten Netzwerk unterbrechen und dann erneut herstellen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann die Anschlußnummer ein.

Geben Sie eine Anschlußnummer zwischen 1 und 65535 ein.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Damit eingehende Pakete für einen bestimmten Anschluß geroutet werden können, müssen Sie im Menü „NAT“ die Parameter „Routing=Yes“ und „Lan=Single IP Addr“ sowie im Menü „Static Mapping *nn*“ den Parameter „Valid=Yes“ und andere Parameter im selben Menü „Static Mapping nn“ auf andere Werte als „0“ festlegen:
  - Legen Sie für den Parameter „Loc Port#“ einen anderen Wert als „0“ fest.
  - Legen Sie für den Parameter „Loc Adrs“ eine andere Adresse als „0.0.0.0“ fest.

  Falls Sie „0“ als Wert für diesen Parameter eingeben, erscheint die Meldung „Invalid Input: Zero input is not Valid“.
- Der Parameter „Protocol“ im selben Menü „Static Mapping nn“ bestimmt, ob es sich bei dem angegebenen Anschluß um einen TCP- oder UDP-Anschluß handelt.
- Falls im Menü „NAT“ der Parameter „Routing=No“ oder der Parameter „Lan=Multi IP Addr“ festgelegt wurde, ist dieser Parameter nicht zutreffend.

Parameter-Ort: Ethernet > NAT > Static Mapping > Static Mapping *nn* (wobei nn eine Zahl zwischen 01 und 10 ist)

Siehe auch: Def Server, Loc Adrs, Loc Port#, Lan, Routing, Protocol, Valid

---

FR address

Beschreibung: Gibt die IP-Adresse an, die verwendet wird, um lokale Adressen in eine offizielle Adresse für den Netzwerkbetrieb über das WAN und den Zugang zum Internet zu übersetzen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann die offizielle IP-Adresse ein.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Sie können die Funktion nur verwenden, wenn Sie eine gültige IP-Adresse eingeben.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Im Verbindungsprofil müssen Sie „Encaps=FR“ festlegen. (Für Verbindungen, die nicht Frame Relay verwenden.)
- Im Menü „NAT“ muß der Parameter „Routing=Yes“ festgelegt werden.

Parameter-Ort: Ethernet > NAT

Siehe auch: Encaps, Routing, Profile, Static Mappings und Def Server.

Lan

Beschreibung: Nur auf Pipeline 75 BRI Version 2 verfügbar. Der Standardwert ist „Single IP Addr“.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen „Single IP Addr“ und „Multiple IP Addr“ umzuschalten. Bei „Single IP Addr“ ist für das entfernte Netzwerk als einziger Host die Pipeline sichtbar. Bei „Multiple IP Addr“ sind alle Hosts, die eine IP-Adresse von der MAX-Einheit (DHCP-Server) erhalten, für das entfernte Netzwerk sichtbar. Bei „Single IP Addr“ empfängt die Pipeline eine IP-Adresse im verlauf der PPP-Verhandlungen von abgehenden Rufen, und sie

verwendet die eigene IP-Adresse bei eingehenden Rufen. „Multiple IP Addr“ unterstützt eingehende Rufe nicht.

Abhängigkeiten: Als Wert für den Parameter „Lan“ muß „Single IP Address“ festgelegt werden, damit eine eingehende Verbindung die NAT initiiert.

Parameter-Ort: Ethernet > NAT

Loc Adrs

Beschreibung: Dieser Parameter gibt den Server an, an den Pakete geroutet werden, wenn die Pipeline konfiguriert wurde, um die NAT durchzuführen und um Pakete, die von einem entfernten Netzwerk für einen bestimmten TCP- oder UDP-Anschluß eingehen, an einen bestimmten Server oder Anschluß auf dem lokalen Netzwerk zu routen.

Hinweis: Falls Sie den Wert dieses Parameters oder eines anderen Parameters in einem Menü „Static Mapping nn“ ändern, wird die Änderung erst bei der nächsten Verbindung, die mit dem im NAT-Profil angegebenen entfernten Netzwerk hergestellt wird, wirksam. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung mit dem entfernten Netzwerk unterbrechen und dann erneut herstellen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann die IP-Adresse an.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Geben Sie „0.0.0.0“, um das Routing von Paketen zu deaktivieren.

Der Standardwert ist 0.0.0.0.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Damit eingehende Pakete für einen bestimmten Anschluß geroutet werden können, müssen Sie im Menü „NAT“ die Parameter „Routing=Yes“ und „Lan=Single IP Addr“ sowie im Menü „Static Mapping *nn*“ den Parameter „Valid=Yes“ und andere Parameter im selben Menü „Static Mapping nn“ auf andere Werte als „0“ festlegen:
  - Legen Sie für die Parameter „Dst Port#“ und „Loc Port#“ einen anderen Wert als „0“ fest.

  Falls Sie „0“ als Wert für diesen Parameter eingeben, erscheint die Meldung „Invalid Input: Zero input is not Valid“.
- Falls im Menü „NAT“ der Parameter „Routing=No“ oder der Parameter „Lan=Multi IP Addr“ festgelegt wurde, ist dieser Parameter nicht zutreffend.

Parameter-Ort: Ethernet > NAT > Static Mapping > Static Mapping *nn* (wobei nn eine Zahl zwischen 01 und 10 ist)

Siehe auch: Def Server, Dst Port#, Loc Port#, Lan, Routing, Protocol, Valid

---

Loc Port#

Beschreibung: Dieser Parameter gibt den Anschluß auf dem lokalen Server an, an den Pakete geroutet werden, wenn die Pipeline konfiguriert wurde, um die NAT durchzuführen und um Pakete, die von einem entfernten Netzwerk für einen bestimmten TCP- oder UDP-Anschluß eingehen, an einen bestimmten Server oder Anschluß auf dem lokalen Netzwerk zu routen. Bei diesem Anschluß muß es sich nicht um den gleichen Anschluß wie auf der Pipeline, an den die Pakete ursprünglich gesandt wurden, handeln.

Hinweis: Falls Sie den Wert dieses Parameters oder eines anderen Parameters in einem Menü „Static Mapping nn“ ändern, wird die Änderung erst bei der nächsten Verbindung, die mit dem im NAT-Profil angegebenen entfernten Netzwerk hergestellt wird, wirksam. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung mit dem entfernten Netzwerk unterbrechen und dann erneut herstellen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann die Anschlußnummer ein.

Geben Sie eine Anschlußnummer zwischen 1 und 65535 ein oder „0“, um das Routing von Paketen zu deaktivieren. „0“ ist der Standardwert.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Damit eingehende Pakete für einen bestimmten Anschluß geroutet werden können, müssen Sie im Menü „NAT“ die Parameter „Routing=Yes“ und „Lan=Single IP Addr“ sowie im Menü „Static Mapping *nn*“ den Parameter „Valid=Yes“ und andere Parameter im selben Menü „Static Mapping nn“ auf andere Werte als „0“ festlegen:
  - Legen Sie für den Parameter „Dst Port#“ einen anderen Wert als „0“ fest.
  - Legen Sie für den Parameter „Loc Adrs“ eine andere Adresse als „0.0.0.0“ fest.

  Falls Sie „0.0.0.0“ als Wert für diesen Parameter eingeben, erscheint die Meldung „Invalid Input: Zero input is not Valid“.
- Der Parameter „Protocol“ im selben Menü „Static Mapping *nn*“ bestimmt, ob es sich bei dem angegebenen Anschluß um einen TCP- oder UDP-Anschluß handelt.
- Falls im Menü „NAT“ der Parameter „Routing=No“ oder der Parameter „Lan=Multi IP Addr“ festgelegt wurde, ist dieser Parameter nicht zutreffend.
- Sie können den gleichen Server und Anschluß nur in einem Menü „Static Mapping *nn*“ angeben.

Parameter-Ort: Ethernet > NAT > Static Mapping > Static Mapping *nn* (wobei *nn* eine Zahl zwischen 01 und 10 ist)

Siehe auch: Def Server, Dst Port#, Loc Adrs, Lan, Routing, Protocol, Valid

Profile

Beschreibung: Dieser Parameter bezeichnet den Namen eines Verbindungsprofils, das verwendet wird, um ein entferntes Netzwerk mit der Pipeline zu verbinden. Falls die Pipeline zur Durchführung von NATs konfiguriert wurde, führt die Pipeline automatisch eine NAT durch, wenn eine Verbindung mit diesem Profil hergestellt wird. Das Profil kann für eingehende Verbindungen, ausgehende Verbindungen oder beide konfiguriert werden. Falls das Profil für eine ausgehende Verbindung verwendet wird, muß der entfernte Server so konfiguriert worden sein, daß er gültige IP-Adressen für NAT bietet, und zwar entweder über PPP-Verhandlungen für eine Adresse oder über DHCP, um mehrere Adressen, die für eine NAT auf einem LAN erforderlich sind, zu erhalten.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann den Namen eines Verbindungsprofils ein.

Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

> **Hinweis:** Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen.

- Falls im Menü „NAT“ der Parameter „Routing=No“ festgelegt wurde, ist dieser Parameter nicht zutreffend.
- Falls Sie ein Verbindungsprofil angeben, das nicht vorhanden ist, führt die Pipeline keine NAT durch.

Parameter-Ort: Ethernet > NAT

Siehe auch: Routing

Protocol

Beschreibung: Dieser Parameter gibt an, ob die Parameter „Dst Port#“ und „Loc Port#“ im selben Menü „Static Mapping nn“ (wobei nn eine Zahl zwischen 01 und 10 ist) einen TCP- oder UDP-Anschluß bezeichnen.

Hinweis: Falls Sie den Wert dieses Parameters oder eines anderen Parameters in einem Menü „Static Mapping nn“ ändern, wird die Änderung erst bei der nächsten Verbindung, die mit dem im NAT-Profil angegebenen entfernten Netzwerk hergestellt wird, wirksam. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung mit dem entfernten Netzwerk unterbrechen und dann erneut öffnen.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

- „TCP“ gibt an, daß die Parameter „Dst Port#“ und „Loc Port#“ im selben Menü „Static Mapping nn“ TCP-Anschlußnummern bezeichnen.

  „TCP“ ist der Standardwert.

- „UDP“ gibt an, daß die Parameter „Dst Port#“ und „Loc Port#“ im selben Menü „Static Mapping nn“ UDP-Anschlußnummern bezeichnen.

  Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Falls im Menü „NAT“ der Parameter „Routing=No“ oder der Parameter „Lan=Multi IP Addr“ festgelegt wurde, ist dieser Parameter nicht zutreffend.

Parameter-Ort: Ethernet > NAT > Static Mapping > Static Mapping *nn* (wobei nn eine Zahl zwischen 01 und 10 ist)

Siehe auch: Dst Port#, Loc Port#

Routing

Beschreibung: Mit diesem Parameter aktivieren oder deaktivieren Sie die NAT.

NAT kann von einem Host oder mehreren Hosts auf dem lokalen Netzwerk, die über keine offizielle IP-Adressen für ein entferntes Netzwerk verfügen, verwendet werden. Es funktioniert folgendermaßen:

- Wenn der lokale Host Pakete an das entfernte Netzwerk sendet, übersetzt die Pipeline automatisch die Privatadresse des Hosts auf dem lokalen Netzwerk in eine offizielle Adresse auf dem entfernten Netzwerk.
- Wenn der lokale Host Pakete vom entfernten Netzwerk empfängt, übersetzt die Pipeline automatisch die offizielle Adresse auf dem entfernten Netzwerk in die Privatadresse des Hosts auf dem lokalen Netzwerk.

Wenn Sie NAT konfigurieren, haben Sie die Wahl zwischen zwei Funktionsweisen:

- Die Pipeline stellt eine Verbindung zu einem entfernten Netzwerk her und erhält über eine PPP-Verhandlung eine offizielle IP-Adresse für das entfernte Netzwerk, die sie für alle Adressenübersetzungen verwendet.
- Die Pipeline stellt eine Verbindung zu einem entfernten Netzwerk her, leiht mehrere offizielle IP-Adressen von einem DHCP-Server auf dem entfernten Netzwerk und verwendet einzelne Adressen für die Übersetzung, wenn Pakete an einen bestimmten Host auf dem lokalen Netzwerk gesendet oder von einem bestimmten Host empfangen werden.

Wenn Sie NAT deaktivieren, gibt die Pipeline die vom entfernten Netzwerk geliehenen IP-Adressen frei, die Übersetzung wird beendet und die Pakete werden zwischen LAN und WAN wie üblich gesendet.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen „Yes“ und „No“ umzuschalten. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

- „Yes“ aktiviert NAT.
- „No“ deaktiviert NAT.

  Der Standardwert ist „No“.

Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Um NAT zu verwenden, muß IP-Routing auf der Pipeline aktiviert sein.
- Die IP-Adressen der Hosts auf dem lokalen Netzwerk, die NAT verwenden, und die Pipeline müssen sich auf demselben Subnetz befinden. Diese Adressen werden nur für die lokale Kommunikation zwischen dem Host und der Pipeline über das Ethernet verwendet.
- Es empfiehlt sich, IP-Adressen, die auf dem lokalen LAN verwendet werden, zu beschränken, damit bei den IP-Adressen von Hosts auf dem Netzwerk, die eine Verbindung zur Pipeline herstellen, jedes Oktett größer als 99 ist (dies trifft nur auf FTP-Sitzungen zu). Beispiel: 192.168.121.101 ist eine empfohlene Adresse, aber 192.168.121.99 nicht.
- Wenn die Pipeline eine Verbindung zu einem entfernten Netzwerk herstellt, muß die MAX-Einheit oder eine andere entfernte Einheit so konfiguriert worden sein, daß sie über PPP-Verhandlungen (wenn die Pipeline eine IP-Adresse für NAT verwendet) oder über DHCP (wenn die Pipeline mehrere IP-Adressen zur Durchführung von NAT mit einem LAN benötigt) dynamische IP-Adressen zuweist.
- Nachdem eine Verbindung beendet wurde, kann nicht garantiert werden, daß dieselbe IP-Adressen für folgende Verbindungen verwendet wird. Sie können für „Idle Timer“ den Wert „0“ eingeben (im Untermenü „Sessions options“ des Verbindungsprofils), um zu verhindern, daß die Pipeline eine ruhende Verbindung beendet. Sie müssen jedoch beachten, daß für die MAX-Einheit oder eine andere Einheit auf dem entfernten Netzwerk möglicherweise ein niedrigerer Wert für „Idle Timer“ festgelegt wurde, der alle von Ihnen festgelegten Werte übergeht.
- Nachdem Sie NAT konfiguriert haben und die Pipeline die Adressen von Clients auf dem lokalen Netzwerk übersetzt, können Sie nur über das lokale LAN oder die serielle Schnittstelle auf die Pipeline zugreifen; ein direkter Zugriff vom WAN aus ist nicht möglich.
- Beachten Sie, daß die Pipeline selbst ein NAT-Client sein kann, d. h. sie kann eine Adresse für sich selbst übersetzen, vorausgesetzt, sie übersetzt keine Adressen für andere Clients auf dem lokalen LAN.

- Achten Sie darauf, „Ignore Def Rt=Yes“ festzulegen. Wenn Sie NAT aktiviert haben, erfolgt das Routing mit der eigenen Standard-Route. Wenn Sie die Pipeline so konfigurieren, daß Standard-Routen ignoriert werden, wird dadurch verhindert, daß eine Standard-Route des ISP die NAT-Route überschreibt.

Parameter-Ort: Ethernet > NAT

Siehe auch: Def Server, Dst Port#, Loc Adrs, Loc Port#, Lan, Routing, Protocol

---

Valid

Beschreibung: Mit diesem Parameter können Sie angeben, ob Pakete, die für einen bestimmten TCP- oder UDP-Anschluß eingehen, an einen bestimmten Server und Anschluß auf dem lokalen Netzwerk geroutet werden können oder nicht. Dieses Routing, das nur im Zusammenhang mit der NAT erfolgt, wird durch die Parameter im selben Menü „Static Mapping *nn*“ (wobei nn eine Zahl zwischen 01 und 10 ist) gesteuert.

Hinweis: Falls Sie den Wert dieses Parameters oder eines anderen Parameters in einem Menü „Static Mapping nn“ ändern, wird die Änderung erst bei der nächsten Verbindung, die mit dem im NAT-Profil angegebenen entfernten Netzwerk hergestellt wird, wirksam. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung mit dem entfernten Netzwerk unterbrechen und dann erneut herstellen.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen „Yes“ und „No“ umzuschalten. Betätigen Sie die Esc-Taste um das Menü zu verlassen, und bestätigen Sie die Änderungen, wenn Sie dazu aufgefordert werden.

- Bei „Yes“ ist das Routing von eingehenden Paketen, die von den anderen Parametern im selben Menü „Static Mapping nn“ festgelegt werden, gestattet.
- Bei „No“ ist das Routing von eingehenden Paketen, die von den anderen Parametern im selben Menü „Static Mapping nn“ festgelegt werden, nicht gestattet.

  Der Standardwert ist „No“.

Hinweis: Die Änderung wird erst wirksam, wenn die nächste Verbindung hergestellt wird. Wenn die Änderung sofort wirksam werden soll, müssen Sie die Verbindung unterbrechen und wieder herstellen.

Abhängigkeiten: Damit eingehende Pakete für einen bestimmten Anschluß geroutet werden können, müssen Sie im Menü „NAT“ die Parameter „Routing=Yes“ und „Lan=Single IP Addr“ sowie für andere Parameter im selben Menü „Static Mapping nn“ andere Werte als „0“ festlegen:

- Legen Sie für die Parameter „Dst Port#“ und „Loc Port#“ einen anderen Wert als „0“ fest.
- Legen Sie für den Parameter „Loc Adrs“ eine andere Adresse als „0.0.0.0“ fest.

Parameter-Ort: Ethernet > NAT > Static Mapping > Static Mapping *nn* (wobei nn eine Zahl zwischen 01 und 10 ist)

Siehe auch: Def Server, Dst Port#, Loc Adrs, Loc Port#, Lan, Routing, Protocol

BOOTP Relay

Das Bootstrap Protocol (BOOTP) definiert, wie ein Computer auf einem TCP/IP-Netzwerk von einem anderen Computer dessen Internet Protocol (IP)-Adresse und andere Informationen erhalten kann, die er zum Starten benötigt. Der Computer, der die Startinformationen anfordert, wird BOOTP-Client genannt, und der Computer, der die Startinformationen liefert, wird BOOTP-Server genannt. Eine Anforderung für Startinformationen, die von einem BOOTP-Client an einen BOOTP-Server gesandt wird, wird BOOTP-Anforderung genannt, und die Antwort des BOOTP-Servers wird BOOTP-Antwort genannt.

Wenn sich der BOOTP-Client und der BOOTP-Server nicht auf demselben LAN befinden, dann muß die BOOTP-Anforderung von einem Netzwerk zu einem anderen übertragen werden. Diese Aufgabe, die BOOTP-Relay genannt wird, kann von einer Pipeline durchgeführt werden.

Ein Gerät, das BOOTP-Anforderungen an ein anderes Netzwerk überträgt, wird BOOTP-Relay-Agent genannt. Ein BOOTP-Relay-Agent ist verantwortlich für die Lieferung von BOOTP-Anforderungen an Server und für die Lieferung von BOOTP-Antworten an Clients. In den meisten Fällen ist der Agent ein Router, der die Netzwerke verbindet, also z. B. eine Pipeline.

Verwenden von BOOTP-Relay

Bei der Standardeinstellung einer Pipeline überträgt sie keine BOOTP-Anforderungen an andere Netzwerke. Wenn Sie die Funktion BOOTP Relay für BOOTP-Clients, die an Ihre Pipeline angeschlossen sind, aktivieren wollen, gehen Sie folgendermaßen vor:

1. Besorgen Sie sich die IP-Adresse von bis zu zwei BOOTP-Servern, die verwendet werden sollen.
2. Öffnen Sie das Menü „Ethernet > Mod Config“:

```
20-A00 Mod Config
 BOOTP Relay...
 >BOOTP Relay Enable=No
  Server=0.0.0.0
  Server=0.0.0.0
```

3. Legen Sie für den Parameter „BOOTP Relay Enable“ den Wert „Yes“ fest.
4. Wählen Sie „Server“, und betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie in dieses Textfeld die IP-Adresse des BOOTP-Server ein. Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen.
5. Falls ein weiterer BOOTP-Server verfügbar ist, wählen Sie das zweite Menüelement „Server“ und geben dessen IP-Adresse ein.

   Es ist nicht notwendig, einen zweiten BOOTP-Server anzugeben.

   Hinweis: Falls Sie zwei BOOTP-Server angeben, bestimmt die Pipeline, die die BOOTP-Anforderung überträgt, wann welcher Server verwendet wird. Die Reihenfolge, in der die BOOTP-Server im Menü „BOOTP Relay“ erscheinen, ist nicht unbedingt die Reihenfolge, in der die Server benutzt werden.

Parameterangaben

BOOTP Relay Enable

Beschreibung: Steuert, ob Bootstrap Protocol (BOOTP)-Anforderungen an ein anderes Netzwerk übertragen werden.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten.

- „Yes“ bedeutet, daß BOOTP-Anforderungen übertragen werden.
- „No“ bedeutet, daß BOOTP-Anforderungen nicht übertragen werden.

  Der Standardwert ist „No“.

Abhängigkeiten: Über den Parameter „Server“ müssen Sie die Adresse von mindestens einem BOOTP-Server angeben. Das Menü „BOOTP Relay“ enthält einen zweiten Parameter „Server“, mit dem Sie einen zweiten BOOTP-Server festlegen können. Falls Sie zwei BOOTP-Server festlegen, bestimmt die Pipeline, die die BOOTP-Anforderung überträgt, wann welcher Server verwendet wird. Die Reihenfolge, in der die BOOTP-Server im Menü „BOOTP Relay“ erscheinen, ist nicht unbedingt die Reihenfolge, in der die Server benutzt werden.

Parameter-Ort: Mod Config, BOOTP Relay

Siehe auch: Server, DHCP Spoofing

Server

Beschreibung: Gibt einen BOOTP-Server für die Verarbeitung von BOOTP-Anforderungen an. Falls sich ein Server auf demselben LAN wie die Pipeline befindet, werden BOOTP-Anforderungen von anderen Netzwerken an den Server übertragen. Falls sich ein Server auf einem anderen Netzwerk befindet, werden BOOTP-Anforderungen von Clients auf demselben LAN, auf dem sich auch die Pipeline befindet, an den entfernten Server übertragen.

Hinweis: Dieser Parameter erscheint zweimal, d. h. Sie können zwei verschiedene BOOTP-Server angeben.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann die IP-Adresse des BOOTP-Servers ein. Betätigen Sie anschließend die Eingabetaste erneut, um das Textfeld zu schließen.

Abhängigkeiten: Falls Sie zwei BOOTP-Server festlegen, bestimmt die Pipeline, die die BOOTP-Anforderung überträgt, wann welcher Server verwendet wird. Die Reihenfolge, in der die BOOTP-Server im Menü „BOOTP Relay“ erscheinen, ist nicht unbedingt die Reihenfolge, in der die Server benutzt werden.

Parameter-Ort: Mod Config, BOOTP Relay

Siehe auch: BOOTP Relay Enable

Erweiterte DHCP-Dienste

Eine Pipeline 50, 75 oder 130 kann eine Reihe von DHCP-Diensten (Dynamic Host Configuration Protocol) ausführen, wie z. B.:

- DHCP-Server-Funktionen, mit denen DHCP-Anforderungen von bis zu 43 Clients an einem beliebigen Zeitpunkt beantwortet werden können. DHCP-Server-Antworten liefern eine IP-Adresse und eine Subnetzmaske. Sie können zwei Adreß-Pools mit jeweils bis zu 20 IP-Adressen festlegen.

  Darüber hinaus können Sie für bis zu drei Hosts, die durch ihre MAC (Ethernet)-Adressen gekennzeichnet werden, eine IP-Adresse für deren ausschließliche Benutzung reservieren.
- Verwalten von Plug & Play-Anforderungen für TCP/IP-Konfigurationseinstellungen von Computern, die Microsoft Windows 95 oder Windows NT verwenden.
- DHCP Spoofing-Antworten, die eine temporäre IP-Adresse für einen Host liefern. Die bereitgestellte IP-Adresse ist immer um eins größer als die der Pipeline. Die IP-Adresse ist nur 60 Sekunden gültig - gerade lang genug, damit ein Sicherheitskartenbenutzer das aktuelle Kennwort von einem ACE- oder SAFEWORD-Server erhalten und eine authentifizierte Einwählsitzung starten kann. Nachdem die Einwählsitzung hergestellt wurde, kann eine offizielle IP-Adresse von einem entfernten DHCP- oder BOOTP-Server abgerufen werden.

  In Verbindung mit der NAT kann ein Computer dadurch eine Verbindung mit einem entfernten Netzwerk, das dynamisch IP-Adressen zuweist, herstellen.

Zuweisen von IP-Adressen

Wenn eine Pipeline als DHCP-Server konfiguriert wurde und sie eine Anforderung von einem DHCP-Client empfängt, weist sie auf eine der folgenden Arten eine IP-Adresse zu:

- Wenn Sie Plug-und-Play aktiviert haben (DHCP PNP Enabled=Yes), inkriminiert die Pipeline die eigene IP-Adresse um eins und sendet sie in der BOOTP-Antwortmeldung zusammen mit IP-Adressen für Default-Gateway und DNS-Server zurück. Plug-und-Play arbeitet mit Microsoft Windows 95 (und potentiell anderen IP-Stapeln), um einer anfragenden Einheit automatisch eine IP-Adresse und andere WAN-Einstellungen zuzuweisen. Über Plug-und-Play können Sie mit der Pipeline entfernten Netzwerken antworten, ohne zuerst eine IP-Adresse konfigurieren zu müssen.

- Falls es eine für den Host reservierte IP-Adresse gibt, weist die Pipeline die reservierte Adresse zu.
- Falls der Host die aktuell verwendete Adresse erneuert, weist die Pipeline dem Host dieselbe Adresse zu.

  Wenn ein Host von einem der Adreß-Pools eine dynamisch zugewiesene IP-Adresse erhält, wird die Gültigkeit der Adresse regelmäßig gemäß DHCP-Protokoll erneuert, bis sie nicht mehr benötigt wird. Falls der Host die Gültigkeit der Adresse verlängert, bevor sie abläuft, weist die Pipeline immer dieselbe Adresse zu.
- Falls von einem Host eine neue Anforderung eingeht und keine IP-Adresse für diesen Host reserviert ist, weist die Pipeline die nächste verfügbare Adresse aus ihren Adreß-Pools zu.

  Es stehen bis zu zwei Adreß-Pools mit je 20 aufeinanderfolgenden IP-Adressen zur Verfügung. Dabei wird die erste verfügbare Adresse im ersten Pool zugewiesen oder, falls es in diesem Pool keine verfügbaren Adressen gibt und ein zweiter Pool vorhanden ist, die erste verfügbare Adresse im zweiten Pool.

Konfigurieren von DHCP-Diensten

Wenn Sie einen DHCP-Dienst konfigurieren wollen, müssen Sie das folgende Menü öffnen:

Ethernet > Mod Config > DHCP Spoofing

Legen Sie jeden Parameter gemäß seiner Funktion wie in der folgenden Liste beschrieben fest.

Hinweis: Obwohl dieses Menü „DHCP Spoofing“ heißt, enthält es Parameter für alle DHCP-Dienste, einschließlich DHCP Spoofing, DHCP Server sowie Plug & Play.

```
20-A00 Mod Config
 DHCP Spoofing...
  DHCP Spoofing=Yes
  DHCP PNP Enabled=Yes
  Renewal Time=10
  Become Def. Router=No
  Dial If link down=No
  Always Spoof=Yes
  Validate IP=Yes
```

```
Maximum no reply wait=5
IP group 1=181.100.100.100/16
Group 1 count=1
IP group 2=0.0.0.0/0
Group 2 count=0
Host 1 IP=181.100.100.120
Host 1 Enet=0080c75Be95e
Host 2 IP=0.0.0.0/0
Host 2 Enet=000000000000
Host 3 IP=0.0.0.0/0
Host 3 Enet=000000000000
```

1 Legen Sie für den Parameter „DHCP Spoofing“ den Wert „Yes“ fest, um einen DHCP-Dienst zu aktivieren. Dieser Parameter, den es bereits in früheren Versionen der Ascend-Software gab, hat jetzt eine andere Bedeutung. Sie müssen den Wert „Yes“ festlegen, um einen DHCP-Dienst aktivieren zu können. Falls Sie den Wert „No“ festlegen, werden andere Einstellungen in diesem Menü ignoriert.

2 Legen Sie für den Parameter „DHCP PNP Enabled“ den Wert „Yes“ fest, um Plug & Play zu aktivieren. Wenn Sie die Unterstützung für Plug & Play aktivieren wollen, müssen Sie lediglich für diesen Parameter und den Parameter „DHCP Spoofing“ den Wert „Yes“ festlegen.

3 „Renewal Time“ gibt an, wie lange eine DHCP IP-Adresse gültig ist, bevor sie erneuert werden muß. Dies betrifft sowohl DHCP Spoofing-Adressen als auch DHCP-Server-Antworten. Falls der Host die Gültigkeit der Adresse verlängert, bevor sie abläuft, weist die Pipeline immer dieselbe Adresse zu. Plug & Play-Adressen verlieren immer nach 60 Sekunden ihre Gültigkeit.

4 Mit der Option „Become Default Router“ können Sie die Adresse Ihrer Pipeline als Standard-Router für alle DHCP-Anforderungspakete bekanntmachen.

5 „Dial If Link is Down“ wird mit DHCP Spoofing zusammen mit BOOTP Relay verwendet. Bisher mußte DHCP Spoofing deaktiviert werden, damit BOOTP Relay funktionieren konnte, weil beide Funktionen versuchten, auf verschiedene Arten auf dieselbe Anforderung zu antworten. Wenn jetzt beide Funktionen aktiviert und keine WAN-Verbindungen aktiv sind, führt die Pipeline DHCP Spoofing durch. Sobald die gewählte Verbindung hergestellt ist, stoppt die Pipeline das Spoofing und tritt als ein BOOTP Relay-Agent auf.

