Release Notes Systemsoftware 7.1.12

Release Notes - Systemsoftware 7.1.12
Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.1.12**.

Haftung

Der Inhalt dieses Dokuments wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Dokument gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen finden Sie unter www.bintec.de.

Als Multiprotokoll-Gateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EC

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.1.12. Systemsoftware 7.1.12 beruht auf Systemsoftware 7.1.1, daher gelten die gleichen Bedingungen den Funktionsumfang und die Einschränkungen beim Downgrade betreffend.

Hinweis

Beachten Sie unbedingt die Hinweise zum Upgrade auf **Systemsoftware 7.1.12**, die Sie auf unserer Website ebenso wie die Software zum Download bereit gestellt finden.

1.1 Gültigkeit

Systemsoftware 7.1.12 kann sowohl für Geräte der neuen **VPN Access** Reihe als auch für die Geräte der X-Generation verwendet werden. Beachten Sie bitte, dass sich der Funktionsumfang zwischen den Geräten unterschiedlicher Reihen unterscheiden kann.

Für die folgenden Geräte ist keine Version von **Systemsoftware 7.1.12 verfügbar:**

- **BinGO! DSL**
- **X1000**
- **X1200**
- **X3200**
- ale Geräte der **BRICK**-Generation.

1.2 BOOTmonitor Update

Ein Update auf **Systemsoftware 7.1.12** erfordert ein BOOTmonitor-Update auf Gateways der **X2000**-Familie, wenn das Gateway ausgehend von einem Release-Stand vor 7.1.1 aktualisiert werden soll. **X2301** und **X2302** sind davon nicht betroffen.

Sie finden die notwendigen Dateien im Download-Bereich Ihres Gateways. Das BOOTmonitor-Update kann genau wie die Systemsoftware mittels des Befehls `update` erfolgen. Eine Beschreibung finden Sie im Handbuch Ihres Gateways im Kapitel "Konfigurationsmanagement".

Achtung!

Das Update des BOOTmonitor muss vor dem Update der Systemsoftware durchgeführt werden. Andernfalls ist ein Update der Systemsoftware nicht möglich.

Für Geräte der X2000-Familie ist ein BOOTmonitor mit einem Stand von mindestens 6.3.8 notwendig.

1.3 DSL-Logik löschen

Auf den Geräten der **X2300**-Familie ist es notwendig, vor dem Update auf **Systemsoftware 7.1.12** die jeweils nicht benötigte DSL-Logik zu löschen. **X2301** und **X2302** sind davon nicht betroffen.

Gehen Sie dazu folgendermaßen vor:

1. Gehen Sie zur Flash ROM Management Shell: `update -i`.
2. Rufen Sie eine Liste aller im Flash ROM gespeicherten Dateien auf: `ls -l`. Sie erhalten (z. B.) folgende Ausgabe auf der Shell:

```
Flash-Sh > ls -l
Flags      Version  Length  Date                Name ...
Vr-x-bc-B  6.3.04   1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129  319696  2003/01/24 15:48:05 X2E-ADSLp.x2c
Vr---l--f  3.8.129  315904  2003/01/16 13:17:42 X2E-ADSLi.x2c
Flash-Sh >
```

Die Datei "X2E-ADSLp.x2c" wird von **X2300** verwendet (ADSL over POTS), "X2E-ADSLi.x2c" von **X2300i** und **X2300is** (ADSL over ISDN).

3. Löschen Sie die nicht Ihrem Gateway-Typ entsprechende Datei: `rm X2E-ADSLi.x2c` oder `rm X2E-ADSLp.x2c`.
4. Stellen Sie sicher, dass die Datei gelöscht worden ist: `ls -l`.
   Sie erhalten nun folgende Ausgabe auf der Shell (wenn Sie z. B. die Logik für ADSL over ISDN gelöscht haben):

```
Flash-Sh > ls -l
Flags      Version   Length  Date               Name ...
Vr-x-bc-B  6.3.04    1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129   319696  2003/01/24 15:48:05 X2E-ADSLp.x2c
Flash-Sh >
```

5. Führen Sie ein "reorg" durch, um die Datei endgültig aus dem Flash ROM zu löschen: `reorg`.
   Optional können Sie zur Kontrolle erneut eine Liste der gespeicherten Dateien aufrufen: `ls -l`.
6. Verlassen Sie die Flash ROM Management Shell: `exit`.

Sie haben die nicht benötigte DSL-Logik gelöscht.

Wenn das fehlschlägt

Obwohl wir die Update-Prozeduren so einfach wie möglich zu halten bemüht sind, können Probleme nicht ausgeschlossen werden. Unter bestimmten