6 Legen Sie „Always Spoof“ folgendermaßen fest:

- **„Yes“ aktiviert den DHCP-Server.** Ein DHCP-Server stellt für jede Anforderung eine IP-Adresse bereit, bis alle IP-Adressen erschöpft sind.
- **„No“ aktiviert DHCP Spoofing.** DHCP Spoofing stellt nur eine IP-Adresse für einen Host auf dem Netzwerk bereit. Es reagiert nicht auf alle Anforderungen.

Falls Sie für die beiden Parameter „DHCP Spoofing“ und „Always Spoof“ den Wert „Yes“ festgelegt haben, ist die Funktion DHCP *Server* aktiviert. Falls Sie „DHCP Spoofing=Yes“ und „Always Spoof=No“ festgelegt haben, ist DHCP *Spoofing* aktiviert und funktioniert wie in früheren Versionen, wenn „Always Spoof=Yes“ festgelegt war.

7 Legen Sie für den Parameter „Validate IP“ den Wert „Yes“ fest, damit überprüft wird, ob eine Spoofing-Adresse, die zugewiesen werden soll, bereits verwendet wird, und damit, falls dies der Fall ist, automatisch eine andere Adresse zugewiesen wird.

8 Legen Sie für den Parameter „Maximum No-Reply Wait“ nur dann einen Wert fest, falls Sie IP-Adressen überprüfen. DHCP überprüft eine IP-Adresse, indem es ein ICMP-Echo (Ping) sendet, um zu prüfen, ob die Adresse benutzt wird. Mit dieser Einstellung wird festgelegt, wie lange es auf eine Antwort wartet. Der Standardwert ist 10 Sekunden.

9 Wenn IP-Adressen dynamisch zugewiesen werden sollen, müssen Sie als Wert für den Parameter „IP Group 1“ die erste Adresse im IP-Adreß-Pools festlegen.

10 Legen Sie als Wert für den Parameter „Group 1 Count“ die Anzahl der Adressen im Pool fest. Der Pool kann bis zu 20 Adressen enthalten.

11 Wenn Sie einen weiteren Adreß-Pool für dynamische Adreßzuweisungen festlegen wollen, müssen Sie als Wert für den Parameter „IP Group 2“ die erste Adresse im zweiten IP-Adreß-Pool festlegen.

12 Legen Sie als Wert für den Parameter „Group 2 Count“ die Anzahl der Adressen im Pool fest. Der zweite Pool, der ebenfalls bis zu 20 Adressen enthalten kann, wird nur verwendet, falls im ersten Pool keine Adressen verfügbar sind.

13 Wenn Sie eine IP-Adresse für einen bestimmten Host reservieren wollen, müssen als Wert für den Parameter „Host 1 IP“ die IP-Adresse für diesen Host festlegen.

14 Legen Sie für den Parameter „Host 1 Enet“ die MAC (Ethernet)-Adresse des Hosts fest. Bei der MAC-Adresse handelt es sich in der Regel um die Ethernet-Adresse der Netzwerk-Schnittstellenkarte, die der Host verwendet, um eine Verbindung mit dem LAN herzustellen. Der DHCP-Server weist diesem Host die von Ihnen angegebene IP-Adresse zu, wenn von dem Host mit der MAC-Adresse eine DHCP-Anforderung für eine IP-Adresse eingeht.

15 Wenn Sie eine IP-Adresse für einen anderen Host reservieren wollen, müssen als Wert für den Parameter „Host 2 IP“ die IP-Adresse für diesen Host festlegen.

16 Legen Sie für den Parameter „Host 2 Enet“ die MAC (Ethernet)-Adresse des Hosts fest.

17 Wenn Sie eine IP-Adresse für einen anderen Host reservieren wollen, müssen als Wert für den Parameter „Host 3 IP“ die IP-Adresse für diesen Host festlegen.

18 Legen Sie für den Parameter „Host 3 Enet“ die MAC (Ethernet)-Adresse des Hosts fest.

Einrichten eines DHCP-Servers

Wenn Sie einen DHCP-Server einrichten wollen, müssen Sie die folgenden Parameter festlegen:

```
DHCP Spoofing...
  DHCP Spoofing=
  Yes
  Always Spoof=Yes
  IP group 1=nnn.nnn.nnn.nnn/nn
  Group 1 count=n
```

Zusätzlich können sie die folgenden Parameter festlegen:

```
  Renewal Time=nn
  IP group 2=0.0.0.0/0
  Group 2 count=0
  Host 1 IP=nnn.nnn.nnn.nnn/nn
  Host 1 Enet=0080c75Be95e
  Host 2 IP=0.0.0.0/0
  Host 2 Enet=000000000000
  Host 3 IP=0.0.0.0/0
  Host 3 Enet=000000000000
```

Einrichten der Unterstützung von Plug & Play

Wenn Sie Plug & Play einrichten wollen, müssen Sie die folgenden Parameter festlegen:

```
DHCP Spoofing...
  DHCP Spoofing=Yes
  DHCP PNP Enabled=Yes
```

Einrichten von DHCP Spoofing

Wenn Sie DHCP Spoofing einrichten wollen, müssen Sie die folgenden Parameter festlegen:

```
DHCP Spoofing...
  DHCP Spoofing=Yes
  Always Spoof=No
```

Zusätzlich können sie die folgenden Parameter festlegen:

```
  Renewal Time=nn
  Become Def. Router=Yes|No
  Dial If Link Down=Yes|No
  Validate IP=Yes
  Maximum no reply wait=n
```

Parameterangaben

DHCP Spoofing

Beschreibung: Aktiviert oder deaktiviert alle DHCP-Funktionen.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten.

- „Yes“ aktiviert alle DHCP-Funktionen.
- „No“ deaktiviert alle DHCP-Funktionen.

  „Yes“ ist der Standardwert.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: Always Spoof

DHCP PNP Enabled

Beschreibung: Legt fest, ob die Pipeline automatisch eine IP-Adresse zuweist und sie zusammen den IP-Adressen von Default Gateway und Domain Name Server an das anfordernde Gerät auf einem entfernten Netzwerk zurücksendet. Der Standardwert ist „Yes“.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen „Yes“ (dem Standardwert) und „No“ umzuschalten.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: BOOTP Relay

Renewal Time

Beschreibung: Gibt an, wie lange eine dynamisch zugewiesene IP-Adresse gültig ist. Dabei handelt es sich um den Zeitraum, für den die IP-Adresse dem Host, wie im DHCP-Protokoll festgelegt, zugewiesen ist. Falls der Host die Adresse erneuert, bevor die Gültigkeitsperiode abläuft, weist der DHCP-Dienst wieder dieselbe Adresse zu.

Verwendung: Geben Sie eine Zeitdauer in Sekunden an. Der Standardwert ist 10.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Become Default Router

Beschreibung: Legt fest, ob die Pipeline sich als Standard-Router in DHCP-Antworten bekanntmachen sollte.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten.

- „Yes“ gibt an, daß es sich bei der Pipeline, die DHCP-Antworten vornimmt, um den Standard-Router handelt.
- „No“ macht die Pipeline nicht als Standard-Router bekannt. „No“ ist der Standardwert.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: BOOTP Relay Enable

Dial If Link Down

Beschreibung: Bestimmt, ob die Pipeline mit dem ersten Verbindungsprofil wählen sollte, um eine DHCP-Antwort zu senden, wenn die WAN-Verbindung unterbrochen wurde.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten.

- „Yes“ erzwingt, daß das erste Verbindungsprofil immer gewählt wird (falls die WAN-Verbindung unterbrochen wurde), wenn die Anforderung eines DHCP-Client beantwortet wird.
- „No“ überläßt es der Pipeline, eine Verbindung gemäß der bereits in der Umgebung vorhandenen Einstellungen herzustellen (z. B. die aktuellen TCP/IP-Einstellungen oder Einstellungen für eine andere Netzwerkverwaltungssoftware, die verwendet wird).
  „No“ ist der Standardwert.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: BOOTP Relay Enable

Always Spoof

Beschreibung: Bestimmt, wie die Pipeline auf DHCP-Anforderungen reagiert:

- Sie kann als DHCP-Server für bis zu 43 Hosts agieren und Adressen aus ihren eigenen Adreß-Pools zuweisen.
- Sie kann DHCP Spoofing für einen Host durchführen, indem Sie eine temporäre IP-Adresse bereitstellt, die gerade lange genug gültig ist, damit ein DHCP-Server auf dem entfernten Netzwerk eine offizielle Adresse bereitstellen kann.

Wenn eine Pipeline DHCP Spoofing durchführt, reagiert sie nur auf die DHCP-Anforderungen eines bestimmten Hosts. Anforderungen anderer Hosts werden ignoriert.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten:

- „Yes“ bedeutet, daß die Pipeline als DHCP-Server agiert.
- „No“ aktiviert DHCP Spoofing. „No“ ist der Standardwert.

Abhängigkeiten: Falls „DHCP Spoofing=No“ festgelegt wurde, ist dieser Parameter nicht zutreffend.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing

Validate IP

Beschreibung: Wenn eine Pipeline eine DHCP-Meldung erhält, mit der eine IP-Adresse angefordert wird, bestimmt dieser Parameter, daß die Pipeline prüfen soll, ob diese Adresse bereits benutzt wird. Ist dies der Fall, weist die Pipeline eine andere Adresse zu.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten:

- „Yes“ aktiviert die Prüfung der IP-Adressen.
- „No“ deaktiviert die Prüfung der IP-Adressen.
  „No“ ist der Standardwert.

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof

Maximum No Reply Wait

Beschreibung: Wenn eine Pipeline eine DHCP-Meldung verarbeitet, mit der eine IP-Adresse angefordert wird und „Validate IP=Yes“ festgelegt wurde, sendet sie eine ICMP-Echo (Ping)-Meldung, um zu überprüfen, ob diese Adresse bereits benutzt wird. Mit diesem Parameter legen Sie die maximale Dauer in Sekunden für zwei Aktionen fest, die mit dieser Überprüfung verbunden sind:

- Er gibt an, wie lange die Pipeline auf eine Antwort auf die ICMP-Echo-Meldung wartet. Falls die Pipeline keine Antwort während dieser Zeit erhält, geht sie davon aus, das sie nicht benutzt wird und reserviert die Adresse für den Host, der die Anforderung abgesandt hatte.

  Hinweis: Während die Pipeline die Adresse überprüft, ignoriert sie die ursprüngliche DHCP-Anforderung und alle weiteren Anforderungen desselben Hosts. Der Host sendet jedoch weiterhin DHCP-Anforderungen, wie im DHCP-Protokoll angegeben.

- Nachdem die Pipeline festgestellt hat, daß die Adresse verfügbar ist, weist sie dem Host die Adresse zu, falls Sie innerhalb der in diesem Parameter angegebenen Sekundenzahl eine weitere DHCP-Anforderung von diesem Host erhält. Falls die Pipeline in diesem Zeitraum keine DHCP-Anforderung erhält, beendet die Pipeline die Reservierung der Adresse.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie eine Zahl zwischen 5 und 300 ein.

10 ist der Standardwert.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls „Validate IP=No“ festgelegt wurde, überprüft die Pipeline nicht die Adressen, die sie zuweist, unabhängig davon, welchen Wert dieser Parameter hat.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Validate IP

IP Group 1

Beschreibung: Welche Bedeutung dieser Parameter hat, hängt davon ab, ob die Pipeline als DHCP-Server (wenn sowohl für „DHCP Spoofing“ als auch für „Always Spoof“ der Wert „Yes“ festgelegt wurde) oder zur Durchführung von DHCP Spoofing (wenn „DHCP Spoofing=Yes“ und „Always Spoof=No“ festgelegt wurde) konfiguriert wurde:

- Falls die Pipeline als DHCP-Server konfiguriert wurde, ist dies die Adresse und Subnetzmaske für die erste IP-Adresse in einem Adreß-Pool, der für die dynamische Adreßzuweisung verwendet wird.
- Falls die Pipeline DHCP Spoofing durchführt, gibt dieser Parameter eine Spoofing-Adresse an. Dabei handelt es sich um eine temporäre Adresse, die dem Host zur Verfügung gestellt wird, während die eigentliche IP-Adresse von einem DHCP-Server auf dem entfernten Netzwerk eingeholt wird.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie die IP-Adresse und Subnetzmaske ein.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Trennen Sie die Subnetzmaske durch einen Schrägstrich von der Adresse. Wenn Sie die erste Adresse im Pool angeben wollen, muß es sich bei der IP-Adresse um eine gültige IP-Adresse auf dem lokalen Ethernet-Netzwerk handeln. Wenn Sie die Adreßzuweisung aus diesem Pool deaktivieren wollen, müssen sie „`0.0.0.0/0`“ eingeben.

Der Standardwert ist „`192.0.2.1/24`“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

`Beispiel:` `10.2.1.1/24`

In diesem Beispiel lautet die IP-Adresse „`10.2.1.1`“. Die Zahl „24“ gibt die Bitanzahl in der Subnetzmaske an. Das Masking von 24 Bit liefert ein Subnetz von `10.2.1.0`.

Abhängigkeiten: Falls „DHCP Spoofing=No“ ist, ist dieser Parameter nicht zutreffend. Der Parameter „Group 1 Count“ gibt die Anzahl der Adressen in einem Pool an. Alle Adressen in einem Pool müssen sich auf demselben Subnetz und das Subnetz muß sich auf dem lokalen Netzwerk befinden. Falls dieser Parameter den Wert „`0.0.0.0/0`“ hat, der die Adreßzuweisung aus diesem Pool deaktiviert, müssen Sie für den Parameter „Group 1 Count“ den Wert „0“ eingeben.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Group 1 Count, IP Group 2

Group 1 Count

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, bestimmt dieser Parameter die Anzahl fortlaufender IP-Adressen im ersten Adreß-Pool.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie eine Zahl zwischen 0 und 20 ein.

Geben Sie „0“ ein, falls für den Parameter „IP Group 1“ der Wert „`0.0.0.0/0`“ festgelegt wurde (deaktiviert die Adreßzuweisung aus diesem Pool) oder falls der Parameter „IP Group 1“ eine DHCP-Spoofing-Adresse angibt.

Der Standardwert ist „1“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Der Parameter „Group 1 Count“ gibt die erste Adresse im Pool an. Alle Adressen in einem Pool müssen sich auf demselben Subnetz und das Subnetz muß sich auf dem lokalen Netzwerk befinden. Falls Sie einen Pool festlegen, darf der Wert nicht „0“ sein.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, IP Group 1

IP Group 2

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, ist dies die Adresse und Subnetzmaske für die erste IP-Adresse im zweiten Adreß-Pool, der für die dynamische Adreßzuweisung verwendet wird. Ein zweiter Pool ist optional; er ist nur erforderlich, falls Sie mehr als 20 IP-Adressen zuweisen müssen oder falls Sie maximal 20 benötigen, aber nicht genug fortlaufende Adressen verfügbar sind. Die Adressen im zweiten Pool werden nur verwendet, falls im ersten Pool keine Adressen verfügbar sind.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie die IP-Adresse und Subnetzmaske ein.

Verwendung: Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Trennen Sie die Subnetzmaske durch einen Schrägstrich von der Adresse. Wenn Sie die erste Adresse im Pool angeben wollen, muß es sich bei der IP-Adresse um eine gültige IP-Adresse auf dem lokalen Ethernet-Netzwerk handeln. Wenn Sie die Adreßzuweisung aus diesem Pool deaktivieren wollen, müssen sie „`0.0.0.0/0`“ eingeben.

Der Standardwert ist `0.0.0.0/0`.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 10.2.1.21/24

In diesem Beispiel lautet die IP-Adresse „`10.2.1.21`“. Die Zahl „24“ gibt die Bitanzahl in der Subnetzmaske an. Das Masking von 24 Bit liefert ein Subnetz von `10.2.1.0`.

Abhängigkeiten: Falls „DHCP Spoofing=No“ ist, ist dieser Parameter nicht zutreffend. Der Parameter „Group 2 Count“ gibt die Anzahl der Adressen in einem Pool an. Alle Adressen in einem Pool müssen sich auf demselben Subnetz und das Subnetz muß sich auf dem lokalen Netzwerk befinden. Falls dieser Parameter den Wert „`0.0.0.0/0`“ hat, der die Adreßzuweisung aus diesem Pool deaktiviert, müssen Sie für den Parameter „Group 2 Count“ den Wert „0“ eingeben.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, IP Group 1, Group 2 Count

Group 2 Count

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, bestimmt dieser Parameter die Anzahl fortlaufender IP-Adressen im zweiten Adreß-Pool.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie eine Zahl zwischen 0 und 20 ein.

Falls als Wert „0“ festgelegt wurde, ist der Pool nicht verfügbar.

Der Standardwert ist „0“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Der Parameter „Group 2 Count“ gibt die erste Adresse im Pool an. Alle Adressen in einem Pool müssen sich auf demselben Subnetz und das Subnetz muß sich auf dem lokalen Netzwerk befinden.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, IP Group 1

Host 1 IP

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, reserviert dieser Parameter eine IP-Adresse für den Host, dessen MAC (Ethernet)-Adresse im Parameter „Host 1 Enet“ angegeben wird. Wenn der Host mit einer DHCP-Meldung eine IP-Adresse anfordert, weist die Pipeline immer diese Adresse zu.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie die IP-Adresse und Subnetzmaske für den Host ein.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Trennen Sie die Subnetzmaske durch einen Schrägstrich von der Adresse. Wenn Sie eine Adresse zuweisen wollen, muß es sich bei der IP-Adresse um eine gültige IP-Adresse auf dem lokalen Ethernet-Netzwerk handeln. Wenn Sie die Adreßzuweisung deaktivieren wollen, müssen sie „`0.0.0.0/0`“ eingeben.

Der Standardwert ist `0.0.0.0/0`.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 10.2.1.41/24

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls Sie für diesen Parameter einen anderen Wert als „`0.0.0.0/0`“ festlegen, müssen Sie eine gültige MAC-Adresse für den Parameter „Host 1 Enet“ eingeben. Wenn Sie die Adreßzuweisung deaktivieren, indem Sie für diesen Parameter „`0.0.0.0/0`“ eingeben, müssen Sie für den Parameter „Host 1 Enet“ den Wert „`000000000000`“ festlegen.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Host 1 Enet

Host 1 Enet

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, gibt dieser Parameter einen Host auf dem lokalen Netzwerk an, für den eine IP-Adresse reserviert wurde. Die reservierte Adresse wird vom Parameter „Host 1 IP“ angegeben. Wenn der Host mit einer DHCP-Meldung eine IP-Adresse anfordert, wird ihm immer diese Adresse zugewiesen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen.

Wenn Sie einen Host angeben wollen, dem eine IP-Adresse zugewiesen werden soll, müssen Sie die MAC-Adresse der Ethernet-Schnittstelle des Hosts eingeben. Wenn Sie die Adreßzuweisung deaktivieren wollen, müssen sie „`000000000000`“ eingeben.

Der Standardwert ist „`000000000000`“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 00d07b5e16e3

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls Sie für diesen Parameter einen anderen Wert als „`000000000000`“ eingeben, müssen Sie für den Parameter „Host 1 IP“ eine gültige IP-Adresse eingeben. Wenn Sie die Adreßzuweisung deaktivieren, indem Sie für diesen Parameter den Wert „`000000000000`“ eingeben, müssen Sie für den Parameter „Host 1 IP“ den Wert „`0.0.0.0/0`“ eingeben.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Host 1 IP

Host 2 IP

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, reserviert dieser Parameter eine IP-Adresse für den Host, dessen MAC (Ethernet)-Adresse im Parameter „Host 2 Enet“ angegeben wird. Wenn der Host mit einer DHCP-Meldung eine IP-Adresse anfordert, weist die Pipeline immer diese Adresse zu.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie die IP-Adresse und Subnetzmaske ein.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Trennen Sie die Subnetzmaske durch einen Schrägstrich von der Adresse. Bei der IP-Adresse muß es sich um eine gültige IP-Adresse auf dem lokalen Ethernet-Netzwerk handeln.

Der Standardwert ist „`0.0.0.0/0`“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 10.2.1.42/24

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls Sie für diesen Parameter einen anderen Wert als „`0.0.0.0/0`“ festlegen, müssen Sie eine gültige MAC-Adresse für den Parameter „Host 2 Enet“ eingeben. Wenn Sie die Adreßzuweisung deaktivieren, indem Sie für diesen Parameter „`0.0.0.0/0`“ eingeben, müssen Sie für den Parameter „Host 2 Enet“ den Wert „`000000000000`“ festlegen.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Host 2 Enet

Host 2 Enet

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, gibt dieser Parameter einen Host auf dem lokalen Netzwerk an, für den eine IP-Adresse reserviert wurde. Die reservierte Adresse wird vom Parameter „Host 2 IP“ angegeben. Wenn der Host mit einer DHCP-Meldung eine IP-Adresse anfordert, wird ihm immer diese Adresse zugewiesen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen.

Wenn Sie einen Host angeben wollen, dem eine IP-Adresse zugewiesen werden soll, müssen Sie die MAC-Adresse der Ethernet-Schnittstelle des Hosts eingeben. Wenn Sie die Adreßzuweisung deaktivieren wollen, müssen sie „`000000000000`“ eingeben.

Der Standardwert ist `000000000000`.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 00d07b5e16e4

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls Sie für diesen Parameter einen anderen Wert als „`000000000000`“ eingeben, müssen Sie für den Parameter „Host 2 IP“ eine gültige IP-Adresse eingeben. Wenn Sie die Adreßzuweisung deaktivieren, indem Sie für diesen Parameter den Wert „`000000000000`“ eingeben, müssen Sie für den Parameter „Host 2 IP“ den Wert „`0.0.0.0/0`“ eingeben.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Host 2 IP

Host 3 IP

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, reserviert dieser Parameter eine IP-Adresse für den Host, dessen MAC (Ethernet)-Adresse im Parameter „Host 3 Enet“ angegeben wird. Wenn der Host mit einer DHCP-Meldung eine IP-Adresse anfordert, weist die Pipeline immer diese Adresse zu.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie die IP-Adresse und Subnetzmaske ein.

Die Adresse besteht aus vier Zahlen zwischen 0 und 255, die durch Punkte getrennt sind. Trennen Sie die Subnetzmaske durch einen Schrägstrich von der Adresse. Bei der IP-Adresse muß es sich um eine gültige IP-Adresse auf dem lokalen Ethernet-Netzwerk handeln.

Der Standardwert ist „`0.0.0.0/0`“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 10.2.1.43/24

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls Sie für diesen Parameter einen anderen Wert als „`0.0.0.0/0`“ festlegen, müssen Sie eine gültige MAC-Adresse für den Parameter „Host 3 Enet“ eingeben. Wenn Sie die Adreßzuweisung deaktivieren, indem Sie für diesen Parameter „`0.0.0.0/0`“ eingeben, müssen Sie für den Parameter „Host 3 Enet“ den Wert „`000000000000`“ festlegen.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Host 3 Enet

Host 3 Enet

Beschreibung: Falls die Pipeline als DHCP-Server konfiguriert wurde, gibt dieser Parameter einen Host auf dem lokalen Netzwerk an, für den eine IP-Adresse reserviert wurde. Die reservierte Adresse wird vom Parameter „Host 3 IP“ angegeben. Wenn der Host mit einer DHCP-Meldung eine IP-Adresse anfordert, wird ihm immer diese Adresse zugewiesen.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen.

Wenn Sie einen Host angeben wollen, dem eine IP-Adresse zugewiesen werden soll, müssen Sie die MAC-Adresse der Ethernet-Schnittstelle des Hosts eingeben. Wenn Sie die Adreßzuweisung deaktivieren wollen, müssen sie „`000000000000`“ eingeben.

Der Standardwert ist „`000000000000`“.

Betätigen Sie die Eingabetaste, um das Textfeld zu schließen.

Beispiel: 00d07b5e16e5

Abhängigkeiten: Falls nicht für beide Parameter „DHCP Spoofing“ und „Always Spoof“ der Wert „Yes“ festgelegt wurde, ist dieser Parameter nicht zutreffend. Falls Sie für diesen Parameter einen anderen Wert als „`000000000000`“ eingeben, müssen Sie für den Parameter „Host 3 IP“ eine gültige IP-Adresse eingeben. Wenn Sie die Adreßzuweisung deaktivieren, indem Sie für diesen Parameter den Wert „`000000000000`“ eingeben, müssen Sie für den Parameter „Host 3 IP“ den Wert „`0.0.0.0/0`“ eingeben.

Parameter-Ort: Ethernet > Mod Config > DHCP Spoofing

Siehe auch: DHCP Spoofing, Always Spoof, Host 3 IP

Erweiterte DNS-Liste

Bisher war die Anzahl der DNS-Adressen, die für Terminal-Server-Anmeldungen aufgelistet wurden, auf sechs beschränkt. Sie können jetzt bis zu 35 Adressen konfigurieren; das ist das Maximum, das von BSD unterstützt wird.

Die neuen Listen-Parameter

„List Attempt“

Falls das DNS-System so eingerichtet wurde, daß es auf eine Anforderung hin Listen mit Host-Adressen zurücksendet, kann der Benutzer eines Terminal-Servers mit dem Parameter „List Attempt“ versuchen, sich bei einem in der DNS-Liste eingetragenen Host anzumelden. Falls diese Verbindung nicht zustande kommt, kann der nächste eingetragene Host versucht werden usw. Dadurch kann vermieden werden, physische Verbindungen zu unterbrechen, wenn ein Host nicht verfügbar ist. Dies ist besonders wichtig bei Sofortdiensten wie Sofort-Telnet oder Rlogin.

„List Size“

Der neue Parameter „List Size“ gibt an, wieviele Adressen aufgelistet werden. Das Maximum ist 35. Wenn Sie diese Funktion verwenden wollen, muß die Funktion „List Attempt“, wie unten gezeigt, aktiviert worden sein:

```
20-A00 Mod Config
DNS...
>Domain Name=abc.com
 Sec Domain Name=Yes
 Allow As Client DNS
 List Attempt=Yes
 List Size=6
 Client PRI DNS=0.0.0.0
 Client Sec DNS=0.0.0.0
```

List Attempt

Beschreibung: Aktiviert oder deaktiviert die Möglichkeit, daß der Benutzer andere DNS-Hosts verwenden kann.

Verwendung: Geben Sie „Yes“ ein, um die Funktion zu aktivieren oder „No“, um sie zu deaktivieren.

Abhängigkeiten: Keine

Parameter-Ort: Ethernet > Mod Config > DNS

Siehe auch: List Size

List Size

Beschreibung: Gibt an, wieviele DNS-Adressen für den Benutzer eines Terminal-Servers verfügbar sind, wenn eine DNS-Anfrage eingeht. Das Maximum ist 35, da 35 die Obergrenze von BSD ist.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen, und geben Sie dann eine Zahl zwischen 0 und 35 ein. Der Standardwert ist „6“.

Abhängigkeiten: Dieser Parameter ist nicht zutreffend, falls „List Attempt“ deaktiviert wurde.

Parameter-Ort: Ethernet > Mod Config > DNS

Siehe auch: List Attempt

Benutzerdefinierbares Timeout für TCP-Verbindung

Sie können mit dem Parameter „TCP timeout“ die maximale Dauer festlegen, die die Pipeline auf die Herstellung einer Verbindung wartet, bevor die von einem DNS-Server über die Funktion „List Attempt“ erhaltene, nächste Adresse versucht wird. Falls die Pipeline keine Verbindung zum ersten Host auf der Liste herstellen kann, probiert sie solange den folgenden, bis eine Verbindung hergestellt wird oder ein Timeout erfolgt.

Bisher hatte das Timeout einen Wert von 170 Sekunden, der nicht vom Benutzer definiert werden konnte. Diese Frist ist länger, als einige Client-Softwareprogramme auf das Timeout warten. Wenn das Tiemout von der Client-Software erfolgte, wurde die Verbindung vernichtet und keine Adressen, die noch auf der DNS-Liste verblieben waren, wurden probiert. Bei jedem Neustart der Pipeline versuchte sie dann, dieselbe Verbindung herzustellen, die zuvor erfolglos abgebrochen wurde.

Wenn Sie diese Funktion verwenden wollen, müssen Sie für „TCP Timeout“ einen Wert zwischen 1 und 200 Sekunden festlegen, damit, falls erforderlich, versucht werden kann, eine Verbindung zu einem anderen Host herzustellen, bevor ein Timeout durch die Client-Software erfolgt. Wenn der Timeout-Wert erreicht wird, ohne daß eine Verbindung hergestellt wurde, versucht die Pipeline die nächste Adresse auf der Liste.

Einen Wert für „TCP Timeout“ wählen:

Welchen Wert Sie für den Parameter „TCP timeout“ festlegen, hängt von den Merkmalen des TCP-Ziel-Hosts ab. Beispiel: falls sich das Ziel auf einem lokalen Netzwerk unter derselben Verwaltungseinheit wie die Pipeline befindet und leicht ausgelastet ist, dann empfiehlt sich ein kurzes Timeout (einige Sekunden), denn wenn ein Host innerhalb dieses Zeitraums nicht antwortet, ist er wahrscheinlich „down“.

Eine längere Timeout-Frist empfiehlt sich, falls die Umgebung Server enthält, die folgende Merkmale aufweisen:

- längere Netzwerklatenzzeiten
- starke Auslastung auf dem Netz oder Router

- die Merkmale des entfernten Hosts sind nicht genau bekannt

Werte zwischen 30 und 60 Sekunden sind die Regel bei UNIX TCP-Implementierungen.

Der Standardwert Null gibt an, daß die Pipeline maximal 170 Sekunden wartet, um eine Verbindung mit einer Adresse auf der Liste herzustellen, bis eine Verbindung erfolgreich hergestellt wird oder bis sie vernichtet wird.

TCP timeout

Beschreibung: Gibt an, wie lange eine Pipeline versuchen wird, eine Verbindung mit einem IP-Host herzustellen, der in einer von einem DNS-Server bereitgestellten Liste enthalten ist.

Da der erste Host auf der Liste vielleicht nicht verfügbar ist, sollten Sie die Timeout-Frist kurz genug halten, damit die Pipeline zur nächsten Adresse auf der Liste gehen kann, bevor ein Timeout durch die Client-Software erfolgt.

Nachdem Sie den Parameter festgelegt haben, wird er allen von der Pipeline initiierten TCP-Verbindungen, einschließlich Telnet, Rlogin, TCP-Clear und den TCP-Teil von DNS-Abfragen, zugewiesen.

Verwendung: Wählen Sie „TCP Timeout“ und geben Sie die Wartezeit in Sekunden ein.

Der gültige Wertebereich für „TCP timeout“ ist 0 bis 200 Sekunden. Sie geben damit an, das die Pipeline nach dem Ablauf dieser Frist keine Versuche mehr unternimmt, um eine Verbindung zur aktuellen IP-Adresse herzustellen und stattdessen weitergeht zur nächsten Adresse auf der Liste.

Hinweis: Es gibt eine eingebaute Höchstzahl von Verbindungsmeldungen, die die Pipeline senden wird, um eine Verbindung mit einem entfernten Host herzustellen. Wenn die Pipeline die Höchstzahl von Meldungen gesendet hat, werden keine Versuche mehr unternommen, um eine Verbindung zu dieser Adresse herzustellen, selbst, wenn die Zeit für „TCP timeout“ noch nicht abgelaufen ist.

Der Standardwert für „TCP timeout“ ist „0“. Falls Sie diesen Wert festlegen, versucht die Pipeline eine Verbindung in zunehmend größeren Abständen herzustellen, bis sie die Höchstzahl von Verbindungsmeldungen gesendet hat. Dies dauert etwa 170 Sekunden, kann aber länger dauern, falls die Pipeline viele andere Aufgaben ausführt. Falls ein Timeout von der Client-Software vorgenommen wird, bevor die Pipeline eine Verbindung herstellt oder weitergeht zur nächsten Adresse auf der DNS-Liste, wird die physische Verbindung vernichtet.

Abhängigkeiten: Der Parameter „List Attempt“ im Untermenü „DNS“ des Menüs „Mod Config“ im Ethernet-Profil muß aktiviert sein. Damit gestatten Sie der Pipeline, mehrere IP-Adressen zu versuchen. Beachten Sie, daß der Parameter „List Attempt“ nicht zutreffend ist, falls sowohl „Telnet“ als auch „Immediate Telnet“ deaktiviert sind.

Parameter-Ort: Ethernet > Mod Config

Siehe auch: List Attempt

DNS-Server für Einwählbenutzer

Es ist jetzt möglich, IP-Adressen vom Domain Name Server (DNS) für Benutzer einzurichten, die in die Pipeline über PPP einwählen. Bisher wurden die beiden DNS-Adressen, die auf der Pipeline mit den primären (PRI) DNS-Parametern konfiguriert wurden, während der IPCP-Verhandlungen (ein Teil von PPP) an alle Einwähl-Clients ausgegeben.

Mit dieser Funktion können Sie einem Einwähl-Client über die Parameter „PRI DNS“ und „SEC DNS“ primäre und sekundäre DNS-Server-Adressen geben. Falls für den Einwählbenutzer keine DNS-Server angegeben wurden, liefert die Pipeline die IP-Adressen für die zwei DNS-Server.

DNS-Informationen werden gemäß der folgenden Regeln ausgegeben:

- Falls die Parameter „Client PRI DNS“ und „Client Sec DNS“ auf Profilebene festgelegt wurden, werden diese Parameter an den Benutzer weitergegeben.
- Falls die DNS-Informationen im Ethernet-Profil festgelegt wurden, gibt die Pipeline diese Parameter an den Benutzer weiter.
- Falls weder auf der Verbindungs- noch auf der Ethernet-Profilebene Client-DNS-Informationen festgelegt wurden und falls für den Parameter „Allow As Client DNS“ der Wert „Yes“ festgelegt wurde, überträgt die Pipeline die primären und sekundären (PRI und SEC) DNS-Informationen, die für die Pipeline festgelegt wurden. Wenn Sie verhindern wollen, daß beim Scheitern aller anderen IPCP DNS-Verhandlungen die Standard-DNS-Informationen zur Pipeline an einen Benutzer weitergegeben werden, müssen Sie „Allow As Client DNS=No“ festlegen.

Konfigurieren von DNS-Servern im Ethernet-Profil

Wenn Sie DNS-Server auf Benutzerebene im Ethernet-Profil konfigurieren wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Menü „Ethernet > Mod Config > DNS“.
Beispiel:

```
30-100 Mod Config
DNS...
Domain Name=
```

```
Pri DNS=111.111.111.11
Sec DNS=0.0.0.0
Allow as Client DNS=Yes
List attempt=Yes
List Size=6
Client Pri DNS=101.10.10.1
Client Sec DNS=101.10.10.2

Enable Local DNS Table=Yes
Loc. DNS Tab Auto Update=Ye
```

2 Legen Sie „Pri DNS“ und „Sec DNS“ als Standardwerte für die Pipeline fest.

3 Legen Sie für „Allow As Client DNS“ den Wert „Yes“ oder „No“ fest, je nachdem, ob DNS-Informationen an Benutzer weitergegeben werden sollen, falls die Client-DNS-Informationen nicht festgelegt wurden. Der Standardwert für dieses Feld ist „Yes“, um eine rückwärtsgerichtete Kompatibilität zu gestatten. Wenn Sie verhindern wollen, daß beim Scheitern aller anderen IPCP DNS-Verhandlungen die DNS-Informationen zur Pipeline an einen Benutzer weitergegeben werden, müssen Sie „Allow As Client DNS=No“ festlegen.

4 Legen Sie Werte für „List Attempt“ und „List Size“ fest.

5 Geben Sie im Feld „Client Pri DNS“ die IP-Adresse des primären DNS-Servers für dieses Profil ein.

Diese Adresse wird an einen Benutzer weitergegeben, falls im Verbindungsprofil kein DNS-Server festgelegt wurde. Falls der Wert „0.0.0.0“ eingegeben wurde, wird er als nicht festgelegt betrachtet.

6 Geben Sie im Feld „Client Sec DNS“ die IP-Adresse des sekundären DNS-Servers für alle Profile ein.

Dabei handelt es sich um die IP-Adresse des sekundären DNS-Servers, die bereitgestellt wird, falls für den Benutzer kein DNS-Server festgelegt wurde. Falls der Wert „0.0.0.0“ eingegeben wurde, wird er als nicht festgelegt betrachtet.

Konfigurieren von DNS-Servern im Verbindungsprofil

Wenn Sie DNS-Server im Verbindungsprofil konfigurieren wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Untermenü „IP“ im Verbindungsprofil.
Beispiel:

```
30-100 Connections
IP Options...
LAN Adrs=0.0.0.0/0
WAN Adrs=0.0.0.0
IP Adrs=0.0.0.0/0
Metric=7
Preference=100
Private=No
RIP=Off
Pool=0
Multicast Client=No
Multicast Rate Limit=5
Client Pri DNS=111.11.11.1
Client Sec DNS=111.11.11.2
Client Assign DNS=Yes
```

2 Geben Sie im Feld „Client Pri DNS“ die IP-Adresse des primären DNS-Servers für Einwählbenutzer für dieses Profil ein.

Diese IP-Adresse wird einem Benutzer mitgeteilt, wenn die Anmeldung über ein Profil erfolgt. Falls der Wert „0.0.0.0“ eingegeben wurde, wird er als nicht festgelegt betrachtet.

3 Geben Sie im Feld „Client Sec DNS“ die IP-Adresse des sekundären DNS-Servers für dieses Profile ein.

Dies ist die zweite IP-Adresse, die einem Benutzer mitgeteilt wird, wenn die Anmeldung über ein Profil erfolgt. Falls der Wert „0.0.0.0“ eingegeben wurde, wird er als nicht festgelegt betrachtet.

4 Legen Sie für den Parameter „Client Assign DNS“ den Wert „Yes“ oder „No“ fest.

Dieser Wert steuert, ob dem Einwählbenutzer DNS-Informationen mitgeteilt werden oder nicht. Der Standardwert ist „Yes“.

Parameterangaben

Allow as Client DNS

Beschreibung: Gibt an, ob die lokalen DNS-Server für PPP-Verhandlungen verfügbar gemacht werden sollen, falls die Client-DNS-Server nicht verfügbar sind.

Client-DNS-Konfigurationen legen DNS-Server-Adressen fest, die den WAN-Verbindungen während der IPCP-Verhandlung vorgelegt werden. Sie stellen eine Möglichkeit dar, um die lokalen DNS-Informationen vor WAN-Benutzern zu schützen. „Client DNS“ bietet zwei Stufen: eine globale Konfiguration, die allen PPP-Verbindungen zugewiesen wird, und eine verbindungsspezifische Konfiguration, die nur dieser Verbindung zugewiesen wird. Die globalen Client-Adressen werden nur verwendet, wenn im Verbindungsprofil keine angegeben wurden.

Dieser Parameter dient als Flag, die es der Pipeline gestattet, der WAN-Verbindung die lokalen DNS-Server vorzulegen, wenn alle Client-DNS-Server nicht festgelegt oder verfügbar sind.

Verwendung: Geben Sie „Yes“ oder „No“ an. Der Standardwert ist „No“.

- „Yes“ gestattet es Clients, die lokalen DNS-Server zu verwenden.
- „No“ verhindert, daß Clients die lokalen DNS-Server verwenden.

Parameter-Ort: Ethernet > Mod Config > DNS

Siehe auch: Client Assign DNS, Client Pri DNS, Client Sec DNS

Client Assign DNS

Beschreibung: Gibt an, ob Client-DNS-Server-Adressen vorgelegt werden, während über diese Verbindung verhandelt wird.

Verwendung: Geben Sie „Yes“ (die Client-DNS-Server werden verwendet) oder „No“ an. Der Standardwert ist „No“.

Beispiel: Client Assign DNS = no

Parameter-Ort: Ethernet > Connections > *Profile* > IP Options

Siehe auch: Client Pri DNS, Client Sec DNS

Client Pri DNS

Beschreibung: Gibt an, daß einem Client, der eine Verbindung mit der Pipeline herstellt, die Adresse eines primären DNS-Servers gesandt wird. „Client DNS“ bietet zwei Stufen: eine globale Konfiguration, die allen PPP-Verbindungen zugewiesen wird, und eine verbindungsspezifische Konfiguration, die nur dieser Verbindung zugewiesen wird. Die globalen Client-Adressen werden nur verwendet, wenn im Verbindungsprofil keine angegeben wurden. Sie können auch wählen, daß die lokalen DNS-Server vorgelegt werden, falls keine Client-Server festgelegt oder verfügbar sind.

Verwendung: Geben Sie die IP-Adresse eines DNS-Servers an, der bei allen Verbindungen, für die keine DNS-Server festgelegt wurde, verwendet werden soll. Der Standardwert ist „0.0.0.0“.

Beispiel: Client Pri DNS=10.9.8.7/24

Parameter-Ort: Ethernet > Mod Config > DNS; Ethernet > Connections > *Profile* > IP Options

---

Client Sec DNS

Beschreibung: Gibt an, daß einem Client, der eine Verbindung mit der Pipeline herstellt, die Adresse eines sekundären DNS-Servers gesandt wird. „Client DNS“ bietet zwei Stufen: eine globale Konfiguration, die allen PPP-Verbindungen zugewiesen wird, und eine verbindungsspezifische Konfiguration, die nur dieser Verbindung zugewiesen wird. Die globalen Client-Adressen werden nur verwendet, wenn im Verbindungsprofil keine angegeben wurden. Sie können auch wählen, daß die lokalen DNS-Server vorgelegt werden, falls keine Client-Server festgelegt oder verfügbar sind.

Verwendung: Geben Sie die IP-Adresse eines sekundären DNS-Servers an, der bei allen Verbindungen, für die keine DNS-Server festgelegt wurde, verwendet werden soll. Der Standardwert ist „0.0.0.0“.

Beispiel: Client Sec DNS=10.9.8.7/24

Parameter-Ort: Ethernet > Mod Config > DNS; Ethernet > Connections > *Profile* > IP Options

---

Sec Domain Name

Beschreibung: Gibt einen sekundären Domänennamen an, unter dem die Pipeline mit DNS suchen kann. Die Pipeline führt zunächst eine DNS-Suche in der in „Domain Name“ und dann in der in „Sec Domain Name“ festgelegten Domäne durch.

Verwendung: Geben Sie einen sekundären Domänennamen an, der bis zu 63 Zeichen lang sein kann.

Beispiel: Sec Domain Name=xyz.com

Parameter-Ort: Ethernet > Mod Config > DNS

Option für lokale DNS-Tabelle mit Host-Adressen

Sie können jetzt eine lokale DNS-Tabelle erstellen, die eine Liste mit IP-Adressen für einen bestimmten Host-Namen für den Fall enthält, daß der entfernte DNS-Server den Host-Namen nicht erfolgreich auflösen kann. Die lokale DNS-Tabelle stellt die Liste der IP-Adressen nur bereit, falls der Name des Hosts, mit dem versucht wurde, eine Verbindung herzustellen, mit dem Namen eines Hosts in der lokalen DNS-Tabelle übereinstimmt.

Wenn Sie die DNS-Tabelle erstellen, müssen Sie die Host-Namen und deren IP-Adressen über den Terminal-Server in die Tabelle eingeben. Eine Tabelle kann bis zu acht Einträge und maximal 35 IP-Adressen pro Eintrag enthalten. Sie brauchen nur die erste IP-Adresse eingeben; alle weiteren IP-Adressen werden der Liste automatisch hinzugefügt, falls Sie die automatische Aktualisierung der Liste aktiviert haben.

Sie können auch festlegen, daß die lokale DNS-Tabelle automatisch aktualisiert wird, wenn eine Verbindung mit einem Host, dessen Name mit dem eines Hosts in der lokalen DNS-Tabelle übereinstimmt, erfolgreich durch den entfernten DNS aufgelöst wird. Wenn die Tabelle aktualisiert wird, werden die für diesen Host-Namen in der lokalen DNS-Liste gespeicherten IP-Adressen durch die vom entfernten Server zurückgesandte IP-Adresse ersetzt.

Sie können die Liste der Host-Namen und der IP-Adressen in der Tabelle mit dem Terminal-Server-Befehl „Show Dnstab“ überprüfen.

Konfigurieren der lokalen DNS-Tabelle

Wenn Sie die lokale DNS-Tabelle aktivieren und konfigurieren wollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Menü „Ethernet Profile: Ethernet > Mod Config > DNS“.
2. Legen Sie „List Attempt=Yes“ fest, damit eine Liste der IP-Adressen angezeigt werden kann, wenn Sie den Terminal-Server-Befehl „Dnstab Entry“ verwenden.
3. Legen Sie über den Parameter „List Size“ fest, wieviele Einträge die Liste enthalten soll.

   Der Mindestwert ist „1“. Der Höchstwert ist „35“.

Wieviele IP-Adressen angezeigt werden, wenn Sie den Befehl „Dnstab Entry“ verwenden, hängt davon ab, welchen Wert Sie für den Parameter „List Size“ festgelegt haben.

Falls „List Attempt=Yes“ festgelegt wurde und der Server eine IP-Adreßliste zurücksendet, wird diese Liste in den Eintrag in der lokalen DNS-Tabelle kopiert, der mit dem Host-Namen übereinstimmt; diese Liste kann maximal so viele Einträge enthalten, wie in „List Size“ festgelegt wurde. Wenn eine Liste mit IP-Adressen eines Eintrags automatisch aktualisiert wird, wird eine für diesen Eintrag vorhandene Liste vernichtet.

Beispiel:

- Falls Sie „List Size=4“ festlegen und der entfernte DNS sendet drei Einträge zurück, wird die gesamte Liste mit IP-Adressen in der lokalen DNS-Tabelle mit den drei zurückgesandten Adressen überschrieben.
- Falls die lokale DNS-Tabelle bereits 35 IP-Adressen für einen Eintrag enthält und der entfernte DNS nur 4 zurücksendet, oder falls Sie „List Size=4“ festlegen, werden die ersten vier IP-Adressen für diesen Eintrag in die Tabelle eingetragen und die restlichen Adressen in der Liste werden als Null festgelegt.
- Falls Sie „List Size=1“ festlegen, kann die Liste nur eine IP-Adresse enthalten; alle weiteren, vom entfernten DNS zurückgesandten Adressen werden ignoriert. Falls Sie den Wert für den Parameter „List Size“ von einer Zahl größer Eins auf Eins ändern, wird nur die erste IP-Adresse beibehalten; alle anderen werden bei der nächsten Aktualisierung dieses Eintrags auf Null gesetzt.

4 Legen Sie „Enable Local DNS Table=Yes“ fest.

Der Standardwert ist „No“.

5 Legen Sie „Loc DNS Tab Auto Update=Yes“, um die automatische Aktualisierung zu aktivieren.

Der Standardwert ist „No“. Falls Sie die automatische Aktualisierung aktiviert haben, wird die Liste mit IP-Adressen für einen Eintrag durch eine Liste vom entfernten DNS ersetzt, wenn der entfernte DNS eine Verbindung mit einem in der Tabelle genannten Host erfolgreich auflöst.

Erstellen der lokalen DNS-Tabelle

Wenn Sie eine lokale DNS-Tabelle erstellen wollen, müssen Sie den DNS-Tabellen-Editor des Terminal-Servers verwenden. Während der Editor aktiv ist, kann die lokale DNS-Tabelle weder gelesen noch aktualisiert werden.

Hinweis: Mit diesem Verfahren legen Sie einen der acht Tabelleneinträge fest, einschließlich Host-Name, IP-Adresse (oder Adressen) und Informationsfelder.

1 Geben Sie am Terminal-Server folgendes ein:

```
dnstab edit
```

Wenn das System zum ersten Mal eingeschaltet wird, ist die Tabelle leer. Wenn der Editor zum ersten Mal eingeschaltet wird, zeigt er für jeden der acht Einträge in der Tabelle Nullen an. Wenn Sie den Tabellen-Editor ohne einen Eintrag vorzunehmen, beenden wollen, müssen Sie die Eingabetaste betätigen.

2 Geben Sie eine Eintragsnummer ein, und betätigen Sie die Eingabetaste.

Falls Sie eine ungültige Eintragsnummer eingeben, erscheint eine Warnung. Falls der Eintrag vorhanden ist, erscheint der aktuelle Name dieses Eintrags auf dem Bildschirm.

3 Geben Sie den Namen des aktuellen Eintrags ein.

Falls der Name akzeptiert wird, wird er in die Tabelle eingetragen und sie werden aufgefordert, die IP-Adresse des gerade eingegebenen Namens anzugeben.

Am Ende dieses Abschnitts finden Sie eine Liste mit Beschränkungen, die Sie bei der Benennung von Einträgen in der DNS-Tabelle befolgen müssen.

4 Führen Sie einen der folgenden Schritte durch:

Geben Sie die IP-Adresse des Eintrags ein.

Das Format der IP-Adresse wird überprüft. Falls das Format korrekt ist, wird die Adresse in die Tabelle eingetragen und der Editor fordert zu einem weiteren Eintrag auf.

5 Wenn Sie alle Einträge vorgenommen haben, geben Sie „0“ ein und betätigen die Eingabetaste, wenn der Editor zu einem weiteren Eintrag auffordert.

Bearbeiten der lokalen DNS-Tabelle

Verwenden Sie den DNS-Tabellen-Editor des Terminal-Servers, um die DNS-Tabelleneinträge zu bearbeiten. Während der Editor aktiv ist, kann die lokale DNS-Tabelle weder gelesen noch aktualisiert werden.

Hinweis: Mit diesem Verfahren legen Sie einen der acht Tabelleneinträge fest, einschließlich Host-Name, IP-Adresse (oder Adressen) und Informationsfelder.

1 Geben Sie am Terminal-Server folgendes ein:

```
dnstab edit
```

Die Nummer des zuletzt bearbeiteten Eintrags erscheint.

2 Geben Sie eine Eintragsnummer ein oder betätigen Sie die Eingabetaste, wenn Sie die aktuell angezeigte Eintragsnummer bearbeiten wollen.

Falls Sie eine ungültige Eintragsnummer eingeben, erscheint eine Warnung. Falls der Eintrag vorhanden ist, erscheint der aktuelle Name dieses Eintrags auf dem Bildschirm.

3 Führen Sie einen der folgenden Schritte durch, und betätigen Sie die Eingabetaste.

- Geben Sie den neuen Namen für den aktuellen Eintrag ein.

  Falls der Name akzeptiert wird, wird er in die Tabelle eingetragen und sie werden aufgefordert, die IP-Adresse des gerade eingegebenen Namens anzugeben.

  Am Ende dieses Abschnitts finden Sie eine Liste mit Beschränkungen, die Sie bei der Benennung von Einträgen in der DNS-Tabelle befolgen müssen.
- Betätigen Sie die Eingabetaste, um den aktuellen Namen zu bestätigen.
- Löschen Sie den Namen, indem Sie die Leertaste und dann die Eingabetaste betätigen.

  Falls Sie einen Eintragsnamen löschen und keinen neuen Namen eingeben, werden alle Informationen aus allen Feldern dieses Eintrags entfernt.

4 Führen Sie einen der folgenden Schritte durch:

- Falls Sie den Namen des Eintrags aber nicht die IP-Adresse ändern, betätigen Sie die Eingabetaste.

– Wenn Sie die IP-Adresse ändern wollen, geben Sie die neue IP-Adresse ein.

Das Format der IP-Adresse wird überprüft. Falls das Format korrekt ist, wird die Adresse in die Tabelle eingetragen und der Editor fordert zu einem weiteren Eintrag auf.

5 Wenn Sie alle Einträge vorgenommen haben, geben Sie „0“ ein und betätigen die Eingabetaste, wenn der Editor zu einem weiteren Eintrag auffordert.

Löschen eines Eintrags aus der lokalen DNS-Tabelle

Wenn Sie einen Eintrag aus der lokalen DNS-Tabelle löschen wollen, gehen Sie folgendermaßen vor:

1 Geben Sie am Terminal-Server folgendes ein, um die Tabelle anzuzeigen:

```
dnstab edit
```

2 Geben Sie die Nummer des zu löschenden Eintrags ein und betätigen Sie die Eingabetaste.

3 Betätigen Sie die Leertaste und dann die Eingabetaste.

Beschränkungen für Namen in der lokalen DNS-Tabelle

- Ein Name darf nur einmal in der Tabelle erscheinen.
- Ein Name muß mit einem Buchstaben in Groß- oder Kleinschreibung beginnen (A bis Z oder a bis z).
- Ein Name darf maximal 256 Zeichen lang sein.
- Punkte am Ende eines Namens werden ignoriert.
- Bei einem Namen kann es sich um einen lokalen Namen oder einen voll qualifizierten Namen, einschließlich des Domänennamens, handeln. Die Pipeline wird vor der Qualifizierung automatisch den lokalen Domänennamen (oder den sekundären Domänennamen, falls die Qualifizierung mit dem Domänennamen scheitert) aus dem DNS-Submenü des Ethernet-Profils hinzufügen.

Änderungen am Befehl „Show“

Es wurden zusätzliche „Show“-Befehle, die am Terminal-Server eingegeben werden können, hinzugefügt, um die DNS-Tabelle einfacher anzeigen und bearbeiten zu können:

- `show ?` zeigt eine Liste an, die die Hilfe zu `Dnstab` enthält.
- `show dnstab` zeigt die lokale DNS-Tabelle an.
- `show dnstab ?` zeigt die Hilfe zum dnstab-Editor an.

Terminal-Server-Befehl „dnstab“

Es gibt drei Variationen des Terminal-Server-Befehls `dnstab`:

dnstab-Befehl	**Beschreibung**
dnstab	Zeigt Hilfeinformationen zur DNS-Tabelle an.
dnstab show	Zeigt die lokale DNS-Tabelle an.
dnstab entry *n*	Zeigt für Eintrag *n* in der lokalen DNS-Tabelle eine Liste an. Die angezeigte Liste enthält den Eintrag und alle für diesen Eintrag gespeicherten IP-Adressen (bis zur maximalen Anzahl von Einträgen, die im Parameter „List Size“ festgelegt wurde. Falls „List Attempt=No“ festgelegt wurde, wird keine Liste angezeigt.

Enable Local DNS Table

Beschreibung: Aktiviert die Verwendung einer lokalen DNS-Tabelle, die eine Liste mit IP-Adressen für einen bestimmten Host-Namen für den Fall enthält, daß der entfernte DNS-Server den Host-Namen nicht erfolgreich auflösen kann. Die lokale DNS-Tabelle stellt die Liste der IP-Adressen nur bereit, falls der Name des Hosts, mit dem versucht wurde, eine Verbindung herzustellen, mit dem Namen eines Hosts in der lokalen DNS-Tabelle übereinstimmt.

Verwendung: Legen Sie „Enable Local DNS Table=Yes“ fest, um die lokale DNS-Tabelle zu aktivieren. „No“ deaktiviert diese Funktion.

Parameter-Ort: Ethernet > Mod Config > DNS

Loc. DNS Tab Auto Update

Beschreibung: Aktiviert oder deaktiviert die automatische Aktualisierung. Falls die automatische Aktualisierung aktiviert ist, wird die Liste mit IP-Adressen für einen Eintrag durch eine Liste vom entfernten DNS ersetzt, wenn der entfernte DNS eine Verbindung mit einem in der Tabelle genannten Host erfolgreich auflöst.

Verwendung: Legen Sie „Loc. DNS Tab Auto Update=Yes“ fest, um die automatische Aktualisierung der IP-Adressen in der lokalen DNS-Tabelle zu aktivieren. „No“ deaktiviert diese Funktion.

Abhängigkeiten: Für den Parameter „Enable Local DNS Table“ muß der Wert „Yes“ festgelegt worden sein. Wenn Sie die Liste mit IP-Adressen zu einem DNS-Tabelleneintrag anzeigen wollen, muß für den Parameter „List Attempt“ der Wert „Yes“ und für den Parameter „List Size“ ein Wert zwischen 1 und 35 festgelegt worden sein. Falls Sie „List Attempt=No“ festlegen, wird mit dem Befehl „`dnstab` show“ nur die erste IP-Adresse in einer Liste angezeigt.

Parameter-Ort: Ethernet > Mod Config > DNS

IPX-Routing

5

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie IPX-Routing auf Ihrer Einheit einrichten:

Unterstützen der Verbreitung von IPX Type 20-Paketen 5-2
Neues Maximum für Server- und Routeneinträge 5-3
Mehr standardmäßige IPX-SAP-Proxy-Server 5-4
Unterstützung für IPX ohne Festlegen eines IPX-Servers 5-4
Optimierter Zugang für anwählende NetWare-Clients 5-5
IPX-Filter 5-6
SPX-Spoofing für IPX hinzugefügt 5-8

Unterstützen der Verbreitung von IPX Type 20-Paketen

Einige Programme (wie z. B. NetBIOS) verwenden IPX Type 20-Pakete, um Namen über ein Netzwerk zu übertragen. Diese Übertragungen werden standardmäßig nicht über geroutete Verbindungen (wie von Novell empfohlen) verbreitet und werden nicht über Verbindungen weitergeleitet, deren Datendurchsatzrate unter 1 Mbit/s liegt.

Da die Pipeline Programme dieser Art nicht unterstützen kann, wurde ein Parameter hinzugefügt, mit dem die Verbreitung von IPX Type 20-Paketen ausgeschaltet werden kann. Bei Bedarf können Sie den eingestellten Wert in „Yes“ ändern.

Handle IPX Type 20

Beschreibung: Aktiviert oder deaktiviert die Verbreitung von IPX Type 20-Paketen.

Verwendung: Betätigen Sie die Eingabetaste, um „Yes“ zu wählen, mit dem die Verbreitung von IPX Type 20-Paketen gestattet wird; oder „No“, mit dem die Verbreitung von IPX Type 20-Paketen verhindert wird.

Die Pipeline unterstützt jetzt ein Flag, mit dem die Verbreitung von IPX Type 20-Paketen ein- und ausgeschaltet werden kann.

Abhängigkeiten: IPX-Routing und IPX SAP Filter müssen aktiviert sein.

Parameter-Ort: Configure > Ethernet > Mod Config > Ether options > IPX SAP Filter

Neues Maximum für Server- und Routeneinträge

In einem umfangreichen IPX-Netzwerk funktioniert die Pipeline nicht korrekt, wenn es mehr als 300 Server- und Routeneinträge gibt. Damit die Pipeline in einem großen Netzwerk, in dem IPX aktiviert ist, funktionsfähig bleibt, wurde für diese Version ein Maximum von 300 Server- und Routeneinträgen festgelegt.

In dieser Erweiterung wird das Maximum sowohl für Server- als auch für Routeneinträge überprüft. Wenn die Pipeline das Maximum von 300 erreicht, werden alle IPX-Routen und SAP-Pakete, die zusätzliche Routen und Services enthalten, vernichtet. Durch diesen Höchstwert entsteht eine unvollständige Tabelle. Sie müssen also eine Begrenzungsfunktion, wie z. B. Proxy-SAP oder IPX-Filtering, aktivieren.

Es gibt zwei Befehle, mit denen Sie anzeigen können, wie die Pipeline Grenzwerte für Server- und Routeneinträge überprüft:

```
ipxservinfo
```

```
ipxroutinfo
```

Wenn Sie den Befehl „Ipxservinfo“ auf dem Diagnosemonitor eingeben, werden folgende Informationen angezeigt:

```
ipx server table info

ipxservcnt is 20/* IPX server table count */

ipxservmax is 300/* IPX maximum server table limit */
```

Wenn Sie den Befehl „Ipxroutinfo“ auf dem Diagnosemonitor eingeben, werden folgende Informationen angezeigt:

```
ipx route table info

ipxroutcnt is 20/* IPX route table count */

ipxroutmax is 300/* IPX maximum route table limit */
```

Mehr standardmäßige IPX-SAP-Proxy-Server

Einige Netzwerke wurden entworfen, um die Verbreitung von RIP- und SAP-Paketen von einem MAX zu einer Pipeline zu verhindern. In früheren Versionen war es in der IPX-SAP-Proxy-Funktion nur möglich, auf einen IPX-SAP-Proxy-Server zu zeigen. Falls dieser Proxy-Server nicht verfügbar war, konnten entfernte Benutzer keine Verbindung mit dem Netzwerk herstellen. Es gibt jetzt drei standardmäßige IPX-SAP-Proxy-Server im Ethernet-Profil.

IPX SAP Proxy Net#n

Beschreibung: Gibt einen standardmäßigen IPX-SAP-Proxy-Server (1 bis 3) an.

Verwendung: Geben Sie bei jedem Parameter die IPX-Netzwerknummer des Servers, der den SAP-Proxy bereitstellt, an. Der Standardwert ist „0“.

Die Pipeline versucht zuerst, den unter „IPX SAP Proxy Net#1“ angegeben Server zu verwenden. Ist er nicht verfügbar, versucht die Pipeline, den unter „IPX SAP Proxy Net#2“ angegeben Server zu verwenden. Ist dieser Server auch nicht verfügbar, versucht die Pipeline, den unter „IPX SAP Proxy Net#3“ angegeben Server zu verwenden.

Abhängigkeiten: Falls „IPX SAP Proxy=No“ festgelegt wurde, ist der Parameter „IPX SAP Proxy Net#*n*“ nicht zutreffend.

Parameter-Ort: Ethernet > Mod Config > Ether Options.

Unterstützung für IPX ohne Festlegen eines IPX-Servers

Sie können jetzt eine Route zu einem Ziel-IPX-Netzwerk angeben, ohne einen IPX-Server im Untermenü „IPX Routes“ des Ethernet-Konfigurationsprofils festzulegen. Bisher trug die Pipeline „NULL“ in der SAP-Tabelle ein, falls Sie eine Route angegeben hatten, ohne auch gleichzeitig einen IPX-Server anzugebem. Dank dieser Funktion wird in der SAP-Tabelle keine Eintrag vorgenommen.

IPX-Netzwerk über die Netzwerknummer erreichen

Diese Funktion verursacht keine Änderung der Benutzerschnittstelle. Das Untermenü „IPX Routes“ ist unverändert. Sie können ein IPX-Netzwerk erreichen, indem Sie die Netzwerknummer eingeben (z. B. Network=00123456), ohne „Server Name“ und „Server Type“ anzugeben.

Optimierter Zugang für anwählende NetWare-Clients

In füheren Versionen ging die Pipeline davon aus, daß sich am anderen Ende einer eingehenden IPX-Verbindung ein anderer IPX-Router befand. Nachdem die Pipeline den Anruf beantwortete, konnte sie den Anrufer anhand der Einstellung „Peer=Dialin“ im Verbindungsprofil des Anrufers als Client erkennen. Bei anwählenden Windows 95-Clients ohne konfiguriertes Profil konnte es über eine Minute dauern, um die Verbindung herzustellen, und dann war der Client nicht in der Lage, die NetWare-Server auf dem lokalen Netzwerk zu sehen.

Das Antwortprofil enthält jetzt auch den Parameter „Peer“, damit die Pipeline eingehende IPX-Verbindungen als Clients behandeln kann, auch wenn konfigurierte Profile nicht verwendet werden.

Das neue Submenü „IPX Options“ im Antwortprofil enthält den Parameter „Peer“, mit dem die Pipeline eine Route zu anwählenden NetWare-Clients herstellen kann, auch wenn der Client kein konfiguriertes Profil aufweist. Der Standardwert für den Parameter „Peer“ ist „Router“, wodurch die Pipeline veranlaßt wird, eingehende IPX-Rufe zu behandeln, als befände sich am anderen Ende ein Router. Die Einstellung „Dialin“ veranlaßt die Pipeline, eingehende IPX-Rufe zu behandeln, als befände sich am anderen Ende ein anwählender NetWare-Client.

In der folgenden Liste sehen Sie den neuen Parameter „Peer“ sowie andere, erforderliche Parameter mit Beispielwerten:

```
Answer
    Profile Reqd=No
    IPX options...
        Peer=Dialin
    PPP options...
        Route IPX=Yes
```

```
Mod Config
    Ether options...
        IPX Enet#=cffff123
        IPX Pool#=cf000888
```

Erforderliche Einstellungen

Wenn Sie diese Funktion verwenden wollen, müssen Sie die Pipeline wie folgt konfigurieren:

- Anrufe, zu denen kein Verbindungsprofil gefunden wird, müssen beantwortet werden.

  Der Anruf erfordert u. U. eine Authentifizierung oder die Verwendung eines SecureID-Kennworts.

  Auf dem anwählenden Client muß die PPP-Software ausgeführt werden.
- Das IPX-Routing im Untermenü „PPP Options“ des Antwortprofils muß aktiviert sein, und die IPX-Netzwerknummer der Ethernet-Schnittstelle des Routers muß im Ethernet-Profil konfiguriert sein.
- Geben Sie im Ethernet-Profil eine IPX Pool-Nummer an, damit die Pipeline eine Route zu anwählenden Clients herstellen kann.

  Die Netzwerknummer muß innerhalb der gesamten IPX-Routing-Domäne der Pipeline (die lokale Routing-Domäne und alle WAN-Verbindungen) eindeutig sein. Dabei handelt es sich um ein „virtuelles“ IPX-Netzwerk, das anwählenden Clients vorbehalten ist. Falls ein Client keine eindeutige Node-Nummer angibt, weist die Pipeline dem Client auch eine eindeutige Node-Nummer hinzu.

  Hinweis: Die Pipeline verbreitet weder RIP noch SAP über die Verbindung und ignoriert RIP und SAP, die vom anderen Ende eingehen. Sie reagiert jedoch auf RIP- und SAP-Abfragen von anwählenden Clients.

IPX-Filter

IPX-Pakete können jetzt mit einer IPX-Filterschnittstelle gefiltert werden. In früheren Versionen wurden nur die Schnittstellen IP und Generic von Filtern unterstützt. Eine neue Auswahl wurde hinzugefügt, die Parameter zum Filtern von IPX-Paketen bieten.

Sie können jetzt einen neuen IPX-Filtertyp angeben. Beispiel:

```
Filter name
    In filter 01
    Valid=Yes
    Type=IPX
    Generic...
    Ip...
    Ipx...
```

Nachdem Sie den IPX-Filtertyp angegeben haben, ist das folgende IPX-Untermenü verfügbar:

```
Ipx...
    Forward=No
    Src Network Adrs=cfff0000
    Dst Network Adrs=cf088888
    Src Node Adrs=111222333
    Dst Node Adrs=aaabbbccc
    Src Socket Cmp=equal
    Src Socket #=0451
    Dst Socket Cmp=equal
    Dst Socket #=0015
```

Der Parameter „Forward“ funktioniert genauso wie bei anderen Filtertypen. Falls für diesen Parameter der Wert „No“ festgelegt wurde, wird ein übereinstimmendes Paket vernichtet. Die folgenden, neuen Filter-Parameter werden unterstützt:

- Src Network Adrs

  Die Adresse des Quell-IPX-Netzwerks. Sie müssen entweder die Quell- oder die Zieladresse (oder beide) angeben.

- Dst Network Adrs

  Die Adresse des Ziel-IPX-Netzwerks. Sie müssen entweder die Quell- oder die Zieladresse (oder beide) angeben.

- Src Node Adrs

  Eine gültige IPX-Knotenadresse. Die Knotenadresse „ffffffffffff“ verweist auf alle Knoten im angegebenen Quellnetzwerk. Sie müssen hier einen Wert festlegen, falls „Src Network Adrs“ nicht leer gelassen wurde.

- Dst Node Adrs

  Eine gültige IPX-Knotenadresse. Die Knotenadresse „ffffffffffff“ verweist auf alle Knoten im angegebenen Zielnetzwerk. Sie müssen hier einen Wert festlegen, falls „Dst Network Adrs“ nicht leer gelassen wurde.

- Src Socket Cmp and Src Socket #

  Bei einigen NetWare-Diensten erfolgt die Kommunikation über bestimmte Sockets; beispielsweise verwenden Datei-Server in der Regel Socket 0451. Falls Sie die Quell-Socket-Nummer angeben, können Sie auch angeben, mit welchem Vergleichstyp die Quell-Socket eines IPX-Pakets und der in diesem Filter angegebene Wert verglichen werden sollen. Sie können angeben, daß der Filter mit dem Paket übereinstimmt, falls die Quell-Socket-Nummer gleich, ungleich, kleiner oder größer als die im Filter angegebene ist.

- Dst Socket Cmp and Dst Socket #

  Falls Sie die Ziel-Socket-Nummer angeben, können Sie auch angeben, mit welchem Vergleichstyp die Ziel-Socket eines IPX-Pakets und der in diesem Filter angegebene Wert verglichen werden sollen. Sie können angeben, daß der Filter mit dem Paket übereinstimmt, falls die Ziel-Socket-Nummer gleich, ungleich, kleiner oder größer als die im Filter angegebene ist.

SPX-Spoofing für IPX hinzugefügt

NetWare-Programme, die eine garantierte Paketlieferung erfordern, verwenden das NetWare-SPX-Protokoll. Dazu gehören Programme wie Print Server (PSERVER), Remote Printer (RPRINTER) und Remote Console (RCONSOLE). Der SPX-Watchdog eines Clients überwacht die Verbindung mit dem Server, während die Verbindung ruht. Die Verbindung wird überwacht, indem der SPX-Watchdog eine Anforderung sendet, durch die eine WAN-Verbindung alle 14 Sekunden aufgerufen wird, während ein SPX-Programm ausgeführt wird.

In vorhergehenden Softwareversionen, führten diese wiederholten Watchdog-Pakete vom SPX-Watchdog des Clients dazu, daß die WAN-Verbindung unnötig aufrechterhalten wurde. Die Pipeline gestattet es jetzt Netware SPX-Clients, angemeldet zu bleiben, ohne die WAN-Verbindung bei Inaktivität aufrechtzuerhalten. Die Pipeline antwortet automatisch auf SPX-Watchdog-Aufforderungen vom LAN mit einem gespooften SPX-Watchdog-Antwortpaket und vernichtet alle SPX-Watchdog-Keep-Alive-Pakete des LAN, ohne sie an das WAN weiterzusenden.

Sie müssen keine Parameter einstellen.

Hinweis: Diese Funktion arbeitet nur, wenn sie von Routern an beiden Enden der Verbindung unterstützt wird.

Sicherheit

6

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie die Sicherheitsfunktionen auf Ihrer Einheit einrichten:

Unterstützung von Secure Access 6-2
Filterbeständigkeit 6-10
BACP-Unterstützung über MP hinzugefügt 6-12
Unterstützung von MS-CHAP 6-13
Unterstützung von „Called Number Authentication“ 6-15
Unterbrechungsursachencode für „CLID auth“ 6-17
„Expect Callback“ hinzugefügt 6-18
SNMP-Schreibsicherheit als Standard deaktiviert 6-19
SNMP-Anforderungsauthentifizierung hinzugefügt 6-21
Aufrufen von MPP-Sitzungsstatistiken mit „SNMP Get“ 6-25
SNMP hilft, einen Ruf einem Gerät zuzuordnen 6-27
SNMP-Erweiterungen 6-28
Feste Schnittstellen erscheinen in SNMP IfTable zuerst 6-29

Unterstützung von Secure Access

Die Pipeline unterstützt jetzt Secure Access Management (SAM), eine grafische Benutzerschnittstelle, mit der Sie IP-Firewalls erstellen können.

Eine vollständige Anleitung, um SAM zu verwenden und um Firewalls zur Pipeline hinzuzufügen, finden Sie in *Ascend Secure Access User's Guide* (Teile-Nr. 7820-0429-001).

Ascend unterstützt zur Zeit einfache „statische" Paketfilter. Eine Verbindung kann über ein Ruf- und/oder Datenfilterprofil verfügen. Ein Filterprofil kann bis zu 12 eingehende und 12 ausgehende Paketfilter aufweisen. Bei einem Paketfilter kann es sich um einen generischen oder einen IP-Filter handeln.

Dank Secure Access verfügt Ascend über folgende zusätzliche Filterfunktionen:

- Einfaches Schreiben von „dynamischen" Paketfiltern, auch „Firewalls" genannt, die es ermöglichen, den Datenverkehr in der Regel zu blockieren und ihn nur freizugeben, wenn ein Auslösefaktor, wie z. B. eine eingehende oder ausgehende Verbindungsanforderung, auftritt.
- Protokolliert den durch den Router gehenden Datenverkehr und bietet damit einen Prüfungspfad, mit dem IP-Verbindungen und Paketinhalte verfolgt werden können.
- Sendet eine entsprechende ICMP-Meldung, wenn ein Paket aufgrund eines Firewalls nicht weitergeleitet wird.

Eine Beschränkung der aktuellen Ascend-Paketfilter und der meisten anderen Router-Paketfilter ist, daß sie nicht in der Lage sind, mit einer Anzahl von IP-Protokollen sicher umzugehen. Secure Access verwendet „dynamische" Paketfilter, mit denen alle Pakete mit Ausnahme derjenigen blockiert werden können, die für eine bestimmte Sitzung erforderlich sind und nur für die Dauer der Sitzung.

Im Gegensatz zur aktuell beschränkten Anzahl von Filtern in einem Profil, ist die Anzahl der Paketfilter (d. h. „Regeln") in einem Firewall-Profil bei Secure Access nicht beschränkt. Die einzige Beschränkung ist die komprimierte Größe des Firewall-Profils oder die Speichergröße des Routers. Die aktuellen Ascend-Paketfilter werden auch weiterhin unterstützt. Daher sind Änderungen an der Pipeline-Konfiguration erst erforderlich, wenn Sie tatsächlich einen Firewall von Secure Access verwenden.

Um Secure Access auf Ihrer Pipeline zu aktivieren, müssen Sie sich einen Hash-Code besorgen.

Verwenden von SAM

Die Konfiguration eines Firewalls wird auf einer Pipeline-externen Workstation, die an das Netzwerk angeschlossen ist, mit der grafischen Benutzerschnittstelle SAM vorgenommen. Der vollständige Firewall wird dann auf der Pipeline, auf dem er verwendet wird, geladen.

Über das externe Programm, Secure Access Manager (SAM), können Sie auswählen, welche Services den Firewall passieren dürfen und welchen Hosts der Zugriff auf die Services gestattet wird.

Nachdem die Daten eingetragen wurden, kann SAM das Firewall-Profil in einer Pipeline laden oder in einer Datei speichern.

Eine vollständige Anleitung, um SAM zu verwenden und um Firewalls zur Pipeline hinzuzufügen, finden Sie in *Ascend Secure Access User's Guide* (Teile-Nr. 7820-0429-001).

Neues Menü in der Telnet-Schnittstelle

In der Telnet-Schnittstelle wurde ein neues Menü „Firewalls" hinzugefügt. Beispiel:

```
20-600 Firewalls
  >20-601 Sales
```

Wenn Secure Access auf der Pipeline aktiviert wurde, erscheint dieses Menü und speichert alle Firewalls, die mit SAM auf Ihrem System geladen wurden. Wenn Sie das Menü „Firewalls" öffnen, wird das Untermenü aufgelistet. Beispiel:

```
20-601 Sales
>Name=Engineering
 Version=1
 Length=2936
```

Beachten Sie, daß nur das Feld „Name" bearbeitet werden kann. Die Parameter „Version" und „Length" werden durch den in SAM erstellten Firewall festgelegt. Firewalls müssen mit SAM geändert werden.

Firewall-Nummern in der Telnet-Schnittstelle

Damit eine rückwärts gerichtete Kompatibilität mit der aktuellen Ascend-Filterimplementierung gegeben ist, müssen Sie mit SAM erstellte Firewalls anders numerieren als Filter, die mit der Telnet-Schnittstelle erstellt wurden. Sie können vorhandene Filter genau wie zuvor Profilen zuweisen. Wenn Sie jedoch einem Profil eine mit SAM erstellte Firewall zuweisen wollen, müssen den beiden letzten Stellen der Indexnummer in der Telnet-Schnittstelle 100 hinzufügen. Das Numerierungsschema für Filter lautet folgendermaßen:

- 0 gibt an, daß kein Filter verwendet wird
- 1-99 gibt an, daß ein mit der Telnet-Schnittstelle erstellter Filter verwendet wird
- 100-199 gibt an, daß ein mit SAM erstellter Filter verwendet wird.

Beispiel: Sie haben bereits die folgenden Ascend-Filter angelegt:

```
90-500 Filters
>90-501 IP Call
 90-502 NetWare Call
 90-503 AppleTalk Call
 90-504 Engineering
 90-505 Test Eng
 90-506 Marketing
 90-507
 90-508
 90-500
 90-510
 90-511
 90-512
```

Falls Sie den Filter „Engineering“ in einem Verbindungs- oder Mod-Config-Profil verwenden wollen, müssen Sie die Zahl 4 im Feld „Data Filter“ oder „Call Filter“ (in einem Verbindungsprofil) oder im Feld „Filter“ (im Feld „Mod Config, Ether options“) eingeben.

Wenn Sie einen Firewall mit SAM erstellt und ihn auf der Pipeline geladen haben, ähnelt das Menü „Firewalls“ dem folgenden Beispiel:

```
20-600 Firewalls
>20-601 Sales
 20-602
 20-603
 20-604
```

Falls Sie den Filter „Sales“ in einem Verbindungs- oder Mod-Config-Profil verwenden wollen, müssen Sie die Zahl 101 im Feld „Data Filter“ oder „Call Filter“ (in einem Verbindungsprofil) oder im Feld „Filter“ (im Feld „Mod Config, Ether options“) eingeben.

Zuweisen von Firewalls zu einem Verbindungsprofil

Mit Firewalls, die einem Verbindungsprofil zugewiesen wurden, wird der ein- und ausgehenden Datenverkehr auf einer WAN-Verbindung gefiltert. Filter, die einem Verbindungsprofil zugewiesen wurden, werden aktiviert, sobald eine WAN-Sitzung online geht.

Wenn Sie einem Verbindungsprofil einen Firewall zuweisen wollen, gehen Sie folgendermaßen vor:

1 Erstellen Sie einen Firewall-Filter mit SAM.

2 Laden Sie ihn auf die Pipeline.

3 Wählen Sie „Ethernet, Connections, *ein Verbindungsprofil*, Session options“.

4 Geben Sie die Nummer des gewünschten Firewall-Filters im Feld „Data Filter“ ein.

Diese Nummer ergibt sich, wenn Sie zu den beiden letzten Stellen der Indexnummer im Menü „Firewall“ 100 hinzufügen. Beispiel: Wenn der Firewall die Nummer 20-503 hat, geben Sie im Feld „Data Filter“ 103 ein.

5 Beenden Sie das Verbindungsprofil, und speichern Sie die Änderungen.

Zuweisen von Firewalls zum Mod-Config-Profil

Mit Firewalls, die dem Mod-Config-Profil zugewiesen wurden, wird der ein- und ausgehenden Datenverkehr auf einer WAN-Verbindung gefiltert. Filter, die dem Mod-Config-Profil zugewiesen wurden, werden aktiviert, sobald Sie die Änderungen an dem Mod-Config-Profil speichern.

Wenn Sie dem Mod-Config-Profil einen Firewall zuweisen wollen, gehen Sie folgendermaßen vor:

1. Erstellen Sie einen Firewall-Filter mit SAM.
2. Laden Sie ihn auf die Pipeline.
3. Wählen Sie „Ethernet, Mod Config, Ether options“.
4. Geben Sie die Nummer des gewünschten Firewall-Filters im Feld „Filter“ ein.

   Diese Nummer ergibt sich, wenn Sie zu den beiden letzten Stellen der Indexnummer im Menü „Firewall“ 100 hinzufügen. Beispiel: Wenn die Firewall die Nummer 20-503 hat, geben Sie im Feld „Filter“ 103 ein.
5. Beenden Sie das Mod-Config-Profil, und speichern Sie die Änderungen.

Neues Feld in „Sys Options“

Im Fenster „Sys Options“ wurde „Secure Access“ hinzugefügt. Alle Software-Produkte, die die Funktion Secure Access beinhalten, werden das Feld „Sec Acc“ aufweisen. Falls die Funktion noch nicht aktiviert wurde, ist die Option „Not Inst“ markiert. Falls sie aktiviert wurde, ist die Option „Installed“ markiert.

```
00-100 Sys Options
>Switched Installed^
 Frm Rel Installed
 Sec Acc Installed  V
```

Neue Parameter

Die folgenden Parameter wurden hinzugefügt oder erweitert, um Firewalls auf Ascend-Produkten zu unterstützen:

- Name
- Version
- Length

Name

Beschreibung: Gibt den Namen des Firewalls an. Dieser Name wurde ursprünglich mit der grafischen Benutzerschnittstelle von Secure Access Manager (SAM) erstellt.

Verwendung: Betätigen Sie die Eingabetaste, um ein Textfeld zu öffnen. Geben Sie dann den Namen des Firewalls ein. Betätigen Sie die Eingabetaste erneut, um das Textfeld zu schließen.

Parameter-Ort: Ethernet > Firewalls > *ein Firewall*

Version

Beschreibung: Ein Firewall enthält eine Versionsnummer, um sicherzustellen, daß ein Firewall, der auf einen Router geladen wird, mit der Firewall-Software auf dem Router kompatibel ist. SAM prüft die Versionsnummer, bevor ein Firewall geladen wird. Falls bei einem Router, der über ein gespeichertes Firewall-Profil verfügt, eine Code-Aktualisierung durchgeführt wird, nach der der vorhandene Firewall nicht mehr kompatibel ist, wird ein Standard-Firewall aktiviert, durch die nur ein Telnet-Zugriff auf die Pipeline möglich ist.

Verwendung: Dieser Parameter kann nicht bearbeitet werden.

Parameter-Ort: Ethernet > Firewalls > *ein Firewall*

Length

Beschreibung: Gibt die Länge des Firewalls an, die von SAM auf die Pipeline geladen wird.

Verwendung: Dieser Parameter kann nicht bearbeitet werden

Parameter-Ort: Ethernet > Firewalls > *ein Firewall*

Syslog-Meldungen

Syslog-Meldungen können für Pakete erzeugt werden, die vom Firewall „gesehen“ werden, falls dies in SAM so festgelegt wurde. Als Standard wird eine Syslog-Meldung für alle Pakete erzeugt, die vom Firewall blockiert werden.

Syslog-Meldungen werden von Firewalls im Standardformat erzeugt:

```
<date> <time> <router name> ASCEND: <interface> <message>
```

- <date>: das Datum, an dem die Meldung von Syslog protokolliert wurde.
- <time>: die Uhrzeit, zu der die Meldung von Syslog protokolliert wurde.
- <router name>: der Router, von dem die Meldung ausging.
- <interface>: der Name der Schnittstelle (ie0, wan0 usw.) oder ‘call’, falls das Paket vom „Call Filter“ bei der Aktivierung der Verbindung protokolliert wurde.
- <message>: eines oder mehrere Felder können vorhanden sein:

  ```
  <protocol> <local> <direction> <remote> <length> <frag> <log>
  <tag>
  ```

  – <protocol>: entweder der Ether-Typ mit 4 Hexadezimalstellen oder der Netzwerk-Protokollname - „arp“, „rarp“, „ipx“, „appletalk“.

  <protocol>: (bei IP-Protokollen) entweder die IP-Protokollnummer (bis zu 3 Dezimalstellen) oder einer der folgenden Namen:

  ip-in-ip

  tcp

  icmp

  udp

  esp

  ah

  Im speziellen Fall von icmp, wird auch der ICMP-Code und Typ ([Code]/[Typ]/icmp) angezeigt.

  – <local>: (bei nicht-IP-Paketen) die Quell-Ethernet-MAC-Adresse von übertragenen Paketen und die Ziel-Ethernet-MAC-Adresse von empfangenen Paketen. Bei einer Non-Bridged-WAN-Verbindung zeigen beide MAC-Adressen nur Nullen an.

<local>: (bei IP-Protokollen) die IP-Quelladresse von übertragenen Paketen und die IP-Zieladresse von empfangenen Paketen. Im Falle von TCP oder UDP wird auch eine TCP- oder UDP-Anschlußnummer angezeigt ([IP-Adresse];[Anschluß]).

– <direction>: ein Pfeil (“<-”, “->”), der anzeigt, in welche Richtung das Paket unterwegs war (Empfang bzw. Sendung).

– <remote>: (bei nicht-IP-Protokollen) hat das gleiche Format wie <local>, zeigt aber die Ziel-Ethernet-MAC-Adresse von übertragenen Paketen und die Quell-Ethernet-MAC-Adresse von empfangenen Paketen an.

  <remote>: (bei IP-Protokollen), hat das gleiche Format wie <local>, zeigt aber die IP-Zieladresse von übertragenen Paketen und die IP-Quelladresse von empfangenen Paketen an.

– <length>: die Länge des Pakets in Oktetten (8 Bit-Byte).

– <frag>: wird verwendet, um „frag“ zu berichten, falls das Paket einen IP-Versatz, der nicht Null ist, aufweist, oder falls „IP More-Fragments“ im IP-Header eingerichtet wurde.

– <log>: erzeugt eine oder mehrere Meldungen auf der Grundlage des Paketstatus oder der Flags des Paket-Headers. Die Paketstatusmeldungen beinhalten:

  corrupt: das Paket zeigt interne Inkonsistenz

  unreach: das Paket wurde mit einer “unreach=”-Regel des Firewalls erstellt

  !pass: das Paket wurde von einem Daten-Firewall blockiert

  bringup: das Paket entspricht dem Sprach-Firewall

  !bringup: das Paket entsprach nicht dem Sprach-Firewall

  Zu den TCP-Flags, die angezeigt werden, gehören „syn“, „fin“, „rst“.

  „syn“ wird nur für das erste Paket angezeigt, für das das Flag „SYN“ und nicht das Flag „ACK“ gesetzt wurde.

– <tag>: enthält vom Benutzer definierte Kennzeichen, die in der von SAM verwendeten Filterschablone angegeben wurden.

Filterbeständigkeit

Dem Verbindungsprofil aller Pipelines, die Filterprofile unterstützen, wurde der Parameter „ Filter Persistence“ hinzugefügt. Sie müssen für diesen Parameter den Wert „Yes“ festgelegt haben, damit die Firewalls einer Verbindung auch nach dem Abbruch einer Verbindung, z. B. durch ein Timeout, weiterhin bestehen. Der Standardwert ist „No“, d. h. das die Firewalls einer Verbindung nicht weiter bestehen, nachdem ein Ruf beendet wurde.

Hinweis: In der Regel wird ein Firewall für etwa eine Stunde weiterbestehen, nachdem die zugehörige Verbindung unterbrochen wurde.

Informationen zu Firewall- und Filterbeständigkeit

Mit dem Parameter „Filter Persistence“ können die Filter-/ Firewallspezifikationen einer Pipeline während der gesamten Dauer ihrer Verbindungen erhalten werden.

Der Unterschied zwischen einem Firewall und einem Filter besteht darin, daß der Firewall sein Verhalten ändert, wenn Datenverkehr durch ihn hindurchgeht, während der Filter unverändert bleibt. Dies erforderte eine Änderung der Art, in der Firewalls und Filter Verbindungen zugeordnet werden.

In ihrer ursprünglichen Implementierung sorgten Ascend-Filter dafür, daß Filter erstellt und zerstört wurden, wenn sich der Zustand einer Verbindung änderte. Dadurch wird die Pipeline veranlaßt, bei Änderungen des Verbindungszustands Filter zu erstellen und zu vernichten, ohne daß der Zustand des Filters berücksichtigt wird.

Bei Secure-Access-Firewalls ist es erforderlich, daß der Firewall-Zustand über alle Umwandlungen hinweg, die die Verbindung durchlaufen kann, unverändert bleibt. Filter können jederzeit erstellt oder vernichtet werden, um Änderungen aufgrund von Multilink- und Ruhezuständen zu entsprechen; bei einer Firewall ist das nicht möglich.

Zur Lösung dieses Problems können Sie Ascend-Filtern und Firewalls eine fortdauernde Beständigkeit zuweisen. Ein beständiger Filter oder Firewall bleibt auch dann erhalten, wenn die zugehörige Verbindung inaktiv wird. Außerdem kann der Filter oder Firewall zugewiesen werden, wenn einer Verbindung eine zusätzliche Sitzung zugeordnet wird, wie dies bei zusätzlichen Kanälen einer MPP-Verbindung der Fall ist.

Hinweis: Firewalls müssen beständig sein, um korrekt funktionieren zu können; bei Filtern ist dies nicht der Fall.

Filterbeständigkeit und Verbindungsprofile

Mit Verbindungsprofilen werden verschiedene Kontaktstellen beschrieben. In einer Firmenzweigstelle könnte es beispielsweise ein Profil für die Hauptniederlassung und ein anderes Profile für den Internet-Provider geben. Auf alle Fälle möchte der Pipeline-Benutzer die Secure-Access-Firewall verwenden, um ein nicht genehmigtes Eindringen in das lokale Netzwerk durch Andere zu verhindern.

Mit Wählen-bei-Bedarf und automatischer Zeitsperre für Rufe würden die dynamischen Firewall-Möglichkeiten der Secure-Access-Firewall verhindern, daß laufende TCP-Sitzungen (z. B. Telnet oder Rlogin) nach der Beendigung und dem erneuten Start (z. B. wegen Inaktivität) fortgesetzt werden. Ohne Beständigkeit wird am Beginn eines Rufs ein neuer Firewall ohne Wissen über eine laufende TCP-Sitzung erstellt. Dies würde dazu führen, daß Pakete für solche Sitzungen blockiert werden würden, wenn die Verbindung wieder hergestellt wird. Dies hätte zur Folge, daß die laufenden Telnet-Sitzungen (oder Rlogin usw.) nicht mehr betriebsfähig wären, und möglicherweise würden davon abhängige, laufende Arbeiten zerstört werden.

Mit „Filter Persistence“ können Sie die Pipeline anweisen, einen Firewall zu erhalten, auch nachdem ein Ruf beendet wurde. Wenn ein neuer Ruf bei derselben Station eingeht (oder von derselben Station empfangen wird), „erinnert“ sich die Pipeline an den ursprünglichen Firewall und verwendet ihn, als wäre der Ruf nie beendet worden. Auf diese Weise kann der Benutzer ohne Verlust weiterarbeiten.

Andererseits kann es vorkommen, daß ein Verbindungsprofil für verschiedene Standorte verwendet wird. Dies könnte z. B. der Fall sein, falls Sie dasselbe Verbindungsprofil verwenden, um mehrer verschiedene Rufer zu beschreiben. In diesem Fall sollten die Filter und Firewalls nicht beständig sein, da die Pipeline nicht wissen kann, ob die Anrufe von den gleichen Benutzern eingehen.

Filter persistence

Beschreibung: Gibt an, ob der Filter oder Firewall, der einem Verbindungsprofil zugewiesen wurde, weiterbesteht, nachdem die Verbindung unterbrochen wurde.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten:

- „Yes“ gibt an, daß der Filter oder Firewall, der dem Verbindungsprofil zugewiesen wurde, weiterbesteht, nachdem die Verbindung unterbrochen wurde.

  Hinweis: In der Regel wird ein Firewall für etwa eine Stunde weiterbestehen, nachdem die zugehörige Verbindung unterbrochen wurde.
- „No“ gibt an, daß der Filter oder Firewall, der dem Verbindungsprofil zugewiesen wurde, weiterbesteht, nachdem die Verbindung unterbrochen wurde.

  Der Standardwert ist „No“.

Parameter-Ort: Ethernet > Connections > *Profil* > Session options

Siehe auch: Call Filter, Data Filter, Name, Version, Length

BACP-Unterstützung über MP hinzugefügt

Beim Bandwidth Allocation Control Protocol (BACP) handelt es sich um den Internet-Standard, der Ascend Multilink Protocol Plus (MP+) entspricht.

Funktionsweise des BACP

BACP läuft über MP und gestattet es einem Gerät, das MP unterstützt (unabhängig von dessen Hersteller), je nach Bedarf eine Bandbreite hinzuzufügen oder zu entfernen. BACP funktioniert ähnlich wie MP+ und verwendet die gleichen Menüelemente wie MP+. Da BACP nicht „Idle Percent“ unterstützt, wurde das Feld aus dem Untermenü „Encaps“ des Ethernet-Verbindungsprofils entfernt.

BACP

Beschreibung: Wird verwendet, um mit dem BACP Daten zu senden oder zu empfangen.

Verwendung: Wählen Sie den Parameter, und markieren Sie mit dem Aufwärts- oder Abwärtspfeil „Yes“ oder „No“. Betätigen Sie die Eingabetaste, um die Auswahl vorzunehmen.

- Für den Empfang legen Sie „BACP=Yes“ in Ethernet > Answer > PPP Options fest.
  Der Standardwert ist „No“.
- Für die Sendung legen Sie „Encaps=MP” in Ethernet > Connection > *Profile* fest. Legen Sie im Untermenü „Encaps option“ „BACP=Yes“ fest.
  Der Standardwert ist „No“.

  Hinweis: Das Feld „Idle Percent“ erscheint nicht im Menü „Encaps options“, wenn für „Encaps“ der Wert „MP“ festgelegt wurde, das nicht auf MP oder BACP zutrifft.

Parameter-Ort: Ethernet > Connections > *Profile* > Encaps options; Ethernet > Answer > PPP options.

Unterstützung von MS-CHAP

Für Windows NT-Systeme wurde die Unterstützung von MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) hinzugefügt.

Sie können eine Pipeline jetzt so konfigurieren, daß die MS-CHAP-Authentifizierung gesendet oder empfangen werden kann. Diese Authentifizierung wird detailliert im Microsoft-Website unter folgender Adresse beschrieben:

`ftp://ftp.microsoft.com/DEVELOPR/RFC/chapexts.txt`

Hinweis: MS-CHAP mit DES- und MD4-Verschlüsselung, die in dieser Version unterstützt wird, funktioniert nur in der Windows NT-Umgebung. Die Pipeline kann ein Windows NT-System authentifizieren, und ein Windows NT-System kann eine Pipeline authentifizieren.

Konfigurieren einer Pipeline für MS-CHAP-Authentifizierung

Die Optionen, die für den Parameter „Recv Auth=“ im Untermenü „PPP Options“ des Antwortprofils verfügbar sind, wurden geändert. Bisher war „Recv Auth=Either“ verfügbar, um eine Pipeline so zu konfigurieren, daß sie empfangenen Datenverkehr mit PAP oder CHAP authentifizierte. Diese Option wurde geändert in „Recv Auth=PAP/CHAP/MS-CHAP“, damit die Pipeline eines der Authentifizierungsprotokolle (PAP, CHAP oder MS-CHAP) bei der Kommunikation mit Windows NT-Systemen verwenden kann.

Wenn Sie eine Pipeline so konfigurieren wollen, daß sie die Authentifizierung mit MS-CHAP durchführt, müssen Sie ein der folgenden Optionen für „Recv Auth=“ auswählen.

Wert für Recv Auth=	Beschreibung
EITHER	Gestattet die Authentifizierung, falls die Gegenstelle dazu eines der angegebenen Authentifizierungsprotokolle verwenden kann.
MS-CHAP	Gestattet die Authentifizierung nur, falls die Gegenstelle MS-CHAP zur Authentifizierung verwendet.

Wenn Sie eine Pipeline so konfigurieren wollen, daß sie mit MS-CHAP-Authentifizierung sendet, müssen Sie „Send Auth=MS-CHAP“ im Untermenü „Encaps options“ des Verbindungsprofils festlegen. Wenn Sie diese Option gewählt haben, setzt die Pipeline die Authentifizierung nur fort, falls die Gegenstelle ebenfalls MS-CHAP-Authentifizierung unterstützt.

Unterstützung von „Called Number Authentication“

Diese Funktion fügt die Authentifizierung anhand der angerufenen Nummer hinzu. Sie ähnelt der Authentifizierung anhand der Anschlußkennung der rufenden Leitung (CLID), verwendet jedoch die Nummer (ID) der gerufenen Einheit statt der Nummer der rufenden Einheit.

Konfigurieren von „Calling“ oder „Called Number Authentication“

Um die Konfiguration für „Called Number Authentication“ zu unterstützen, wurden die folgenden Änderungen vorgenommen:

Profil	Beschreibung der Änderung
Verbindungsprofil	Das neue Feld „Called #“ wurde hinzugefügt. „Called #“ gleicht in der Regel „Dial #“, jedoch fehlt das Leitungsbündel oder die Vorwahl.
Antwortprofil	„Clid Auth=“ wurde in „Id Auth=“ geändert.

Einstellung	Beschreibung der Änderung
Ignore	Weder CLID (Anschlußkennung der rufenden Leitung) noch DNIS (angerufener Anschluß) wirken sich auf die Authentifizierung eingehender Rufe aus (beide werden ignoriert).
Prefer	Keine Änderung
Require	Keine Änderung
Fallback	Keine Änderung
Called Require	Gleicht „Require“, jedoch wird statt der rufenden die gerufene Nummer überprüft.

Einstellung	Beschreibung der Änderung
Called Prefer	Gleicht „Prefer“, jedoch wird statt der rufenden die gerufene Nummer überprüft.

Called #

Beschreibung: Fügt Authentifizierung durch „Called Number“ hinzu, indem die Nummer (ID) der gerufenen statt der Nummer der rufenden Einheit verwendet wird. „Called #“ gleicht in der Regel „Dial #“, jedoch fehlt das Leitungsbündel oder die Vorwahl.

Verwendung: Wählen Sie den Parameter und gehen Sie die Optionen durch.

- „Ignore“ - die anrufende Nummer oder die gerufene Nummer wird ignoriert.
- „Prefer“ - verwendet Authentifizierung mit rufender Kennnummer, aber falls diese nicht verfügbar ist, wird die Authentifizierung nit Name/Kennwort verwendet.
- „Require“ - verwendet Authentifizierung mit angerufener Kennnummer.
- „Fallback“ trifft auf die Pipeline nicht zu.
- „Called Require“ - gleicht „Require“, jedoch wird statt der rufenden die gerufene Nummer verwendet.
- „Called Prefer“ - gleicht „Prefer“, jedoch wird statt der rufenden die gerufene Nummer verwendet.

Abhängigkeiten: Es empfiehlt sich, auch alle Informationen für die Authentifizierung nit Name/Kennwort anzugeben, falls die angerufene Nummer blockiert ist (durch die Telefongesellschaft). Beide Authentifizierungstypen *werden nicht* an einer Verbindung durchgeführt.

Parameter-Ort: Ethernet > Connections > *Profile*

Siehe auch: Id Auth

Unterbrechungsursachencode für „CLID auth“

Wenn in einer ISDN-Verbindung die CLID-Authentifizierung scheitert, sendet die Pipeline eine Unterbrechungsmeldung. Die Meldung „Cause Element in the Disconnect“ kann darauf hinweisen, warum die CLID-Authentifizierung gescheitert ist. Sie können den Unterbrechungsursachencode für das Scheitern der CLID-Authentifizierung auf „User Busy“ oder „Normal call clearing“ einrichten.

Legen Sie den Wert für „Disconnect Cause“ im „Ethernet-Profil > Mod Config > Auth“ fest:

```
X0-X00 Mod Config
 Auth...
  CLID Fail Busy=No
  APP Server=No
  APP Host=N/A
  APP Port=N/A
```

CLID Fail Busy

Beschreibung: Gibt die Unterbrechungsursache an, wenn die CLID-Authentifizierung aufgrund einer Zeitsperre gescheitert ist.

- „No“ legt den Unterbrechungsursachencode als „Normal call clearing“ fest und ist der Standardwert.
- „Yes“ legt den Unterbrechungsursachencode als „User Busy“ fest.

Verwendung: Wählen Sie den Parameter, und betätigen Sie die Eingabetaste, um die verfügbaren Einstellungen durchzugehen. Betätigen Sie die Esc-Taste, um den Parameter zu verlassen.

Abhängigkeiten: Die CLID-Authentifizierung muß aktiviert sein, um diesen Parameter festlegen zu können. Legen Sie ihn fest in Ethernet > Answer > ID Auth.

Parameter-Ort: Ethernet > Mod Config > Auth.

Siehe auch: ID Auth.

„Expect Callback“ hinzugefügt

Ein Parameter wurde dem Untermenü „Telco options“ im Menü „Connections“ hinzugefügt, damit die Pipeline so konfiguriert werden kann, daß sie einen Rückruf von der gerufenen Einheit erwartet. Dadurch werden Probleme verhindert, die entstehen, wenn auf der Einheit, von der ein Rückruf erwartet wird, für CLID der Wert „Required“ festgelegt wurde.

Funktionsweise von „Expect Callback“

Wenn die Pipeline einen Ruf einleitet und die Verbindung hergestellt wird, beendet die angerufene Einheit den Ruf und leitet sofort einen Ruf an die anrufende Einheit ein (Rückruf), bevor eine Kennwortauthentifizierung durchgeführt wird.

In der folgenden Abbildung wird ein Befehl „Ping“ oder „Telnet“ über eine MAX-Einheit an eine Pipeline initiiert, und „CLID=Required“ wurde auf der Pipeline (die Seite, die den Rückruf durchführen wird) festgelegt. Das führt dazu, daß die Pipeline den eingehenden Ruf ablehnen wird, bevor sie ihn beantwortet. Die MAX-Einheit (die initiierende Seite) erhält den Eindruck, daß der Ruf nicht durchgekommen ist.

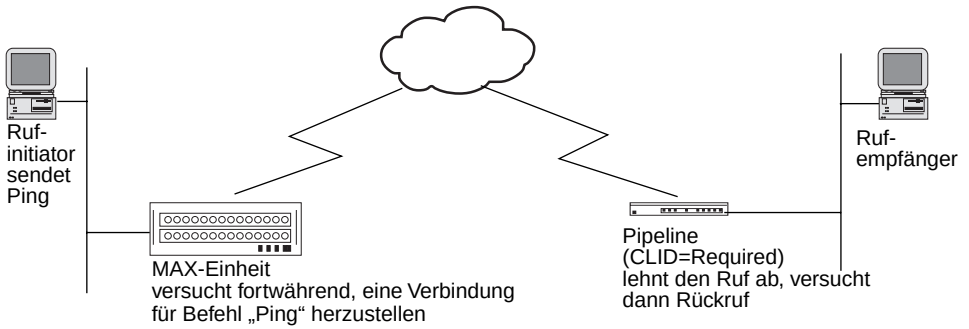


Abbildung 6-1.Rückrufverbindung gescheitert

Dies ist ein spezielles Problem mit den Befehlen „Ping“ und „Telnet“, weil diese Prozesse fortwährend versuchen, eine Verbindung herzustellen und einen Rückruf ablehnen, da der Prozeß bereits versucht, eine Verbindung herzustellen.

Wenn Sie „Expect Callback=Yes“ festgelegt haben, werden abgehende Rufe, die gewählt wurden, für die aber keine Verbindung zustande kam (gleichgültig, aus welchem Grund), auf eine Liste gesetzt, die keine weiteren Rufe zu diesem Ziel für 90 Sekunden gestattet. Dadurch erhält die Gegenstelle Gelegenheit, den Rückruf durchzuführen.

Aktivieren von „Expect Callback“

Sie sollten für den Parameter „Expect Callback“ nur in Profilen abgehender Rufe den Wert „Yes“ (TRUE) festlegen und ihn nicht bei eingehenden Rufen verwenden.

Wenn Sie „Expect Callback=Yes“ festlegen wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie „Ethernet > Connections > *alle Profile* > Telco“.

2 Legen Sie „Exp Callback=Yes“.

Hinweis: Falls ein Ruf aus irgendeinem Grund scheitert, gleichgültig, ob die gerufene Einheit CLID erfordert und einen Rückruf versucht oder nicht, muß die anrufende Einheit dennoch 90 Sekunden warten, bevor sie versucht, dieselbe Nummer erneut anzurufen, falls Sie „Expect Callback=Yes“ festgelegt haben.

SNMP-Schreibsicherheit als Standard deaktiviert

Ein neuer Parameter „R/W Comm Enable“ mit dem Standardwert „No“ deaktiviert Einstellungsbefehle. Bisher wurden SNMP-Einstellungsbefehle standardmäßig gestattet.

Aktivieren der SNMP-Schreibsicherheit

Mit SNMP-Einstellungsbefehlen können Sie die Systemkonfiguration einer Pipeline über TFTP laden und speichern sowie die Konfiguration der Einheit ändern. Ab dieser Softwareversion werden SNMP-Einstellungsbefehle nicht mehr standardmäßig gestattet.

Über den neuen Parameter „R/W Comm Enable“ in dieser Funktion können Sie angeben, daß SNMP-Einstellungsbefehle aktiviert sind. Wenn Sie SNMP-Einstellungsbefehle aktivieren wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie „Ethernet > Mod Config > SNMP Options“.

```
90-B00 Mod Config
 SNMP options...
  Read Comm=public
 >R/W Comm Enable=No
  R/W Comm=N/A
```

2 Legen Sie „R/W Comm Enable=Yes“ fest.

Wenn Sie „R/WComm Enable=No“ festlegen, ist der Parameter „R/W Comm“ nicht zutreffend.

Hinweis: Wenn Sie einen Einstellungsbefehl verwenden wollen, muß Ihnen die Community-Zeichenfolge für den Lese- und Schreibzugriff bekannt sein, selbst, wenn „R/W Comm Enable=Yes“ festgelegt wurde.

R/W Comm Enable

Beschreibung: Aktiviert und deaktiviert die Verwendung von SNMP-Einstellungsbefehlen.

Verwendung: Betätigen Sie die Eingabetaste, um „Yes“ oder „No“ zu wählen.

- „Yes“ aktiviert die Verwendung von SNMP-Einstellungsbefehlen. Wenn Sie einen Einstellungsbefehl verwenden wollen, muß Ihnen die Community-Zeichenfolge für den Lese- und Schreibzugriff bekannt sein, der im Parameter „R/W Comm“ angegeben wurde.
- „No“ deaktiviert die Verwendung von SNMP-Einstellungsbefehlen.

  Der Standardwert ist „No“.

Parameter-Ort: Ethernet > SNMP Options > Mod Config

SNMP-Anforderungsauthentifizierung hinzugefügt

Diese Funktion führt die SNMP-Anforderungsauthentifizierung, einschließlich Antwortschutz, in die Produktlinie der Ascend-Router ein. Diese Implementierung der SNMP-Anforderungsauthentifizierung ist kompatibel mit standardmäßigen SNMPv1-Verfahren und wirkt sich auf die Interpretation von SNMP-Meldungen durch die Router, die sie verwenden, aus. Bisher bot die Pipeline keine Möglichkeit zur Authentifizierung von SNMP-Anforderungen.

Sie können SNMP für sicherheitsbezogene Vorgänge verwenden, z. B. den Betriebszustand des Routers (Neustarten, Laden von Konfigurationen usw.) oder Firewall-Konfigurationen ändern. Da die vorhandene SNMPv1 im Grunde genommen unsicher ist, wird mit dieser Funktion die Authentifizierung hinzugefügt, um sicherzustellen, daß nur auf SNMP-Anforderungen reagiert wird, wenn sie bekanntermaßen von einem autorisierten System ausgehen und auch dann nur, wenn sie jüngeren Datums sind.

Authentifizierungselemente

Diese Funktion verwendet vier Elemente, um SNMP-Pakete zu authentifizieren:

- geheimer Authentifizierungsschlüssel
- Daten, die zu authentifizieren sind
- zeitabhängige Zustandsvariablen (für Antwortschutz)
- MD5-Hash-Wert mit Schlüssel, Daten und Zeit kalkuliert.

Die Daten-, Zeit- und Hash-Werte werden zusammen mit dem Paket übertragen. Dadurch können die Management-Station und der Router überprüfen, ob das Paket von einem autorisierten System erstellt wurde, und daß das Paket bei der Übertragung nicht geändert oder ausschlaggebend verzögert wurde.

Das MD5-Hash garantiert mit hoher Wahrscheinlichkeit, daß nur ein System, dem der geheime Authentifizierungsschlüssel bekannt ist, das Paket erzeugt haben kann. Die Zeit-Variable garantiert mit hoher Wahrscheinlichkeit, daß kein Angreifer ein authentifiziertes Paket eingesammelt und es zu einem von ihm gewählten Zeitpunkt nach einer beträchtlichen Verzögerung übertragen hat.

Änderungen an der Community-Zeichenfolge

Mit dieser Funktion wird die interne Struktur der Community-Zeichenfolge für den Schreibzugriff in der Routerkonfiguration geändert. Die ursprüngliche SNMPv1-Definition der Community-Zeichenfolge ist, daß es sich um eine Folge von Oktetten handelt, die mit einer ähnlichen Folge in der empfangenden ENMP-Einheit verglichen wird. Falls die Zeichenfolge im Paket genau mit der Community-Zeichenfolge in der empfangenden Einheit übereinstimmt, dann wird das Paket als authentisch betrachtet. Im Augenblick bestehen vorhandene Community-Zeichenfolgen aus einfachen ASCII-Zeichenfolgen ohne interne Struktur. Sie können diese Zeichenfolgen als Teil der Routerkonfiguration ändern.

Die Standardwerte lauten z.Z.:

Ethernet > Mod Config > SNMP Options > Read comm=public

Ethernet > Mod Config > SNMP Options > R/W comm=write

Die neue Struktur der Community-Zeichenfolge trennt die Zeichenfolge durch einen senkrechten Strich vom Schlüssel:

Ethernet > Mod Config > SNMP Options > R/W comm=write|secretkey

Dadurch wird es für den Router erforderlich, die Authentifizierung von SNMP-SET-REQUEST-Paketen anzufordern, wobei „secretkey“ als gemeinsam benutztes (aber nicht übertragenes) Geheimnis verwendet wird.

Eine authentifizierte Community-Zeichenfolge enthält die folgende Struktur:

Die Community-Zeichenfolge

- ein Oktett mit dem Wert Null
- ein vom Router erstellter und festgelegter "Magic Cookie"
- die aktuelle Nutzzeit des Routers (in Sekunden)
- 16 Byte MD5-Hash berechnet aus:
  - geheimem Schlüssel
  - Magic Cookie
  - Nutzzeit
  - Protocol Data Unit (PDU), d. h. die Daten im Paket

Diese Struktur wird vom Router interpretiert, wenn er ein SNMP-Paket empfängt, und sie wird vom Router erstellt, wenn er auf eine empfangene SNMP-Anforderung antwortet, die eine authentifizierte Community-Zeichenfolge enthielt.

Cookie- und Nutzzeit-Variable

Es wird erwartet, daß die Kombination von Cookie und Nutzzeit ein eindeutiger Ausdruck der Echtzeit für alle Routers ist, selbst Router, die die Kalenderzeit nicht aktualisieren, wie z. B. die Pipeline 50 und Pipeline 75.

Die Nutzzeit wird einmal pro Sekunde beim Routerbetrieb inkriminiert. Das bedeutet, daß sich die Nutzzeit z. B. zwischen dem Neustarten auf voraussagbare Weise ändert. Der Router vergleicht den Wert der Nutzzeit im Paket mit seinem eigenen Wert und berechnet den Unterschied. Es wird davon ausgegangen, daß Pakete über einen neu kalkulierten Hash-Wert verfügen, wenn der Unterschied kleiner als 10 Sekunden ist, was darauf hinweist, daß das Paket weniger als 10 Sekunden alt ist.

Wenn der Router neu gestartet wird, erstellt ein Zufallsalgorithmus einen neuen Cookie, sobald das erste authentifizierte SNMP-Anforderungspaket eingeht.

Dank der Kombination eines Cookie-Wertes, der sich bei jedem Neustarten ändert, und einem Nutzzeitwert, der sich zwischen jedem Neustarten ändert, kann der Router garantieren, daß ein authentifiziertes Paket über einen eindeutigen MD5-Hash-Wert verfügt und daß sich die einzelnen authentifizierten SNMP-Pakete voneinander unterscheiden.

Cookie und Nutzzeit werden nicht verschlüsselt oder verborgen. Nur der geheime Schlüssel wird vor nicht befugten Benutzern verborgen.

Funktionsweise der SNMP-Authentifizierung

1 Wenn der Router eine SNMP-Authentifierungsanforderung empfängt überprüft er die Community-Zeichenfolge im Paket und vergleicht sie mit seinen eigenen Community-Zeichenfolgen.

- Falls die Community-Zeichenfolge im Paket mit einer nicht authentifizierten Community-Zeichenfolge im Router übereinstimmt, verhält sich der Router normal, d. h. er interpretiert des Paket und erzeugt ein Antwortpaket mit derselben Community-Zeichenfolge.

- Falls die Community-Zeichenfolge im Paket weder mit einer nicht authentifizierten noch mit einer authentifizierten Community-Zeichenfolge im Router übereinstimmt, wird das Paket vernichtet.
- Falls die Community-Zeichenfolge im Paket mit einer authentifizierten Community-Zeichenfolge im Router übereinstimmt, authentifiziert der Router das Paket.

2 Der Router berechnet den MD5-Hash-Wert mit dem Geheimsschlüssel, dem Magic Cookie, der Nutzzeit und der PDU. Falls der berechnete Hash-Wert nicht mit dem Hash-Wert im Paket übereinstimmt, vernichtet der Router das Paket ohne einen weiteren Hinweis.

3 Der Router vergleicht die Werte für Magic Cookie und Nutzzeit im Paket mit seinen eigenen Werten für Magic Cookie und Nutzzeit.

4 Falls die Cookie-Werte im Paket und im Router nicht genau übereinstimmen oder falls es einen Unterschied von mehr als 10 Sekunden zwischen den Nutzzeitwerten im Paket und im Router gibt, sendet der Router ein Antwortpaket mit folgendem Inhalt: der aktuelle Cookie-Wert des Routers, die aktuelle Nutzzeit, keine PDU (abgesehen von der Reihennummer, Errstat und ErrIndex) und ein Hash-Wert, der mit dem Geheimschlüssel, dem Magic Cookie, der Nutzzeit und der abgeschnittenen PDU errechnet wurde.

Der Wert für „ErrStat“ lautet 99 und weist auf einen “Antwortfehler” hin, und der Wert für „ErrIndex“ ist Null.

Das Antwortpaket enthält die aktuellen Cookie- und Nutzzeitwerte des Routers, damit der Absender der Anforderung die neuen Informationen in ein zukünftiges Paket integrieren kann. Der Absender der Anforderung erstellt ein neues Paket, das die aktualisierten Cookie- und Nutzzeitwerte sowie einen neuen (unterschiedlichen) Hash-Wert enthält. Dieses neue Paket sollte die Authentifizierung bestehen.

5 Der Router empfängt das neue Paket und vergleicht die darin enthaltenen, aktualisierten Werte und den neuen Hash-Wert.

6 Wenn ein Paket vom Router authentifiziert wurde, erstellt der Router die entsprechende SNMP-Antwort (z. B. aktualisierte „var-binds“ in „get-response“ usw.).

Der Router nimmt den Cookie-Wert und eine aktualisierte Kopie der Nutzzeit in das Paket auf, die es dem Absender des Pakets erlauben, seine Messung der Router-Nutzzeit mit der des Routers zu synchronisieren.

Konfigurieren der SNMP-Authentifizierung

Wenn Sie die SNMP-Authentifizierung konfigurieren wollen, müssen Sie die Community-Zeichenfolge für den Lese- und Schreibzugriff im Parameter „R/W_comm“ im Untermenü „SNMP Options“ des Ethernet-Profils eingeben. Die Community-Zeichenfolge für den Lese- und Schreibzugriff sollte folgendes Format haben:

name|*secretkey*

wobei:

- `name` für den Namen steht, den Sie der Community-Zeichenfolge für den Lese- und Schreibzugriff zuweisen wollen.
- `secretkey` für den alphanumerischen Schlüssel steht, der zur Authentifizierung verwendet wird.
- ein senkrechter Strich `name` und `secretkey` trennt.

Aufrufen von MPP-Sitzungsstatistiken mit „SNMP Get“

Gilt nur für die Pipeline 75 und 130. MPP-Sitzungsstatistiken erscheinen im Statusfenster „Dyn Stat“. Sie können diese Werte jetzt mit SNMP-Get-Anforderungen abrufen. „mppActiveStatsTable“ wurde zu „systemStatusGroup“ in Ascend MIB (.1.3.6.1.4.1.529.12) hinzugefügt und enthält die Objekte, die für eine SNMP-Get-Anforderung von Sitzungsstatistiken erforderlich sind.

MPP-Sitzungsstatistiken mit einer Get-Anforderung erhalten

Die Änderungen an der Benutzerschnittstelle wurden in den SNMP-Get-Anforderungen vorgenommen. Wenn Sie z. B. ein einfaches SNMP-Walk-Dienstprogramm verwenden, um eine Walk-Anforderung an der Objektkennung `.1.3.6.1.4.1.529.12.4` durchzuführen, entsprechen die daraufhin erhaltenen Wertesätze denjenigen, die auf der LCD-Anzeige im Fenster „Dyn Stats“ für eine MPP-Sitzung angezeigt werden. Einem Wertesatz wird eine MpID zugewiesen.

Hinweis: Bei einem `walk`-Dienstprogramm handelt es sich um eine Form einer `get next`-Anforderung, die mit dem Null-Index beginnt. Da der Null-Index nicht existiert (der Index beginnt mit 1), sendet das Dienstprogramm den ersten verfügbaren Index, bei dem es sich in der Regel um 1 handelt, zurück, und fährt damit fort, bis es keine verfügbaren Indizes mehr gibt.

Wertesätze als Ergebnis einer Get-Anforderung

Die in der folgenden Tabelle enthaltenen Werte erscheinen in einem Wertesatz, der das Ergebnis einer SNMP-`walk-` oder `get`-Anforderung bezüglich einer mppStatsMpID ist. Weitere Informationen zu diesen Parametern finden Sie im mit der Dokumentation gelieferten Referenzhandbuch.

Wert in mppStatsTable	Dyn Stats-Parameter	Beschreibung
mppStatsRemoteName	*Profil*	Name des Verbindungsprofils, das in der Pipeline für diese Verbindung eingerichtet wurde; erscheint in der ersten Zeile im Fenster „Dyn Stats“.
mppStatsQuality	Qual	In der zweiten Zeile im Fenster „Dyn Stats“ wird die Verbindungsqualität angezeigt. Mögliche Werte sind: „Good“, „Fair“, „Marg“, „Poor“ und „N/A“ (die Verbindung ist nicht online).
mppStatsStartingTimeStamp	*time*	Die Zeit, die die Verbindung bereits aktiv ist. Wenn eine Verbindung mehr als 96 Stunden online ist, wird die Dauer in Tagen angezeigt.
mppStatsBandwidth	*data rate*	In der dritten Zeile des Fensters „Dyn Stats“ wird die aktuelle Übertragungsgeschwindigkeit angezeigt.
mppStatsTotalChannels	*n* channels	Die Anzahl der Kanäle, für die die in mppStatsBandwidth angegebene Geschwindigkeit gilt.

Wert in mppStatsTable	Dyn Stats-Parameter	Beschreibung
mppStatsCLU	CLU *n*%	Current Line Utilization (aktuelle Leitungsnutzung).
mppStatsALU	ALU *n*%	Average Line Utilization (durchschnittliche Leitungsnutzung).

SNMP hilft, einen Ruf einem Gerät zuzuordnen

Gilt nur für Pipeline 130. Wenn ein Benutzer den Kundendienst-Support anruft und ein Problem mit einer Verbindung berichtet, kann das Management-Programm jetzt über SNMP das Gerät, bei dem der Benutzer angemeldet ist, isolieren.

Überblick

Ein neuer Parameter im Leitungsprofil weist einer T1-Leitung bis zu drei Hunt-Gruppen zu. Ein Netzwerk-Management-Programm kann diese Informationen über neue SNMP-Variablen aufrufen und eine Tabelle, die die Geräte und die Hunt-Gruppennummern enthält, in ihren WAN-Leitungsprofilen speichern. Wenn ein Benutzer ein Problem berichtet, kann anhand dieser Tabelle das Gerät isoliert werden, das der vom Benutzer angerufenen Hunt-Gruppennummer zugeordnet ist.

Konfigurieren der Hunt-Gruppennummern

1. Öffnen Sie das „Net/T1 Line“-Profil für eine Leitung, die einer Hunt-Gruppe zugewiesen ist.
2. Geben Sie in „Hunt-n #“ die Telefonnummern von bis zu drei Hunt-Gruppen ein, die der Rufprotokollierung zugeordnet werden sollen.

```
10-1** Factory
>Line 2...
 Hunt-1 #=
 Hunt-2 #=
 Hunt-3 #=
```

3 Speichern Sie die Änderungen.

Hunt-*n*#

Beschreibung: Gibt eine Hunt-Gruppe an (von 1 bis 3), die der T1-Leitung in einem bestimmten Leitungsprofil zugeordnet wurde. Ein SNMP-Manager kann diese Nummern von Ascend-Geräten abrufen und in einer Tabelle, die das Gerät, von dem die Informationen abgerufen wurden, und die Hunt-Gruppennummern enthalten, in ihren WAN-Leitungsprofilen speichern.

Verwendung: Geben Sie die Telefonnummer der Hunt-Gruppe, die der aktuellen Leitung zugewiesen wurde, im Parameter „Hunt-x #“ ein.

Beispiel: Hunt-1 #=847-4747

Abhängigkeiten: Die Nummern, die Sie als Werte für die Parameter „Hunt-n #“ eingeben, müssen identisch sein mit den Nummern, die den T1-Kanälen zugewiesen wurden.

Parameter-Ort: Net T1 Line Profile > Line Config

SNMP-Erweiterungen

Für „sysConfigTftpCmd { ascend systemStatusGroup sysConfigTftp 1 }“ können jetzt folgende Werte festgelegt werden:

- tsave (1): speichert die aktuelle Konfiguration in einer Datei. Es werden nur Parameterwerte gespeichert, die nicht den Standardwerten entsprechen.
- trestore (2): lädt eine gültige Konfiguration über TFTP aus einer Datei.
- tsave -a (3): speichert die aktuelle Konfiguration in einer Datei. Es werden alle Parameterwerte gespeichert, auch solche, die den Standardwerten entsprechen.
- tsave -m (4): speichert die aktuelle Konfiguration in einer Datei und verwendet dabei die MIB OID- statt der VT100-Schnittstellennamen. Es werden nur Parameterwerte gespeichert, die nicht den Standardwerten entsprechen.

- tsave -am (5), speichert die aktuelle Konfiguration in einer Datei und verwendet dabei die MIB OID- statt der VT100-Schnittstellennamen. Es werden alle Parameterwerte gespeichert, auch solche, die den Standardwerten entsprechen.

Folgende Werte gehen von den { mib-2 system sysObjectID } Pipeline-Identifizierungs-OIDs ein:

- { ascend products pipeline 5 } für Pipe50
- { ascend products pipeline 6 } für Pipe75
- { ascend products pipeline 7 } für Pipe130

Feste Schnittstellen erscheinen in SNMP IfTable zuerst

Feste Einheiten, z. B. Hardware-Einheiten, erscheinen in IfTable vor Software-Einheiten. Da in der MIB häufig auf IfNumber verwiesen wird, sehen andere Tabellen folgerichtiger als zuvor aus. Diese Änderung ist kompatible mit vorhergehenden MIB-Versionen, da es sich um statische Informationen handelt.

Administration

7

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie Ihre Einheit verwalten:

Anzeigen unerwünschter Wählpakete 7-2
Rufblockierung bei gescheiterten Verbindungen 7-8
Befehl „Traceroute“ zum Terminal-Server hinzugefügt 7-9
Neue Option „-a“ im Befehl „tsave“ 7-12
Neue Option „-m“ im Befehl „tsave“ 7-13
Größere Ausführungsdateien 7-15
Neue SNMP Traps für gescheiterte Telnet-Kennwortüberprüfungen 7-20
Befehl zum Anzeigen der Systemversion hinzugefügt 7-21
Mehr Informationen im Protokoll „Fatal Error“ 7-22
Benutzerdefinierbarer Anschluß für Syslog-Meldungen 7-24
Terminal-Server und Diagnosefunktionen 7-25
Einstellen der Systemuhr mit SNMP 7-26
Beenden von PPP-Rufen bei Authentifizierungs-Timeout 7-26
Konfigurieren eines Anschlusses für Syslog-Meldungen 7-27
TFTP prüft Kompatibilität geladener Dateien 7-28

Anzeigen unerwünschter Wählpakete

Mit einer neuen Diagnoseoption können Pakete erfaßt und angezeigt werden, die die Pipeline veranlassen, zu wählen. Sie können diese Daten dann verwenden, um Daten zu schreiben oder um Filter aufzurufen, mit denen die Pakete daran gehindert werden, unerwünschte Verbindungen herzustellen.

Mit dieser Erweiterung wird dem Diagnosemonitor die Option „wan-data dial-out (wdDialout)“ hinzugefügt.

Wenn Pakete nicht erfaßt werden

Falls aus einem der folgenden Gründe ein Wahlvorgang ausgelöst wird, wird ein Paket *nicht* von der Option „wdDialout“ erfaßt:

- Wählen verursacht durch Eingabe des Tastaturbefehls Strg-D
- Wählen verursacht von Rückrufsicherheit
- Wählen auf festen Kanälen
- Wählen von NAT (Network Access Translation), die eine IP-Adresse anfordert, verursacht
- Wählen für IP über X.25 initiiert, wenn sich das X.25-Internet-Profil in aktiv ändert und Daten darauf warten, daß X.25 die Verbindung herstellt wird
- Wählen von IGMP (Internet Group Management Protocol)-Multicast-Weiterleitung verursacht
- Wählen, um während der PPP-Verhandlungen eine DNS-Adresse zu erhalten
- Wählen in Reaktion auf eine DHCP-Discover-Meldung
- Wählen von der Pipeline verursacht, die ein DHCP-Paket zur Verarbeitung an einen DHCP-Client sendet
- Wählen in Reaktion auf eine APP (Ascend Password Protocol) Connect Request-Meldung

Aktivieren der Diagnoseoption

1 Rufen Sie den Diagnosemodus auf, indem Sie folgendes schnell eingeben:
Esc [Esc =

2 Geben Sie nach der Eingabeaufforderung „>“ folgendes ein:

`help ascend`

In der Regel müßten Sie jetzt die Option „wdDialout“ aufgelistet sehen. Als Standard ist die Option deaktiviert.

3 Wenn Sie die Option aktivieren wollen, geben Sie folgendes ein:

`wdDialout`

```
WANDATA dialout display is ON
```

Dabei handelt es sich um einen Umschaltbefehl, d. h. wenn Sie ihn erneut eingeben, deaktivieren Sie die Option. Nähere Informationen zur Anzeige von Paketen im Diagnosemonitor finden Sie im nächsten Abschnitt.

4 Wenn Sie den Diagnosemodus verlassen und zur VT100-Schnittstelle zurückkehren wollen, müssen Sie folgendes eingeben:

`quit`

Anzeige von Paketen

Die Ausgabe der Option „wdDialout“ erscheint im Diagnosemonitor. Dieser Abschnitt enthält mehrere Beispiele.

Beispiel 1

Im folgenden Beispiel wurden „Date“ und „Time“ der Pipeline weder durch einen vom Benutzer eingegebenen Befehl noch durch den SNTP-Server eingestellt. Daher sind Datum und Zeit im erfaßten Paket ungültig. Die nach dem Empfang dieses Pakets gewählte Nummer lautet 92233002.:

```
 Date: 01/01/1990.          Time: 00:00:53
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 42 octets @ 2C6950
  [0000]: ff ff ff ff ff ff 00 c0 7b 61 44 fe 08 06 00 01
  [0010]: 08 00 06 04 00 01 00 c0 7b 61 44 fe cc b2 d7 7b
  [0020]: 00 00 00 00 00 00 cc b2 d7 13

  [0000]: ff ff ff ff ff ff 00 80 c7 5b e9 5b 08 06 00 01
  [0010]: 08 00 06 04 00 01 00 80 c7 5b e9 5b cc b2 d7 13
  [0020]: 00 00 00 00 00 00 cc b2 d7 16 00 00 00 00 00 00
  [0030]: 00 00 00 00 00 00 00 00 00 00 00 00
```

Der Eintrag „type OLD-STYLE-PADDED“ bedeutet, daß das Paket über 14 Byte MAC (Ethernet)-Header + Datagramm (ARP-Anforderungsmeldung) verfügt. Das Paket enthält folgende Informationen:

```
destination MAC address   ff:ff:ff:ff:ff:ff
source MAC address        00:c0:7b:61:44:fe   /* 123 */
arp packet type           08:06
arp_hrd                   00:01               /* Ethernet 1 */
arp_prot                  08:00               /* IP=0x800 */
arp_hlen                  06                  /* hlen = 6 */
arp_plen                  04                  /* plen = 4 */
arp_op                    00:01               /* arp ARP_REQ */
arp_sha                   00:c0:7b:61:44:fe   /* 123 */
arp_spa                   cc:b2:d7:7b         /* 123 */
arp_tha                   00:00:00:00:00:00
arp_tpa                   cc:b2:d7:13         /* 19 */
```

Beispiel 2

In diesem Beispiel lautet die nach dem Empfang dieses Pakets gewählte Nummer 92233002. Der Eintrag „type OLD-STYLE-PADDED“ bedeutet, daß das Paket über 14 Byte MAC (Ethernet)-Header + Datagramm verfügt. Hierbei handelt es sich um eine Broadcast- IP-RWHO-Meldung:

```
Date: 01/01/1990.  Time: 00:00:56
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 198 octets @ 296810
  [0000]: ff ff ff ff ff ff 00 80 c7 5b e9 5b 08 00 45 00
  [0010]: 00 b8 0d c3 00 00 3f 11 24 fa cc b2 d7 13 cc b2
  [0020]: d7 ff 02 01 02 01 00 a4 e5 8a 01 01 00 00 32 46
  [0030]: 5e 26 00 00 00 00 63 6d 61 72 69 6e 65 72 00 00
  [0040]: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  [0050]: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  [0060]: 00 00 32 46 4a e3 74 74 79 63 32 00 00 00 72 79
  [0070]: 75 00 00 00 00 00 32 46 4b 35 00 00 02 59 74 74
  [0080]: 79 63 33 00 00 00 72 79 75 00 00 00 00 00 32 46
  [0090]: 4b 39 00 00 00 3d 74 74 79 63 34 00 00 00 72 79
  [00a0]: 75 00 00 00 00 00 32 46 4b 3e 00 00 00 97 74 74
  [00b0]: 79 70 30 00 00 00 72 79 75 00 00 00 00 00 32 46
  [00c0]: 5e 00 00 00 00 01
```

Das Paket enthält folgende Informationen:

```
destination MAC address   ff:ff:ff:ff:ff:ff
source MAC address        00:80:c7:5b:e9:5b
source IP adddress        cc:b2:d7:13       /* 204.178.215.19 */
destination IP address    cc:b2:d7:ff       /* 204.178.215.255
sub                                          network broadcast */
```

Beispiel 3

In diesem Beispiel lautet die nach dem Empfang dieses Pakets gewählte Nummer 92233002. Der Eintrag „type OLD-STYLE-PADDED“ bedeutet, daß das Paket über 14 Byte MAC-Header + Datagramm verfügt. Hierbei handelt es sich um eine Unicast-IP-ICMP-Echopaketmeldung:

```
Date: 01/01/1990.     Time: 00:01:13
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 98 octets @ 291EC8
  [0000]: 08 00 20 1f 5b ce 00 80 c7 5b e9 5b 08 00 45 00
  [0010]: 00 54 0e 09 00 00 ff 01 66 10 cc b2 d7 13 cc b2
  [0020]: d7 16 08 00 f5 1b bb 07 98 00 37 5e 46 32 3a 48
  [0030]: 0d 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
  [0040]: 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
  [0050]: 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
  [0060]: 36 37
```

Das Paket enthält folgende Informationen:

```
destination MAC address   08:00:20:1f:5b:ce
source MAC address        00:80:c7:5b:e9:5b
source IP address         cc:b2:d7:13      /* 204.178.215.19 */
destination IP address    cc:b2:d7:ff      /* 204.178.215.22 */
```

Beispiel 4

In diesem Beispiel lautet die nach dem Empfang dieses Pakets gewählte Nummer 917007337921. Beachten Sie, daß es keinen MAC-Header gibt. Hierbei handelt es sich um ein IPX-Paket: eine „Get Nearest Server Request“ mit „service type File Server (0004)“:

```
Date: 01/01/1990.        Time: 00:01:43
Cause an attempt to place call to 917007337921
WD_DIALOUT_DISP: chunk 261022 type IPX.
: 34 octets @ 2C6AA0
  [0000]: ff ff 00 22 00 11 00 00 00 00 ff ff ff ff ff ff
  [0010]: 04 52 00 00 00 00 00 a0 24 be d5 84 40 09 00 03
  [0020]: 00 04
```

Das Paket enthält folgende Informationen:

```
chksum            ff:ff
packet len        00:22       /* 34 */
Transport Control 00          /* 0 */
packet type        11          /* 17 NetWare Core Protocol Packet */
dest network      00:00:00:00
dest Node         ff:ff:ff:ff:ff:ff
dest Socket       04:52        /* Service Advertising Protocol*/
source network    00:00:00:00:00
source Node       00:a0:24:be:d5:84  /*physical addr of src Node*/
Source Socket     40:09         /*4000h-7fffh Dynamic socket*/
Sap operation     00:03         /* Get Nearest Server Request */
Sap Service Type  0:04          /* File Server */
```

Beispiel 5

In diesem Beispiel lautet die nach dem Empfang dieses Pakets gewählte Nummer 92233002. Der Eintrag „type OLD-STYLE-PADDED“ bedeutet, daß das Paket über 14 Byte MAC-Header + Datagramm verfügt:

```
Date: 01/01/1990.  Time: 02:40:35
Cause an attempt to place call to 92233002
WD_DIALOUT_DISP: chunk 260126 type OLD-STYLE-PADDED.
: 60 octets @ 2AE950
  [0000]: 00 80 5f 74 93 d5 00 80 c7 2f 32 4c 00 2a ff ff
  [0010]: 00 29 00 11 30 6c 6b 00 00 00 00 00 00 01 04 51
  [0020]: 82 c1 b6 bf 00 80 c7 2f 32 4c 40 03 22 22 3f 03
  [0030]: 01 00 16 00 02 15 01 ff ff ff ff ff
```

Das Paket enthält folgende Informationen:

```
destination MAC address   00:80:5f:74:93:d5
source MAC address        00:80:c7:2f:32:4c
chksum            ff:ff
packet len        00:29        /*41*/
packet type       11            /*17 NetWare Core Protocol Packet */
dest network      30:6c:6b:00
dest Node         00:00:00:00:00:01
dest Socket       04:51         /*NetWare Core Protocol (NCP Pkt)*/
source network    82:c1:b6:bf
source Node       00:80:c7:2f:32:4c  /* physical addr of src Node */
Source Socket     40:03             /*4000h-7fffh Dynamic socket*/
```

Rufblockierung bei gescheiterten Verbindungen

Betrifft nur die Pipeline 50 und 75. Sie können jetzt weitere Versuche, eine Verbindung herzustellen, blockieren, falls bereits eine bestimmte Anzahl von Versuchen gescheitert sind, und Sie können die Dauer der Rufblockierung festlegen.

Überblick

Wenn eine Verbindung scheitert, versucht die Pipeline weiterhin, die Verbindung herzustellen. Mit dieser Funktion können Sie festlegen, wie oft eine Pipeline erfolglos versuchen kann, eine Verbindung herzustellen, bevor weitere Versuche blockiert werden. Nachdem die angegebene Anzahl Versuche unternommen wurden und gescheitert sind, beginnt der Timer der Rufblockierung zu laufen. Die Pipeline blockiert alle Rufe (vernichtet Pakete) für die angegebene Dauer.

Konfigurieren der Rufblockierung

1. Öffnen Sie das Untermenü „Session options“ im Verbindungsprofil.
2. Legen Sie fest, wieviele Versuche die Pipeline zuläßt, indem Sie eine Zahl in „Block calls after=“ eingeben.
3. Legen Sie fest, wie lange die Pipeline Rufe blockiert, indem Sie eine Zahl in „Blocked duration=“ eingeben.

Parameterangaben

Zwei neue Variablen wurden dem Untermenü „Session“ im Verbindungsprofil zugefügt.

Block calls after

Beschreibung: Gibt an, wieviele erfolglose Versuche die Pipeline unternehmen kann, bevor weitere Rufe blockiert werden (Pakete werden vernichtet).

Verwendung: Geben Sie an, wieviele Versuche zur Herstellung einer Verbindung gestattet sind, bevor die Pipeline weitere Rufe blockiert (Pakete werden vernichtet). Das Maximum, das Sie eingeben können ist 65535 (65535 Versuche). Der Standardwert ist „0“.

Parameter-Ort: Untermenü „Session Options“ im Verbindungsprofil.

Siehe auch: Blocked duration

Blocked duration

Beschreibung: Gibt an, wieviele Sekunden die Pipeline Rufe blockiert (Pakete werden vernichtet).

Verwendung: Geben Sie die Anzahl Sekunden an, die die Pipeline alle Rufe für diese Verbindung blockieren soll. Nach Ablauf dieses Zeitraums gestattet die Pipeline wieder Rufe für diese Verbindung.

Parameter-Ort: Untermenü „Session Options“ im Verbindungsprofil.

Siehe auch: Block calls after

Befehl „Traceroute“ zum Terminal-Server hinzugefügt

Der Befehl „Traceroute“, der dem vorhandenen Terminal-Server-Befehl „Ping“ entspricht, wurde der Terminal-Server-Schnittstelle hinzugefügt. Sie können „Traceroute“ bei Netzwerktests, Messungen und Management verwenden. Er ist dazu geeignet, um langsame Router zu lokalisieren und um IP-Routing-Probleme zu diagnostizieren. Er ist verfügbar auf allen Plattformen, die über eine Terminal-Server-Schnittstelle und IP-Routing sowie Telnet oder Rlogin verfügen.

Hinweis: Der Befehl „Traceroute“ ist über die Terminal-Server-Schnittstelle verfügbar, falls „Telnet“ oder „Rlogin“ für abgehende Rufe aktiviert wurde, oder falls der Benutzer über Operations-Sicherheit verfügt.

Das Internet ist eine dicke und komplexe Ansammlung von Netzwerk-Hardware, die über Gateways miteinander verbunden ist. Es kann schwierig sein, die Route, die ein Paket nimmt, zu verfolgen oder das Gateway, das Ihre Pakete vernichtet, zu finden. Der Befehl „Traceroute“ verwendet das Feld „time to live“ im IP-Protokoll und versucht, von jedem Gateway auf dem Weg zu einem Host eine ICMP-Time-Exceeded-Antwort zu erhalten.

Der Befehl „Traceroute“ hat folgende Syntax:

```
traceroute [ -n ] [ -v ] [ -m max_ttl ] [ -p port ] [ -q nqueries
]
[ -w waittime ] host [ datasize ]
```

Hinweis: Der einzige obligatorische Parameter ist der Name des Ziel-Hosts oder die IP-Nummer.

Die Optionen sind:

-n	Druckt Hop-Adressen in numerischer an Stelle von symbolischer und numerischer Weise (verhindert, daß für jeden Gateway, der auf dem Pfad gefunden wird, eine Adresse-zu-Namen-Suche auf einem Nameserver durchgeführt wird).
-v	Umfangreiche Ausgabe. Alle empfangenen ICMP-Pakete mit Ausnahme von „Time Exceeded“ und „ICMP Port Unreachable“ werden aufgelistet.
-m *max_ttl*	Legt das Maximum für „time-to-live“ (maximale Anzahl Hops) in ausgehenden Testpaketen fest. Der Standardwert ist „30“.
-p *port*	Legt die Basis-UDP-Anschlußnummer, die in Tests verwendet wird, fest. Bei Verwendung des Befehls „Traceroute“ wird davon ausgegangen, daß keine anderen Einheiten an einem der UDP-Anschlüsse zwischen dem Quell- und dem Ziel-Host mithören (d. h. eine Meldung „ICMP-Port-Unreachable“ ergeht, um die Routenprüfung zu beenden). Falls eine Einheit an einem Anschluß im Standardbereich mithört, können Sie mit dieser Option einen unbenutzten Anschlußbereich auswählen. Der Standardwert ist „33434“.

-q *nqueries*	Legt die maximale Anzahl von Abfragen pro Hop fest. Der Standardwert ist „3“.
-w *waittime*	Legt fest, wie lange auf die Antwort auf eine Abfrage gewartet wird. Der Standardwert ist „3 seconds“.
host	Dieser obligatorische Parameter gibt den Namen oder die IP-Adresse des Ziel-Hosts an.
datasize	Legt fest, wie groß das Datenfeld im UDP-Test-Datagramm ist, das der Befehl „Traceroute“ abgesandt hat. Der Standardwert ist „0“. Dies ergibt eine Datagramm-Größe von 38 Byte (ein UDP-Paket, daß keine Daten enthält).

Hinweis: Die Optionen „-r“ und „-s“ (in der UNIX-Version von Traceroute vorhanden) werden nicht unterstützt.

Der Befehl „Traceroute“ versucht, die Route, die ein IP-Paket zu einem Internet-Host nehmen würde, zu verfolgen, indem er UDP-Testpakete mit einer geringen TTL (Time To Live) absendet und dann auf eine ICMP-Antwort “Time Exceeded” von einem Gateway wartet. Die Tests beginnen mit einer TTL von eins und werden um je eins gesteigert, bis eine ICMP-Meldung “Port Unreachable” eingeht (d. h. der Host wurde erreicht) oder die maximale TTL erreicht wird.

Es werden drei Tests pro TTL-Einstellung gesendet, und eine Zeile wird gedruckt, die die TTL, die Gateway-Adresse und die Rückkehrzeit pro Test enthält. Wenn Antworten von verschiedenen Gateways eingehen, wird die Adresse der jeweils antwortenden Systeme gedruckt. Falls keine Antwort innerhalb einer 3-sekundigen Timeout-Periode erfolgt, erscheint für diesen Test ein “*” im Ausdruck.

Da der Ziel-Host die UDP-Testpakete nicht verarbeiten soll, wird für den Ziel-Anschluß ein unwahrscheinlicher Wert, z. B. 33434, eingegeben.

In der folgenden Tabelle werden Anmerkungen aufgelistet, die nach dem Zeitfeld erscheinen können:

!H	Host wurde erreicht.
!N	Netzwerk nicht erreichbar.
!P	Protokoll nicht erreichbar.
!S	Quell-Route gescheitert. Dies sollte nicht auftreten und weist u. U. auf ein Problem mit dem zugehörigen Gerät hin.
!F	Fragmentierung ist erforderlich. Dies sollte nicht auftreten und weist u. U. auf ein Problem mit dem zugehörigen Gerät hin.
!h	Kommunikation mit dem Host wird durch Filterung verhindert.
!n	Kommunikation mit dem Netzwerk wird durch Filterung verhindert.
!c	Kommunikation wird anderweitig durch Filterung verhindert.
!?	Weist auf einen ICMP-Subcode hin. Sollte nicht auftreten.
!??	Antwort mit unpassendem Typ empfangen. Sollte nicht auftreten.

Neue Option „-a“ im Befehl „tsave“

Wenn Sie die Befehlsoption „tsave -a“ verwenden, erhalten Sie eine Liste aller Parametereinstellungen. Sie müssen auf einen UNIX-Host mit einem TFTP-Server zugreifen, wenn Sie „tsave -a“ verwenden wollen. Wenn Sie die Liste erstellen wollen, müssen mit „Telnet“ auf die Pipeline zugreifen. Geben Sie „Strg-D“ ein, um das DO-Menü aufzurufen und wählen Sie „D=Diagnostics“. Geben Sie den Befehl am Terminal-Server mit folgender Syntax ein:

```
tsave -a nnn.nnn.nnn.nnn file.name
```

Die einzelnen Elemente haben folgende Bedeutung:

-a	Listet alle Menüelemente in der Software für die Einheit auf.
nnn.nnn.nnn.nnn	Die lokale IP-Adresse eines UNIX-Hosts mit einem TFTP-Server.
file.name	Der Name einer leeren Datei, die Sie zuvor im TFTP-Boot-Verzeichnis des UNIX-Hosts erstellt haben. Stellen Sie sicher, daß Sie über Lese- und Schreibberechtigung für diese Datei verfügen. (Probleme treten meist im Zusammenhang mit mangelnden Lese-/Schreibberechtigungen auf.) Die Ausgabedatei wird im TFTP-Boot-Verzeichnis des UNIX-Hosts gespeichert.

Neue Option „-m“ im Befehl „tsave“

Die Textkonfigurationsdatei, die Sie mit dem Befehl „tsave“ erstellen können, enthält als Standard die Parameternamen der VT-100-Schnittstelle. Dem Befehl „tsave“ wurde die neue Option „-m“ hinzugefügt, damit Sie die Konfigurationsdatei mit den MIB-Feldnummern anstelle der Parameternamen speichern können.

Hinweis: Die Dateien, die mit den Befehlen „tsave“ und „tsave -m“ erstellt wurden, können mit dem Befehl „trestore“ wiederhergestellt werden.

Alle Ascend-Produkte unterstützen diese neue Option.

Wenn Sie den Befehl „tsave“ verwenden wollen, müssen Sie zuerst den Diagnosemodus aufrufen, indem Sie schnell die folgenden vier Zeichen eingeben:

```
Esc [ Esc =
```

Um die Konfiguration der Pipeline mit den MIB-Feldnamen anstelle der Parameternamen zu speichern, müssen Sie die folgende Befehlszeile eingeben:

tsave -m <ipaddr> <filename>

Sehen Sie sich folgendes Beispiel an:

tsave -m 200.253.164.100 all

Mit dieser Befehlszeile speichern Sie die gesamte Konfiguration der Pipeline mit IP-Adresse 200.253.164.100 in einer „all“ genannten Datei.

Die Werte werden im folgenden Format gespeichert:

OOOO:MMMM.FFFF

wobei

- OOOO für die Nummer des Auftretens (Occurrence) steht (falls > 0),
- MMMM für den MIB-Typ steht (falls > 0),
- FFFF für die MIB-Feldnummer steht (falls MMMM > 0).

Beispiel

Die folgende Textdatei ergab sich, nachdem der Befehl „tsave“ an einem Mustersystem durchgeführt wurde:

```
START=FILT=900=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=900=0
```

Wenn der Befehl „tsave -m“ verwendet wird, ergibt sich folgende Datei:

```
START=FILT=900=0
54.1=IP Call
1:54.2,55.1=Yes
1:54.3,55.1=Yes
1:54.3,1:55.4,55.2=Yes
1:54.3,1:55.5,55.2=Yes
```

```
END=FILT=900=0
```

Sehen Sie sich folgendes Beispiel an:

```
1:54.3,1:55.5,55.2=Yes (Out filter
01...Ip...Forward=Yes)
```

[Out Filter] Bezeichnet das erste Auftreten des Out-Filter-Arrays; „Out filter 01...“ gehört zum 54. MIB-Typ; es ist das dritte Feld in diesem MIB-Typ. Dadurch ergibt sich die MIB-Kennung „1:54.3“.

[IP] Bezeichnet das erste Auftreten eines IP-Filters; „IP...“ gehört zum 54. MIB-Typ; es ist das 5. Feld in diesem MIB-Typ. Dadurch ergibt sich die MIB-Kennung „1:55.5“.

[Forward] Es gibt kein mehrfaches Auftreten dieses Felds, daher ist die Nummer des Auftretens „0“; „Forward“ gehört zum 55. MIB-Typ; es ist das 2. Feld in diesem MIB-Typ. Dadurch ergibt sich die MIB-Kennung „55.2“.

Alle drei MIB-Kennungen werden dann zu einer (durch Kommas getreten) MIB-Kennung zusammengefaßt: 1:55.3,1:55.5,55.2.

Größere Ausführungsdateien

Dank eines neuen Systems zum Laden größere Systemausführungsdateien können Sie „tloadcode“ und „TFTP“ aus dem Diagnosemonitor verwenden. Bisher verhinderten die redundanten Ausführungsdateien, die in der „unteren“ und „oberen“ Hälfte der Flash-Memory gespeichert wurden, Systemausführungsdateien, die größer als 448 KB waren.

Laden einer dicken Systemausführungsdatei

Eine Ausführungsdatei wird dann als „dick“ bezeichnet, wenn sie eine komprimierte Größe von 448 KB für die Pipeline überschreitet. Diese Systemausführungsdateien erfordern spezielle Ladeverfahren, die unten beschrieben werden.

Laden einer dicken Ausführungsdatei

Eine dicke Systemausführungsdatei kann nur mit dem Befehl „tloadcode“ (TFTP) des Diagnosemonitors geladen werden. Dicke Ausführungsdateien können nicht über den Konsolenanschluß geladen werden.

Eine ältere Ausführungsdatei, die kleiner als das Maximum von 448 KB ist, kann nach wie vor in der gleichen Weise geladen werden. Sie werden als „dünne“ Ausführungsdateien bezeichnet.

Falls Ihre Einheit z. Z. eine Systemversion für „dünne“ Ausführungsdateien verwendet, die nicht für dicke Ausführungsdateien geeignet ist, müssen Sie sie zuerst aktualisieren, damit sie für dicke Ausführungsdateien geeignet ist. Es empfiehlt sich, eine Sicherungskopie der dünnen auf dem PC anzulegen, falls eine dicke Ausführungsdatei scheitert. Siehe „Laden einer dünnen, für dicke Ausführungsdateien geeigneten Systemausführungsdatei“ auf Seite 7-17.

Laden einer für dicke Ausführungsdateien geeigneten Systemausführungsdatei mit TFTP:

1 Greifen Sie über die Telnet-Schnittstelle auf den Diagnosemonitor zu, indem Sie die folgenden Zeichen in schneller Abfolge eingeben:

`Esc [ Esc = (or Control "d",` wählen Sie dann `"D-diag")`

2 Geben Sie nach der Eingabeaufforderung „>“ folgendes ein:

`tloadcode` *`Host-Name Dateiname`*

Dabei steht „Host-Name“ für den Namen oder die IP-Adresse Ihres TFTP-Servers, und „Dateiname“ steht für den Namen der Systemsoftware auf dem Server.

Beispielsweise werden Sie mit dem Befehl:

```
tloadcode tftp-server ascend.bin
```

die Software „ascend.bin“ vom Gerät „tftp-server“ in die Flash-Memory laden. Die aktuelle Konfiguration wird vorsichtshalber ebenfalls in Flash-Memory gespeichert, bevor der neue Code empfangen wird.

3 Verschiedene Meldungen können angezeigt werden:

Die folgende Meldung wird mit der Standard-Übertragungsgeschwindigkeit 9600 bit/s angezeigt, falls die Ausführungsdatei dünn ist:

```
UART initialized
thin load: inflate
..................................................
```

```
starting system...
```

Die folgende Meldung wird mit der Standard-Übertragungsgeschwindigkeit 9600 bit/s angezeigt, falls es sich um eine dicke Ausführungsdatei handelt:

```
UART initialized
fat load: inflate
.................................................
starting system...
```

Damit ist das Laden des Codes abgeschlossen, falls keine Fehler auftreten.

Laden einer dünnen, für dicke Ausführungsdateien geeigneten Systemausführungsdatei

Falls bei einer dicken Ausführungsdatei ein CRC-Fehler (Cyclic Redundancy Check = Zyklische Redundanzprüfung) auftritt, erscheint die folgende Meldung:

```
UART initialized
fat load: bad CRC!!
forcing serial download at 57600 bps
please download a "thin" system...
```

Sofort im Anschluß an diese Meldung wird die Übertragungsgeschwindigkeit der seriellen Konsole auf 57600 bit/s umgeschaltet, und die Steuerung wird auf die serielle Xmodem-Laderoutine des Boot-ROM übertragen. Um nach diesem Fehler eine Wiederherstellung durchzuführen und um die dicke Systemausführungsdatei zu laden, müssen Sie eine dünne Systemausführungsdatei laden, die für dicke Ausführungsdateien geeignet ist. Diese dünne Ausführungsdatei ist hier erforderlich, da der Boot-ROM nichts über das neue, dicke Ausführungsdateienformat bekannt ist und nur die herkömmliche, dünne Ladung unterstützt. Bei dieser dünnen Ausführungsdatei handelt es sich wahrscheinlich nicht um das System, das sie tatsächlich ausführen werden, aber es muß zur Vorbereitung zuerst geladen werden, um dann die gewünschte, dicke Systemausführungsdatei mit dem befehl „tloadcode“ über das Ethernet laden zu können.

1. Rufen sie die Xmodem-Software auf, um die dünne Ausführungsdatei über den Konsolenanschluß zu laden.
2. Starten Sie den Ladevorgang einer dünnen Ausführungsdatei mit dem Befehl „tloadcode“.

   ```
   >>>> tloadcode:
   ```

Die Ausgabe von „tloadcode“ wurde leicht geändert. Wenn Sie eine herkömmliche dünne Ausführungsdatei laden, erscheint folgendes auf dem Diagnosemonitor:

```
> tload yourmachinename /loads/newload.bin
saving config to flash


.....................................
.
loading code from nnn.nnn.nnn.nnn:nn
file /loads/newload.bin...
thin load:
.....................................................................
.............
```

Newload ist der Name der binären Datei, die Sie zu laden versuchen. Die Änderung ist die Hinzufügung der Zeile “thin load:” zwischen dem Dateinamen und der langen Reihe mit Punkten.

3 Nachdem der Ladevorgang abgeschlossen ist, müssen sie die Einheit erneut starten.

4 Starten Sie den Ladevorgang einer dicken Ausführungsdatei mit dem Befehl „tloadcode“.

Wenn Sie eine dicke Ausführungsdatei laden, erscheint folgendes auf dem Diagnosemonitor:

```
> tload yourmachinename /loads/newload.bin
saving config to flash
.....................................
loading code from nnn.nnn.nnn.nnn:nnn
file /loads/newload.bin...
fat load part 1:
.....................................................................
..............
fat load part 2:
.........................................
```

Beachten Sie die Meldungen „fat load part *x*:“. Hier wird Ihnen mitgeteilt, wenn die erste und zweite Hälfte der dicken Ausführungsdatei geladen wird.

Hinweis: In seltenen Fällen kann ein Kunde über eine aus einer Engineering-Version stammende, dicke Ausführungsdatei verfügen, die in einem älteren Format geschrieben wurde. Der Befehl „tloadcode“ stellt das veraltete Format automatisch fest und wird sich weigern den Ladevorgang durchzuführen. Ein Meldung, die der folgenden ähnelt wird angezeigt:

```
> tload squiddly /loads/mhpt1bri-moldy.bin
saving config to flash
.....................................
loading code from nnn.nnn.nnn.nnn:nnn
file /ascend/mb4/rtr/mhpt1bri/mhpt1bri-fatty.bin...
obsolete fat load format--discarding downloaded data...
------------------------------------------------------------
-----------------
```

Zukünftig nicht unterstützte Ausführungsdateien

Falls Sie zukünftig versuchen, eine Systemausführungsdatei zu laden, die nicht das mir dieser Version eingeführte Format für dicke Ausführungsdateien verwendet, wird die Ausführungsdatei abgelehnt, falls Ihr System das neue Format nicht unterstützt.

```
> tload yourmachinename /loads/oldload-moldy.bin
saving config to flash

.....................................

loading code from 192.168.1.82:69
file /ascend/mb4/rtr/mhpt1bri/oldload-fatty.bin...
incompatible fat load format--discarding downloaded data
```

Neue SNMP Traps für gescheiterte Telnet-Kennwortüberprüfungen

Diese Funktion teilt die IP-Adresse eines Telnet-Clients mit, dessen Anmeldeversuch gescheitert ist. Die Adresse ist in der Meldung zu Sicherheitsverletzungen enthalten, die immer dann ausgegeben wird, wenn die Höchstzahl von Telnet-Anmeldungsversuchen bei einer Pipeline überschritten wurde.

Änderungen an der Trap Meldung

Wenn Sie sich über Telnet bei einer Pipeline anmelden wollen, müssen Sie das entsprechende Kennwort eingeben, das dann überprüft wird. Falls Sie nicht das korrekte Kennwort eingeben, wird eine SNMP-Trap an alle SNMP-Clients gesandt, die SNMP-Sicherheitsmeldungen empfangen können.

Die Meldung beinhaltet folgende Informationen:

- Die Sitzungsnummer der versuchten Telnet-Sitzung.
- Die IP-Adresse des Host (die Pipeline).
- Die zugehörige IP-Adresse des Telnet-Clients, der versuchte, die Verbindung zu erstellen.

Die Meldung hat folgendes Format:

```
mm.mmm.mmm.mmm  Enterprise Specific Trap (15) Uptime: xx:xx:xx
Name.iso.org.dod.internet.private.enterprises.ascend.sessionStatus Group.
IpAddress: ttt.ttt.ttt.ttt
sessionStatusTable.sessionStatusEntry.ssnStatusUserIPAddress%d
```

Dabei haben die Elemente folgende Bedeutung:

`mmm.mmm.mmm.mmm`	IP-Adresse des Hosts
`ttt.ttt.ttt.ttt`	IP-Adresse des Telnet-Clients
%d	Nummer der versuchten Telnet-Sitzung

Diese SNMP Trap Meldung gab es bereits in der Trap Liste als Scheitern der Authentifizierung (RFC-1215 Fangstellentyp 4). Ein SNMP Trap gibt beim Scheitern der Authentifizierung an, daß es sich bei der Pipeline, die die Trap Meldung sendet, um den Adressaten einer Protokollmeldung handelt, die nicht korrekt authentifiziert wurde. Als einzige Änderung wurde der SNMP Trap die IP-Adresse der Station hinzugefügt, bei der die Authentifizierung gescheitert ist.

Befehl zum Anzeigen der Systemversion hinzugefügt

Den Befehlszeilenoptionen für den Befehl „Show“ des Terminal-Servers wurde der Befehl „Show Revision“ hinzugefügt.

Der Befehl „Show Revisions“

Mit dem Befehl „show revision“ werden der Systemtyp und Informationen zur Version des Systems, das gerade auf der Pipeline ausgeführt wird, angezeigt, und zwar u. a.:

- Systemname
- Build-Name
- Versionsnummer der geladenen Software

Wenn Sie in der Befehlszeile den Befehl

```
show revision
```

eingeben, werden die angezeigten Informationen den folgenden ähneln:

```
Pipeline system revision: mhpt1bip 4.6Bp10
```

Hilfe für Befehl „show“ beinhaltet „show revision“

Sie können eine Liste der Optionen, die mit dem Befehl „show“ verfügbar sind, anzeigen. Wenn Sie die Hilfe zum Befehl „show“ aufrufen, indem Sie in der Befehlszeile

```
show ?
```

eingeben, beinhaltet die daraufhin angezeigte Liste der Optionen den neuen Befehl „show revision“:

```
show revision       Display system revision.
```

Mehr Informationen im Protokoll „Fatal Error“

Das Protokoll „Fatal Error“ zeigt jetzt detailliert an, warum ein System zurückgesetzt wurde und beschreibt das Zurücksetzen nicht mehr als „fatal error“.

Beschreibungen des Zurücksetzens

Bisher wurde das Zurücksetzen eines Systems im Protokoll „Fatal Error“ nicht als Zurücksetzen aufgelistet, sondern als unkorrigierbarer Abbruchfehler; es wurden auch keine Gründe für das Zurücksetzen genannt. Jetzt zeigt das Protokoll ein Zurücksetzen als solches an und nennt den Grund dafür.

Beispiel: Zurücksetzen über einen NVRAM-Befehl

Falls Sie eine Einheit mit dem Diagnosebefehl „NVRAMCLEAR“ zurücksetzen, sieht die Ausgabe in etwa folgendermaßen aus:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
        Date: 08/04/1996.       Time: 22:31:19
        NVRAMCLEAR Reset from unknown in security
profile 1.
OPERATOR RESET:  Index: 99   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:32:23
        NVRAM was rebuilt
```

```
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Beispiel: „RESET“ über den Diagnosebildschirm

Falls Sie den Diagnosebefehl „RESET“ verwenden, sieht die Ausgabe in etwa folgendermaßen aus:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
        Date: 08/04/1996.       Time: 22:32:23
       DEBUG Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Beispiel: Zurücksetzen über „Sys Reset“

Falls Sie „Sys Reset“ aus dem Untermenü „Sys Diag“ im Systemprofil wählen, sieht die Ausgabe in etwa folgendermaßen aus:

```
OPERATOR RESET:  Index: 99   Revision: 4.6Bp10
        Date: 08/04/1996.       Time: 22:32:23
        MENU Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100   Revision: 4.6Be0
        Date: 08/04/1996.       Time: 22:33:00
```

Ausnahmen bei Meldungen

Falls in NVRAM nur eine Meldung gestattet ist, erscheint die Meldung „SYSTEM IS UP“ nicht.

Benutzerdefinierbarer Anschluß für Syslog-Meldungen

Sie können den Zielanschluß auf einem Syslog-Host, über den die Syslog-Meldungen einer Ascend-Einheit empfangen werden, angeben. Syslog-Meldungen umfassen Warnungen, Hinweise und CDR-Datensätze aus den lokalen Systemprotokollen der Einheit. Die Ascend-Einheiten können unterschiedliche Anschlüsse angeben, wodurch der Host mehrere Einheiten verwalten kann. Bisher wurde davon ausgegangen, daß der Syslog-Host den bekannten Anschluß 514 verwendet.

Log Port

Beschreibung: Gibt den Zielanschluß auf einem Syslog-Host, über den die Syslog-Meldungen einer Ascend-Einheit empfangen werden, an.

Syslog-Meldungen umfassen Warnungen, Hinweise und CDR-Datensätze aus den den lokalen Systemprotokollen der Einheit.

Die Ascend-Einheiten können unterschiedliche Anschlüsse angeben, wodurch der Host mehrere Einheiten verwalten kann.

Verwendung: Wählen Sie den Parameter „Log Port“, und geben Sie eine Anschlußnummer ein. Beim „Log Port“ handelt es sich um den Anschluß auf dem Syslog-Host, über den die Meldungen empfangen werden. Der Standardwert ist „514“.

Abhängigkeiten: Für den Parameter „Syslog“ müssen Sie den Wert „Yes“ festgelegt haben. Der Parameter „Log Host“ muß die IP-Adresse der Station enthalten, die die Syslog-Meldungen empfangen wird.

Parameter-Ort: Ethernet > Mod Config > Log

Siehe auch: Syslog, Log Host

Terminal-Server und Diagnosefunktionen

Dem Do-Menü wurden die zwei neuen Optionen „Termsrv“ und „Diagnostics“ hinzugefügt. Zuvor konnte auf die Funktionen, die diese Optionen bieten, nicht über die Menüschnittstelle zugegriffen werden.

Zugreifen auf die neuen Parameter

Dem Do-Menü wurden die zwei neuen Elemente „E=Termsrv“ und „D=Diagnostics“ hinzugefügt. Die im Benutzerprofil festgelegten Berechtigungen bestimmen, ob diese Optionen einem Benutzer zur Verfügung stehen.

Betätigen Sie Strg-D, um das DO-Menü anzuzeigen:

```
Main Edit Menu
DO...
0=Esc
P=Password
C=Close TELNET
E=Termsrv
D=Diagnostics
```

Zugreifen auf den Terminal-Server in anderen Menüs

Die Option „DO E“ im Menü „Main Edit DO“ erfüllt die gleiche Funktion wie die Option „Term Serv“ im Menü „Sys Diag“.

Zugreifen auf den Terminal-Server mit Tastaturbefehlen

Mit der folgenden Serie von Tastaturbefehlen können Sie auf den Terminal-Server zugreifen:

<Esc> [<Esc> 0

Einstellen der Systemuhr mit SNMP

Der Ascend MIB wurde ein Objekt hinzugefügt, damit Sie die Systemuhr mit SNMP einstellen können.

Beenden von PPP-Rufen bei Authentifizierungs-Timeout

Falls eine Authentifizierung auf einer PPP-Verbindung aufgrund eines falschen Kennworts oder eines Authentifizierungs-Server-Timeouts scheitert, beendet die Pipeline standardmäßig die PPP-Verbindung taktvoll, indem sie dem einwählenden Benutzer eine LCP-CLOSE-Anforderung sendet. Wenn Windows 95 diese Anforderung während einer Authentifizierung empfängt, geht es von einem abgewiesenen Kennwort aus. Daraufhin wird eine Meldung angezeigt, die dem Benutzer mitteilt, daß das Kennwort ungültig ist.

Disc on Auth Timeout

Beschreibung: Hiermit können Sie festlegen, ob die Pipeline PPP-Verbindungen nach einem Authentifizierungs-Timeout taktvoll beendet.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen „Yes“ und „No“ umzuschalten.

- „Yes“ gibt an, daß die Pipeline die PPP-Verbindungen nach einem Authentifizierungs-Timeout nicht sauber beendet, sondern einfach auflegt.
- „No“ gibt an, daß die Pipeline eine Verbindungen nach einem Authentifizierungs-Timeout taktvoll beendet wird.

  Der Standardwert ist „No“.

Abhängigkeiten: Falls „If PPP=No“ festgelegt wurde, dann ist „Disc on Auth Timeout“ nicht zutreffend.

Parameter-Ort: Antwortprofil: Ethernet > Answer > PPP Options

Siehe auch: PPP

Konfigurieren eines Anschlusses für Syslog-Meldungen

Um Ihnen mehr Flexibilität bei der Steuerung von Anschlüssen in einem Syslog-Host zu gewähren, können Sie jetzt angeben, über welchen Anschluß ein entfernter Syslog-Host die Syslog-Meldungen von einer Pipeline empfängt. Mit dieser Funktion können Sie mehrere Kopien des Syslog-Dämons auf dem Syslog-Host ausführen, während Pipelines Syslog-Meldungen an verschiedene Anschlüsse senden.

Überblick

Sie können jetzt angeben, über welchen Anschluß ein entfernter Syslog-Host die Syslog-Meldungen von einer Pipeline empfängt. Syslog-Meldungen umfassen Warnungs-, Hinweis- und CDR (Call Data Reporting)-Datensätze aus den lokalen Systemprotokollen, die an den Syslog-Host gesandt werden. Beim „Log Host“ handelt es sich um die Station, an die die Pipeline Systemprotokollmeldungen sendet, und beim „Log Port“ handelt es sich um den Anschluß des Syslog-Hosts, über die der Host diese Meldungen empfängt.

Bisher wurde immer davon ausgegangen, daß der Syslog-Host die Meldungen über einen bekannten Anschluß (Anschluß 514) empfängt. Es war nicht möglich, einen anderen Anschluß festzulegen.

Konfigurieren des „Log Port“

1 Öffnen Sie „Ethernet > Mod Config“.

```
90-C00 Mod Config
 Log...
  Syslog=Yes
  Log Host=206.65.212.205
  >Log Port=514
  Log Facility=Local0
```

2 Achten Sie darauf, daß „Syslog“ aktiviert und für „Log Host“ eine IP-Adresse angegeben wurde.

3 Wählen Sie „Log Port“, und geben Sie die Anschlußnummer ein, über die der Syslog-Host die Meldungen von dieser Pipeline empfangen soll.

Der Standardanschluß ist Anschluß 514.

4 Schließen Sie das Menü „Mod Config“, und speichern Sie die Änderungen.

TFTP prüft Kompatibilität geladener Dateien

Ab dieser Version vergleicht die Pipeline die Software, die mit dem Befehl „TFTP“ geladen werden soll, mit der aktuell geladenen Software. Falls die Plattform oder Netzwerkschnittstelle nicht übereinstimmt, bricht die Pipeline den Ladevorgang ab und zeigt an, warum der Abbruch erfolgte. Die Pipeline wird diese Prüfung umgehen, falls Sie den Befehl „TFTP“ mit dem Flag „-f“ verwenden.

Diese Funktion schützt Sie davor, aus Unwissenheit Software zu laden, die mit Ihrer Pipeline nicht kompatibel ist. Bisher konnten Sie eine beliebige Software auf einer beliebigen Pipeline laden. Der Versuch, eine nicht kompatible Software zu laden, scheiterte, und die zuvor geladene Software wurde wiederhergestellt, aber Sie erhielten keine Hinweise darauf, warum der Ladevorgang gescheitert war.

Die Überprüfung wird von der aktuell geladenen Software initiiert. Falls die Pipeline eine Version der Software verwendet, die diese Funktion bietet und Sie versuchen, eine ältere Version der Software zu laden, die nicht über diese Funktion verfügt, wird der Ladevorgang abgebrochen. Der Abbruch erfolgt, weil die ältere Software nicht über die Plattformkennungen verfügt, die die aktuell geladene Software zur Kompatibilitätsprüfung verwendet. In diesem Fall müssen Sie den Befehl „TFTP“ mit dem Flag „-f“ verwenden, damit die Pipeline keine Kompatibilitätsprüfung durchführt und die ältere Software lädt.

Beispiele

Im folgenden Beispiel versucht ein Benutzer, eine Pipeline 50-Software (b.p50) mit dem Befehl „TFTP“ auf einer neueren Pipeline 75 zu laden, auf der die Software „b.v2p75“ ausgeführt wird:

1 Der Benutzer ruft den Diagnosebildschirm über die VT100-Schnittstelle auf.

2 Er gibt folgenden Befehl ein:

```
tloadcode tftpserver.ascend.com b.p50
```

3 Die Pipeline 75 zeigt folgende Informationen auf dem Bildschirm an:

```
saving config to flash

.....................................
.
loading code from tftpserver.ascend.com
file /tftpboot/b.p50...
thin load:
This load appears to be for another platform.
This load appears not to support your network interface
Download aborted. Use 'tloadcode -f' to force.
```

Die Pipeline 75 hat die zu ladende Datei b.p50 mit der aktuell geladenen Datei „b.v2p75“ verglichen. Die Meldung gibt an, daß der Benutzer versuchte, eine nicht kompatible Plattform und eine nicht kompatible Netzwerkschnittstelle zu laden.

Im folgenden Beispiel versucht ein Benutzer, eine alte Version der Software (die nicht diese Funktion aufweist) mit dem Befehl „TFTP“ auf einer Pipeline 75, die über diese Funktion verfügt, zu laden:

1 Der Benutzer ruft den Diagnosebildschirm über die VT100-Schnittstelle auf.

2 Er gibt folgenden Befehl ein:

```
tloadcode tftpserver.ascend.com b.p50
```

3 Die Pipeline 75 zeigt folgende Informationen auf dem Bildschirm an:

```
saving config to flash

.....................................
.
loading code from tftpserver.ascend.com
file /tftpboot/b.p50...
thin load:
```

```
This load has no platform identifier. Proceed with caution.
Download aborted. Use 'tloadcode -f' to force.
```

Im vorhergehenden Beispiel entscheidet der Benutzer, daß er oder sie die ältere Version benötigt und erzwingt, daß sie geladen wird.

1 Der Benutzer gibt folgenden Befehl ein:

```
tloadcode -f tftpserver.ascend.com b.p50
```

2 Die Pipeline 75 zeigt folgende Informationen auf dem Bildschirm an:

```
Download forced by user...
..................................................
..................................................
..................................................
>
```

Falls Sie eine ältere Softwareversion auf einer neueren Pipeline 50 oder 75 laden, wird die Einheit deaktiviert, und Sie müssen sie an Ascend zurücksenden, um sie neu einrichten zu lassen.

Pipeline 75 Sprachfunktionen

A

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie die Sprachfunktionen der Einheit verwenden:

Statusanzeige für Sprachrufe A-2
WAN LED leuchtet bei Sprachrufen A-2
Unterstützt einen 2-Kanalruf auf einem SPID A-3
Konferenzschaltung A-4
CallerID unterstützt A-5
IDSL-Unterstützung für Sprachrufe von Pipeline 75 oder TA A-5
Unterstützung für ausgehende 3,1K-Audiorufe hinzugefügt A-9

Statusanzeige für Sprachrufe

Betrifft nur Pipeline 75. Im Statusfenster „10-100“ der Pipeline oder Pipeline 75 wird angezeigt, ob ein Sprachruf gehalten wird. Eine Beschreibung folgt im nächsten Abschnitt.

Überwachen von Telefonverbindungen

Das Statusmenü „10-100“ zeigt an, ob einer oder beide B-Kanäle für die ISDN-Leitung verwendet werden. Ein „*“ rechts von B1 oder B2 gibt an, daß der Kanal entweder für einen Sprach- oder Datenruf verwendet wird. Der Buchstabe „h“ gibt an, daß ein Sprachruf gehalten wird. Der Buchstabe „D“ gibt an, daß ein Ruf gewählt wird.

Im folgenden Beispiel wird B1, der erste B-Kanal, verwendet.

```
10-100 1
 Link  D
 B1    *
 B2
```

Im folgenden Beispiel wird auf B2, dem zweiten B-Kanal, ein Sprachruf gehalten, und es gibt darauf einen aktiven Sprachruf.

```
10-100 1
 Link  D
 B1
 B2    h *
```

WAN LED leuchtet bei Sprachrufen

Betrifft nur Pipeline 75. Die WAN LED auf der Vorderseite der Pipeline 75 leuchtet auf, wenn die ISDN-Leitung für einen Sprach- oder Datenruf verwendet wird.

Unterstützt einen 2-Kanalruf auf einem SPID

Betrifft nur Pipeline 75. Dank dieser Funktion können Kunden, die AT&T 5ESS NI-1 benutzen, denselben CES (Channel Endpoint Suffix) für einen 2-Kanalruf (ein Sprach- und ein Datenruf) auf demselben SPID (Service Provider Identifier) wiederverwenden. Diese Funktion ist für Kunden, die DMS-100 NI-1 benutzen, nicht verfügbar.

Derselbe CES kann unter folgenden Umständen wiederverwendet werden, um 2-Kanalrufe zu unterstützen (diese Informationen beziehen sich auf die Bereitstellung der Leitung):

- Es handelt sich um einen Datenruf auf einem bestimmten CES.
- „Phone Number Binding=Yes“ wurde festgelegt und bei dem neuen Rufversuch handelt es sich um einen Sprachruf über eine bestimmte CES, die einem Datenruf zugeordnet ist.

Diese Funktion ist für DMS-Benutzer nicht verfügbar, da die oben genannten Rufversuche von DMS-100 NI-1 abgelehnt werden.

Konfigurieren für 2-Kanalrufe mit einem SPID

Es wurden keine Änderungen an der Benutzerschnittstelle vorgenommen, um diese Funktion zu unterstützen, aber Sie müssen die Parameter im Profil „Configure“ folgendermaßen festlegen:

Parameter	**Erforderliche Einstellung**
My Num A	Gültige Telefonnummer (die gleiche wie in einer standardmäßigen NI-1-Konfiguration mit 2 SPID)
SPID 1 *oder* SPID 2	Einer der SPID-Parameter muß einen gültigen SPID aufweisen. Dieser Wert wird automatisch zum anderen SPID-Parameter kopiert.
Data Usage	Sie müssen **A** festlegen.

Parameter	Erforderliche Einstellung
Phone 1 Usage oder Phone 2 Usage	Sie müssen für beide Felder einen der folgenden Werte festlegen: • **A** • **None**
Phone Num Binding	Sie müssen **Yes** festlegen. Dadurch wird die Pipeline gezwungen, die korrekte SPID zu verwenden.

Konferenzschaltung

Betrifft nur Pipeline 75. Falls Ihr ISDN-Service eine Konferenzschaltungsfunktion bietet, können Sie über die Pipeline Konferenzschaltungen herstellen. Bei Konferenzschaltungen können mehr als zwei Personen gleichzeitig miteinander sprechen. Falls Ihre Telefongesellschaft die Konferenzschaltungsfunktion anbietet, sind entweder 3-Weg-Konferenzschaltungen (Sie und bis zu zwei andere Teilnehmer) oder 6-Weg-Konferenzschaltungen (Sie und bis zu fünf andere Teilnehmer) möglich.

Verwenden der Konferenzschaltung

Wenn Sie eine Konferenzschaltungen herstellen wollen, gehen Sie folgendermaßen vor:

1 Rufen Sie eine Person an, die an der Konferenz beteiligt sein soll, oder veranlassen Sie die Person, Sie anzurufen.

2 Schalten Sie einen Ruf auf Halten, indem Sie kurz auf die Hörergabel drücken und wieder loslassen.

3 Rufen Sie eine weitere Person an, die an der Konferenz beteiligt sein soll, oder veranlassen Sie die Person, Sie anzurufen.

4 Geben Sie alle gehaltenen Rufe frei, indem Sie die Hörergabel zweimal kurz drücken und wieder loslassen.

5 Wenn Sie der Konferenzschaltung weitere Teilnehmer hinzufügen wollen, müssen Sie die Schritte 2-4 wiederholen.

Ein Teilnehmer verläßt eine Konferenzschaltung, indem er auflegt. Sie können die Verbindung zum zuletzt hinzugefügten Teilnehmer folgendermaßen unterbrechen:

Drücken Sie zweimal kurz die Hörergabel und lassen Sie sie wieder los.

CallerID unterstützt

Die Nummer des anrufenden Teilnehmers ist im ISDN BRI-Datenstrom enthalten. Sie können die Nummer feststellen, es sei denn der Anrufer hat sie blockiert, indem Sie eine CallerID-Einheit an die POTS-Anschlüsse der Einheit anschließen.

IDSL-Unterstützung für Sprachrufe von Pipeline 75 oder TA

Betrifft nur Pipeline 75. Die IDSL-Karte (ISDN Digital Subscriber Line) von Ascend unterstützt jetzt Sprachrufe von einer Pipeline 75 oder einem ISDN-Terminal-Adapter (TA), der die Blockwahl unterstützt. Damit sind Sie in der Lage, einen Sprachruf von einem ISDN-Gerät über eine IDSL-Leitung an eine Pipeline vorzunehmen. Die Pipeline kann den Ruf dann an das Sprach-Netzwerk routen.

Damit IDSL-Sprachrufe von einer Pipeline 75 oder einem anderen ISDN-Gerät unterstützen kann, muß das ISDN-Gerät die Q.931-Blockwahl unterstützen. Eine Einheit, die die Blockwahl unterstützt, gibt die gewählten Nummern in der Einstellungsmeldung an, die sie an die Einheit sendet, mit der sie eine Verbindung herstellt. Die Pipeline, in der die IDSL-Karte installiert wurde, kann dann einen Ruf anhand dieser Informationen zum Sprach-Netzwerk routen.

Konfigurieren eines IDSL-Sprachrufs

Konfigurieren Sie die Pipeline folgendermaßen:

1. Wählen Sie „System > Sys Config“
2. Legen Sie „Trunk Groups=Yes“ fest.
3. Beenden Sie das Systemprofil, und speichern Sie die Änderungen.
4. Wählen Sie aus dem Hauptbearbeitungsmenü BRI/LT > Line Config > erstes „Line“-Profil.
5. Wählen Sie die Nummer der Leitung, die Sie konfigurieren wollen.
6. Legen Sie für die Parameter „B1 Slot“ und “B2 Slot“ die Nummer der Position fest, an die Sie eingehende Rufe routen wollen.

   Beispiel: wenn Sie Rufe vom ersten B-Kanal an Position 2 routen wollen (eine T1/PRI-Leitung), müssen Sie „B1 Slot=2“ festlegen.
7. Beenden Sie das erste „Line“-Profil, und speichern Sie es.
8. Konfigurieren Sie alle Leitungen, für die Sie einen Sprachdienst bereitstellen wollen.

Konfigurieren Sie eine Pipeline oder ein ähnliches Gerät folgendermaßen:

1. Achten Sie darauf, daß das Gerät die Blockwahl unterstützt.

   Legen Sie für die Pipeline im Menü „Configure“ „Switch Type=Japan“ fest.
2. Wenn Sie wählen, müssen Sie darauf achten, der zu wählenden Nummer, die Nummer des Leitungsbündels vorauszustellen.

   Beispiel: Wenn Sie die Nummer 555-5555 anrufen wollen, müssen Sie „2-555-5555“ wählen, um über die zweite T1/PRI-Leitung hinaus zukommen. Falls Sie die Nummer des Leitungsbündels auslassen, wird der Ruf wie jeder andere behandelt und an der Pipeline beendet.
3. Nachdem Sie die letzte Ziffer der Telefonnummer eingegeben haben, müssen Sie ein Endezeichen eingeben, um der Pipeline mitzuteilen, daß Sie die gesamte Telefonnummer eingegeben haben.

   Geben Sie auf einer Pipeline das Zeichen „#“ nach der Telefonnummer ein; bei anderen ISDN-Geräten kann es andere Endezeichen geben.

Switch Type

Beschreibung: Gibt den Typ der Netzwerkvermittlungsstelle an, die den ISDN BRI-Dienst für die Pipeline bereitstellt.

Bei einer Netzwerkvermittlungsstelle handelt es sich um die Vermittlungsstelle oder PBX, die die ISDN BRI-Leitung an der MAX-Einheit beendet und die MAX-Einheit mit dem leitungsvermittelten WAN verbindet. Dabei handelt es sich um eine leitungsvermittelte Verbindung, die aus einem oder mehreren Kanälen besteht.

Verwendung: Betätigen Sie die Eingabetaste, um die Auswahl durchzugehen. Die Auswahlmöglichkeiten unterscheiden sich je nach Profile und aktivierten Optionen.

Sie können einen der Vermittlungsstellentypen aus der folgenden Tabelle angeben:.

Tabelle A-1. Vermittlungstyp des Profils konfigurieren

Vermittlungs-stellentyp	Erklärung
AT&T/P-T-P	AT&T Point-to-Point ist der Standard.
AT&T/Multi-P	ATT&T Mulitpoint.
NTI	Northern Telecommunications, Inc. Verwenden Sie diese Einstellung, falls es sich bei Ihrer Vermittlungsstelle um DMS-100 Custom handelt.
NI-1	National ISDN 1.
NI-2	National ISDN-2.
IDSL	Identisch mit AT&T Point-to-Point, unterstützt jedoch Q.931-Blockwahl.

Tabelle A-1. Vermittlungstyp des Profils konfigurieren (Continued)

Vermittlungs-stellentyp	Erklärung
U.K.	United Kingdom: ISDN-2 Hong Kong: HKT Switchline BRI Singapore: ST BRI Europäische ISDN-Länder: Österreich, Belgien, Dänemark, Deutschland, Finnland, Italien, Niederlande, Portugal, Spanien, Schweden Identisch mit NET 3.
SWISS	Schweiz: Swiss Net 2
NET 3	Identisch mit U.K.
GERMAN	Deutschland 1TR6-Version: DBP Telecom
MP GERMAN	Deutschland: 1TR6 Multipoint
FRANCE	Frankreich: FT Numeris
DUTCH	Niederlande 1TR6-Version: PTT Netherlands BRI
BELGIUM	Belgien: Prä-Euro ISDN Belgacom Aline
JAPAN	Japan: NTT INS-64
AUSTRALIA	Australien und Neuseeland

Abhängigkeiten: Beachten Sie diese zusätzlichen Informationen:

- Der Parameter „Switch Type“ ist bei einer Verbindung, die Inband-Nachrichtenübermittlung (Call Type=56K oder 56KR) verwendet oder ausschließlich aus festen Kanälen (Call Type=Nailed) besteht, nicht zutreffend.

Bei der Inband-Nachrichtenübermittlung werden 8 Kbit/s eines 64 Kbit/s-Kanals zur WAN-Synchronisierung und -Nachrichtenübermittlung und die verbleibenden 56 Kbit/s zur Übermittlung von Benutzerdaten verwendet.

Switched-56-Leitungen arbeiten mit der Inband-Nachrichtenübermittlung.

- Alle internationalen Vermittlungsstellentypen mit Ausnahme der deutschen arbeiten im Point-to-Point-Modus.

Parameter-Ort: Profil „Configure“

Unterstützung für ausgehende 3,1K-Audiorufe hinzugefügt

Betrifft nur Pipeline 75. Die Unterstützung für ausgehende 3,1K-Audiorufe wurde hinzugefügt, um Rufe an Faxmaschinen und andere Geräte (besonders in Japan) zu ermöglich, die einen Ruf nur annehmen, wenn er in der ISDN-SETUP-Meldung als ein 3,1K-Audioruf ausgewiesen wird.

Funktionsweise von 3,1K-Audiorufen

Im Konfigurationsmenü lauten die aktuellen Standardwerte „Phone 1 Usage=A“ und „Phone 2 Usage=B“. Das bedeutet, daß es sich bei den Geräten, die an die analogen Anschlüsse 1 und 2 angeschlossen sind, um Telefone handelt. Ein ausgehender Ruf vom entsprechenden Anschluß verwendet „Speech information transfer“ in seiner ISDN-SETUP-Meldung.

Falls Sie „Phone 1 Usage=A 3.1K audio“ festlegen, handelt es sich bei dem an den analogen Anschluß 1 angeschlossenen Gerät nicht um ein Telefon und ein Ruf von einem entsprechenden analogen Anschluß verwendet „3.1K audio information transfer“ in seiner ISDN-SETUP-Meldung.

Hinweis: Die Parameter „Phone N Usage=A 3.1K audio“ und „Phone N Usage=B 3.1K audio“ beziehen sich nur auf ausgehende Rufe. Viele Faxgeräte erfordern „Speech“ in der SETUP-Meldung, daher nimmt die Pipeline Rufe an, die entweder „Speech“ oder „3.1K audio information transfer“ verwenden.

Konfigurieren von 3,1K-Audioruf

Wenn Sie die Pipeline konfigurieren wollen, um einen 3,1K-Audioruf zu senden, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Menü „Configuration“.

2 Legen Sie „Phone N Usage=A 3.1K audio call“ fest.

N steht entweder für 1 oder 2, d. h. Telefon 1 oder Telefon 2. Damit wird der analoge Anschluß angegeben, der für ausgehende 3,1K-Audiorufe verwendet wird.

3 Speichern Sie die Konfiguration.

Pipeline 130 Fehlersuche und -beseitigung

B

Überblick

Die folgenden, neuen Funktionen wirken sich möglicherweise darauf aus, wie Sie auf der Einheit eine Fehlersuche und -beseitigung durchführen:

Timer-Unterbrechung von Reserveverbindung B-2
T1-Prüfschleife für die Pipeline 130 .....B-2
Manuelle Prüfschleife für Pipeline 130 .....B-4
Unterstützung der Inband-Prüfschleife für T1 .....B-6
Manuelle T1-Prüfschleife mit dem Leitungs-Transceiver B-7
SNMP Traps für BRI linkUp und linkDown B-8

Timer-Unterbrechung von Reserveverbindung

Gilt nur für die Pipeline 130. Wenn die feste T1-Verbindung auf der Pipeline scheitert, wird die ISDN-Reserveverbindung hergestellt. Mit dieser Funktion können Sie die ISDN-Reserveverbindung durch einen Timer unterbrechen lassen, wenn die feste T1-Verbindung wiederhergestellt ist.

Die Pipeline bietet eine ISDN-Reserveverbindung für ihre primäre feste T1-Verbindung. Bisher mußte die ISDN-Reserveverbindung manuell unterbrochen werden, nachdem die primäre Verbindung nach einem Scheitern wiederhergestellt worden war. Dies konnte in komplexen Routing-Umgebungen Probleme verursachen, weil z. B. ein ISP nicht vollständig verhindern kann, daß Rufe von ihrem Netzwerk über die ISDN-Leitungen gehen. Die Pipeline kann jetzt feststellen, ob die primäre Verbindung wiederhergestellt wurde und routet dann den ganzen Verkehr über diese primäre Verbindung. Dadurch wird der Timer der ISDN-Verbindung aktiviert, der sie nach Ablauf einer bestimmten Periode der Inaktivität unterbricht.

T1-Prüfschleife für die Pipeline 130

Die feste T1-Verbindung der Pipeline unterstützt jetzt einen Prüfschleifentest. Wenn sich die T1-Verbindung der Pipeline im Prüfschleifenmodus befindet, sendet Sie alle von der Vermittlungsstelle empfangenen Signale an die Vermittlungsstelle zurück. Prüfschleifen können dazu beitragen, festzustellen, ob die Verbindung über die digitale Zugriffsleitung und das WAN sicher ist.

Zur Unterstützung des T1-Prüfschleifentests wurden die folgenden Änderungen in der Benutzerschnittstelle der Pipeline vorgenommen:

- Der neue Parameter „Loop Back“ wurde dem Menü „Mod Config > Nailed T1 Mod Config“ hinzugefügt.
- Dem WAN-Statusfenster wurde ein neues Feld hinzugefügt.

Der Parameter und das Feld im Statusfenster werden weiter unten beschrieben:

Loop Back

Beschreibung: Gestattet Ihnen, einen Prüfschleifentest an der festen T1-Verbindung der Pipeline durchzuführen. Wenn sich die T1-Verbindung der Pipeline im Prüfschleifenmodus befindet, sendet Sie alle von der Vermittlungsstelle empfangenen Signale an die Vermittlungsstelle zurück. Prüfschleifen können dazu beitragen, festzustellen, ob die Verbindung über die digitale Zugriffsleitung und das WAN sicher ist.

Verwendung: Betätigen Sie die Eingabetaste, um zwischen den Optionen umzuschalten:

- „Normal“ gibt an, daß die Leitung nicht im Prüfschleifenmodus arbeitet.
- „Relay Loopback“ gibt eine direkte, metallische Prüfschleife des Signals, das von der Netzwerkschnittstelle erzeugt wurde, an.
- „Line loopback“ bezeichnet die Prüfschleife des Signals, das von der Netzwerkschnittstelle erzeugt wurde, und zwar bei der Stromkreistärke, die aktuell im Feld „Build out“ im Menü „Nailed T1“ festgelegt ist.

Abhängigkeiten: Die T1-Leitung kann nicht für Kommunikationszwecke verwendet werden, während sie sich im Prüfschleifenmodus befindet.

Parameter-Ort: Nailed T1 > Mod Config

Neues Feld im Leitungsstatusfenster

Im Leitungsstatusfenster „10-100“ gibt es jetzt unter dem Feld „T1/CSU“ ein Feld, das angibt, ob sich die T1-Leitung im Prüfschleifenmodus befindet.

Beispiel: Falls Sie für den Parameter „Loop Back“ im Profil „Nailed T1 Mod Config“ den Wert „Normal“ festgelegt haben, ähnelt das angezeigte Leitungsstatusfenster dem folgenden:

```
10-100 1   T1/CSU
Link   X   CARRIER
B1     *.....
B2     *.....
:
```

Falls Sie für den Parameter „Loop Back“ im Profil „Nailed T1 Mod Config“ den Wert „Loopback“ festgelegt haben, ähnelt das angezeigte Leitungsstatusfenster dem folgenden

```
10-100 1   T1/CSU
Link   X   LOOPBACK
B1     *.....
B2     *.....
:
```

Durchführen eines Prüfschleifentests

Wenn Sie einen Prüfschleifentest durchführen wollen, gehen Sie folgendermaßen vor:

1. Wählen Sie aus dem Hauptbearbeitungsmenü „T1 > Mod Config“.
2. Legen Sie für den Parameter „Loop Back“ den Wert „Loopback“ fest.
3. Verlassen Sie das Profil „Mod Config“, und speichern Sie die Änderungen.
4. Sobald Sie das Profil gespeichert haben, wird die Leitung in Prüfschleifenmodus geschaltet.

   Wenn sich die feste T1-Leitung im Prüfschleifenmodus befindet, ist keine Kommunikation über das WAN möglich.

Manuelle Prüfschleife für Pipeline 130

Dem Profil „Nailed 56“ wurde eine manuelle Prüfschleifenfunktion hinzugefügt. Dabei handelt es sich um eine Prüfschleife für einen entfernten Standort, bei der das Signal von der Vermittlungsstelle erzeugt und zur Vermittlungsstelle zurückgeschleift wird. Dies ist anders als die lokale Prüfschleife, die in POST verwendet wird und bei der das Pipeline-Signal auf sich selbst zurückgeschleift wird.

Die Vermittlungsstelle kann den Pipeline-Benutzer u. U. auffordern, daß er die Pipeline in den Prüfschleifenmodus schaltet, wenn sie Probleme zu isolieren versucht. Der Standardmodus ist „Normal“ (nicht „looped back“), da keine Kommunikation erfolgen kann, während sich die Pipeline im Prüfschleifenmodus befindet.

Konfigurieren der manuellen Prüfschleife

Dem Menü „Nailed 56 > Mod Config“ wurde ein Feld hinzugefügt, damit Sie die Pipeline in den Prüfschleifenmodus schalten können.

Hinweis: Sehen Sie sich das Statusfenster „10-100“ an, um zu prüfen, ob sich die Pipeline im normalen Modus oder im Prüfschleifenmodus befindet (siehe unten in „“Anzeigen im Leitungsstatusfenster für den Prüfschleifenmodus.”“).

Wenn Sie eine Pipeline in den manuellen Prüfschleifenmodus schalten wollen, gehen Sie folgendermaßen vor:

1 Öffnen Sie das Profil „Nailed 56“.

Betätigen Sie bei Bedarf so lange die Esc-Taste, bis das Hauptbearbeitungsmenü angezeigt wird. Wählen Sie dann „Nailed 56“, und betätigen Sie die Eingabetaste.

2 Wählen Sie „Mod Config“.

Das abgebildete Menü „Mod Config“ erscheint.

```
30-100 Mod Config
 Nailed Grp=1
 Activation=Enabled
 Loop Back=Normal
```

3 Wählen Sie „Loop Back“.

Für dieses Feld gibt es zwei mögliche Werte: „Normal“ oder „Loop“, bei dem es sich um den Prüfschleifenmodus handelt.

4 Speichern Sie, und betätigen Sie die Eingabetaste.

Hinweis: Denken Sie daran, die Pipeline wieder in den Modus „Normal“ zu schalten. Während Sie sich im Prüfschleifenmodus befindet, ist keine Kommunikation möglich.

Anzeigen im Leitungsstatusfenster für den Prüfschleifenmodus

Den Anzeigen im Statusfenster „10-100“ wurde eine Anzeige für den Prüfschleifenmodus hinzugefügt (siehe unten):

Statusanzeige	Bedeutung
X	Leitung unterbrochen
A	Leitung steht
L	Leitung im Prüfschleifenmodus

Unterstützung der Inband-Prüfschleife für T1

Die Inband-Prüfschleife ist jetzt für die Pipeline 130-Modelle mit einer T1-Schnittstelle verfügbar. Bisher ignorierte die Pipeline 130 das Befehlssignal der Inband-Prüfschleife. Daher konnten T1-Techniker an der Vermittlungsstelle keine Prüfschleife für die Leitung zur Problemdiagnose schalten.

Hinweis: Bei dieser Prüfschleife handelt es sich um die gleiche, die über manuelle Befehle im T1-Profil verfügbar ist.

Änderungen im WAN-Statusfenster

Im WAN-Statusfenster können Sie die folgenden Änderungen sehen:

- Im Feld „Line State“ werden mehr Leitungen angezeigt.
- Die Definition von „Loopback“ wurde erweitert und umfaßt jetzt sowohl die manuelle Prüfschleife als auch die Inband-Prüfschleife.

	Bisherige Anzeige	**Neue Anzeige**
RED	Kein Signal erfaßt	Keine Änderung
YELLOW	Gelbes Alarmsignal erfaßt	Keine Änderung
CARRIER	T1 CARRIER (LINE UP) erfaßt	Keine Änderung
Loopback	Manuelle Prüfschleife aktiv	Manuelle Prüfschleife aktiv (falls Sie den Befehl am Terminal eingeben) oder Inband-Prüfschleife aktiv (falls das Inband-Signal von der Telefongesellschaft gesendet und von der Netzwerkschnittstelle empfangen wird).
BLUE	(Wurde erfaßt, aber nicht angezeigt.)	Blaues Alarmsignal erfaßt und angezeigt.

Manuelle T1-Prüfschleife mit dem Leitungs-Transceiver

Der Pipeline 130 wurde ein weiterer Prüfschleifentest hinzugefügt, mit dem ein vollständiger, manueller T1-Prüfschleifentest über den Leitungs-Transceiver durchgeführt werden kann.

Konfigurieren des manuellen Prüfschleifentests

1 Öffnen Sie das Menü „Mod Config > Nailed T1“.

2 Legen Sie „Loop Back=Line Loopback“ fest.

SNMP Traps für BRI linkUp und linkDown

Die Pipeline 130 unterstützt die beiden BRI SNMP-Traps „linkUp“ und „linkDown“, die von Alarmereignisse oder Fehlerereignissen ausgelöst werden. Ein SNMP Trap wird von der Pipeline 130 ausgesandt, um anzuzeigen, daß eines der folgenden Ereignisse eingetreten ist:

- „LinkUp“ zeigt an, daß eine Basisanschlußleitung physisch mit einem Basisanschluß verbunden wurde, während die Pipeline 130 aktiv ist, oder daß eine Basisanschlußleitung während des Boot/Kaltstartprozesses initialisiert wurde.
- „LinkDown“ zeigt an, daß ein Basisanschlußleitung physisch von einem Basisanschluß entfernt wurde, während die Pipeline 130 aktiv ist.

Index

Zeichen

„Group“-Nummer 2-8

Zahlen

2-Kanalrufe auf einem SPID A-3
3,1K-Audiorufe A-9

A

ACE 4-30
Adresse der entfernten Schnittstelle 3-43
Adreß-Pools 3-28, 4-31
alternative Wählnummern 1-12
Anschluß-Routing 4-4
  Konfigurieren 4-4
anwählende NetWare-Clients 5-5
anwählende Windows 95-Clients 5-5
Anzahl Anschlüsse 4-3
Anzeigen
  IP-Routing-Tabelle 3-33
Anzeigen von Wählpaketen 7-2
Ascend Tunnel Management Protocol (ATMP) 2-5
AT&T Point-To-Point-Service 1-9
ATMP verwendet UDP-Anschluß 5150 2-6
ATMP-Tunnel 2-5
Attribut „Ascend-Home-Agent-Password“ 2-6
Authentifizierungskopfzeilen 3-2, 3-3
Authentifizierungs-Timeout 7-26
automatische SPID-Feststellung 1-8
automatische Vermittlungsstellenauswahl 1-8
automatisches Zuweisen von IP-Adressen 4-30
Average Line Utilization (ALU) 6-27

B

B8ZS-Modus 2-16
Bandwidth Allocation Control Protocol (BACP) 2-3, 6-12
Befehl
  Diagnostics 7-25
  fclear 1-5
  gnvram 1-5
  iproute 3-33
  iproute show 3-33
  IPsecdblog 3-20
  IPsecSADump 3-16
  IPsecSchemeDump 3-18
  ipxroutinfo 5-3
  ipxservinfo 5-3
  Show 3-47
  Show ? (Hilfe) 7-22
  Show Revisions 7-21
  Termsrv 7-25
  TFTP 7-15, 7-28

tloadcode 7-15
Traceroute 7-9
trestore 6-28
tsave 6-28
tsave -a 7-12
tsave -m 7-13
Befehl zum Anzeigen der Systemversion 7-21
bekanntgemachte Routen 3-25
Beschreibungen des Zurücksetzens 7-22
BOOTP Relay 4-27
BOOTP-Client 4-26
BOOTP-Server 4-26, 4-30
Bootstrap Protocol (BOOTP) 4-26
BRI linkUp und linkDown B-8

C

Called Number Authentication 6-15
Channel Service Unit (CSU) unterstützt 2-12
Clid Auth in Id Auth geändert 6-15
Community-Zeichenfolge 6-22, 6-23
Community-Zeichenfolge für den Lese- und Schreibzugriff 6-25
Cookie 6-23
Current Line Utilization (CLU) 6-27

D

D4-framed T1-Leitungen nicht von FDL unterstützt 2-13
DHCP Spoofing
Antwort 4-30
Einrichten 4-35
DHCP-Client 4-9
DHCP-Server 4-2, 4-30
Einrichten 4-34
Diagnoseausgabe von „ippacket“ 3-38
Diagnosebefehl
FWALLversion 3-23
wdDialout 7-3
Diagnosemeldungen 3-20
Diagnoseoption, mit der Wählpakete angezeigt werden 7-2
Dicke Ausführungsdateien 7-16
DNS
Allow as Client DNS 4-57
Client Assign DNS 4-57
Client Pri DNS 4-58
Client Sec DNS 4-58
sekundärer Domänenname 4-59
verbindungsspezifische Server angeben 4-58
DNS-Liste 4-49
DNS-Tabelle mit Host-Adressen 4-60
Domain Name Server (DNS) für Benutzer einrichten 4-54
DS0-Ursprung 2-15
Dynamic Host Configuration Protocol (DHCP) 4-8, 4-30

E

eingehende Datenrufe auf welcher Leitung 1-9
Einstellen der Systemuhr mit SNMP 7-26
Encapsulating Security Payload (ESP) 3-3
Endpunkt eines lokalen ATMP-Agenten 2-4
Expect Callback 6-18
konfigurieren 6-19
Extended Super Frame (ESF)-Format 2-12

F

Facilities Data Link (FDL) 2-12
Fangstelle für Telnet-Kennwortüberprüfung 7-20
FDL (Facilities Data Link)-Protokoll, angeben 2-13

Fehlerton bei Konfigurierung mit Tastfernsprecher 1-6
Fenster
  Line Status 1-9
Firewalls 6-2
  einem Verbindungsprofil zuweisen 6-5, 6-6
  Konfigurieren für Anschluß-Routing 4-4
  numerieren 6-4
Flags in der Routing-Tabelle 3-36

G

geheimer Authentifizierungsschlüssel 6-21

H

Hunt-Gruppen 6-27

I

IDSL-Unterstützung für Sprachrufe A-5
IGMP-Multicast-Clients 3-48
IGMP-Pakettypen 3-49
Inband-Prüfschleife für T1 B-6
Internet Group Membership Protocol (IGMP) 3-45
Inverse Address Resolution Protocol (InARP) 2-4
IP Security
  Festlegen des Parameters 3-11
  konfigurieren 3-4
IPCP-Verhandlungen 4-54
IP-Routing-Tabelle, Felder 3-35
IP-Sicherheit 3-2
  Syslog 3-20
IPX Type 20-Pakete 5-2
IPX-Filter 5-5, 5-6
IPX-Netzwerk 5-5
IPX-Routeneinträge 5-3
IPX-Server-Einträge 5-3
IPX-Verbindung von anwählendem Benutzer 5-5

K

Kodierungsmodus 2-15
Konferenzschaltung A-4
Konfigurieren eines Anschlusses für Syslog-Meldungen 7-27
Konfigurieren mit Tastfernsprecher 1-5

L

Länge des Benutzernamens 1-14
Länge von Telefonnummern 1-14
LED leuchtet bei Sprachrufen A-2
Leitungsstatusfeld 2-10
Leitungsstatusfenster für Prüfschleifenmodus B-6
Leitungsstatusfenster für T1/CSU B-3
Leitungs-Transceiver B-7
linkDown B-8
linkUp B-8
Liste der in DOV abgelehnten Nummern 1-3
Load-Name 1-10
lokale DNS-Tabelle 4-60
  Erstellen 4-62
  Konfigurieren 4-60
  Löschen 4-64
lokaler Agent in Router-Modus konfiguriert 2-6
Lokalisieren langsamer Router 7-9

M

MAC (Ethernet)-Adressen 4-30
manuelle Prüfschleife für T1-Verbindungen B-4
MAX als DHCP-Server 4-9
MD5 3-3
MD5-Hash 6-21, 6-24
Menü
  DHCP Spoofing 4-31
  Line Status 1-9
mib-2 system sysObjectID 6-29
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) 6-13
Mobile-Schema 3-4
MP-Verbindungen 2-2
MS-CHAP mit DES- und MD4-Verschlüsselung 6-13
Multicast-Weiterleitung 3-45

N

NAT 4-2
NAT DHCP-Anforderung 4-10
NAT für Frame Relay 4-13
NAT mit einer Adresse Konfigurieren 4-4
NAT mit mehreren Adressen Konfigurieren 4-10
NAT mit mehreren Anschlüssen 4-8
NAT-Profil 4-5
Network Address Translation (NAT) 4-2
Netzwerknummer, über die ein IPX-Netzwerk erreicht wird 5-5
Netzwerktest 7-9
Nicht unterstützte Ausführungsdateien 7-19
Numerieren von Firewalls 6-4
numerierte Schnittstellen 3-41
Nutzzeit-Variable 6-23

P

Paket-Filter 6-2
Parameter
  3DES IV Length 3-8
  3DES Key n 3-9
  Activation 2-9
  Allow as Client DNS 4-57
  Always Spoof 4-37
  Ans Voice Call 1-3
  Become Default Router 4-36
  Block calls after 7-8
  Blocked duration 7-9
  BOOTP Relay Enable 4-28
  CLID Fail Busy 6-17
  Client Assign DNS 4-57
  Client Gateway 3-29
  Client Pri DNS 4-58
  Client Sec DNS 4-58
  Data Over Voice (DOV) 1-3
  Data Usage 1-9
  Def Server 4-14
  DES IV Length 3-10
  DES Key 3-10
  DHCP PNP Enabled 4-36
  DHCP Spoofing 4-35
  Dial If Link Down 4-37
  Disc on Auth Timeout 7-26
  Dst Network Adrs 5-7
  Dst Node Adrs 5-8
  Dst Port# 4-15
  Dst Socket # 5-8
  Dst Socket Cmp 5-8
  Filter Persistence 6-10, 6-12
  Forward 5-7
  FR address 4-17
  Group 2-7, 2-9
  Group 1 Count 4-41
  Group 2 Count 4-43
  Handle IPX Type 20 5-2

Host 1 Enet 4-44
Host 1 IP 4-43
Host 2 Enet 4-46
Host 2 IP 4-45
Host 3 Enet 4-48
Host 3 IP 4-47
Hunt-n# 6-28
Id Auth 6-15
IF Adrs 3-41, 3-42
IP Group 4-40
IP Group 2 4-42
IPX SAP Proxy Net#n 5-4
Lan 4-17
Lan Adrs 3-43
Length 6-7
List Attempt 4-50
List Size 4-50
Loc Adrs 4-18
Loc Port# 4-19
Log Port 7-24
Loop Back B-3
Maximum No Reply Wait 4-39
MD5 Key 3-11
Multicast Forwarding 3-46
Multicast Profile 3-46
Name 6-7
Peer, im Antwortprofil hinzugefügt 5-5
Protocol 4-22
R/W Comm Enable 6-20
Recv Auth 6-14
Renewal Time 4-36
Sec Domain Name 4-59
Security Parameters Index (SPI) 3-14
Server 4-28
SHA-1 Key 3-13
Src Network Adrs 5-7
Src Node Adrs 5-7
Src Socket # 5-8
Src Socket Cmp 5-8
TCP Timeout 4-52
Tunnel Address 3-15
Valid 4-25
Validate IP 4-38
Version 6-7
WAN Alias 3-43
Paramter
Clock Source 2-14
Physische Spezifikationen von V.35 2-11
Plug & Play 4-30
Einrichten 4-35
PPP-Verhandlungen 4-3
Private Adressen/offizielle Adressen 4-2
Protokoll „Fatal Error“ 7-22
Prüfungspfad für IP-Verbindungen 6-2

Q

Q.922-Adresse 2-4

R

Registered Ports 4-8
Reserveverbindung für T1-Verbindungen B-2
reservierte IP-Adressen 4-30
RIP und SAP, Bezug zu anwählenden Clients 5-6
Routenpräferenzen 3-30
Anzeige 3-36
Routing auf Boxbasis 3-40
Routing auf Schnittstellenbasis 3-40, 3-44
Routing auf Systembasis 3-40
Routing eingehender Pakete deaktivieren 4-7
Routing-Tabelle
ALU (Average Line Utilization) 3-48
Client 3-48
CLU (Current Line Utilization) 3-48
Counts 3-48
Expire time 3-48
Group address 3-47
Hash 3-47
Members ID 3-47
RecvCount 3-48

Version 3-48
Rückseiten abgebildet 1-2
Rufblockierung bei gescheiterten Verbindungen 7-8

S

SAFEWORD 4-30
Scheme-Datenbank 3-4
Schnittstelle
blackhole 3-28, 3-37
mcast 3-38
reject 3-28
secretkey 6-25
Secure Access Firewall 3-40
Secure Access Management (SAM) 6-2
Security Association (SA) 3-2
Security Parameters Index (SPI) 3-2
Security-Schema 3-3
Sekundärprofil 1-12
serielle WAN-Datenübertragungsgeschwindigkeit 2-7
Serieller WAN-V.35-Anschluß 2-7
SNMP IfTable 6-29
SNMP-Authentifizierung 6-23
SNMP-Einstellungsbefehle 6-19
SNMP-Get-Anforderung 6-25
SNMP-Schreibsicherheit 6-19
SPX-Spoofing 5-8
Standard-Route pro Benutzer 3-28
Static-Schema 3-4
Statusanzeige für Sprachrufe A-2
Statusfenster „Dyn Stats“ 6-26
Statusfenster „Sys Option“ 6-6
Stiftzahlen von V.35 2-11
Superframe-Format 2-13
Syslog-Host 7-24
Syslog-Meldungen vom Firewall 6-8

T

T1
D4-frames nicht von FDL unterstützt 2-13
Empfangstaktgeberrate 2-14
Inband-Prüfschleife B-6
Leitungsstatusfenster B-3
manuelle Prüfschleife B-4
Prüfschleife B-2
Prüfschleifentest mit dem Leitungs-Transceiver B-7
Qualität und Leistung 2-12
Reserveverbindung B-2
Übertragungstaktgeberrate 2-14
Verbindung B-2
Taktgeberrate 2-7
TCP-Anschlüsse 4-2
Transform (Verkapselung) 3-3
Tunnel, ATMP konfigurieren 2-5
Tunnel, bei IP-Sicherheit verwendet 3-3

U

UDP-Anschlüsse 4-2
UDP-Testpakete 7-11
Unterbrechungsursachencode
Normal Call Clearing 6-17
User Busy 6-17
Unterbrechungsursachencode beim Scheitern der Authentifizierung 6-16
Unterbrechungsursachencode für Authentifizierungsfehler 6-17
Untermenü
IPX Options, im Antwortprofil hinzugefügt 5-5
IPX Routes 5-5

V

Verbreiten von RIP- und SAP-Paketen 5-4
vernichtete IPX-Routen und SAP-Pakete 5-3
Verschlüsselung 3-2
Verwendete RIP-Protokolle 3-30
Virtuelle private Netzwerke 2-4

W

Watchdog 5-8
Well Known Ports 4-8
werkseitig eingestellte Standardwerte 1-5

Z

zeitabhängige Zustandsvariablen 6-21
Zielanschluß am Syslog-Host 7-24
Zuweisen von IP-Adressen 4-30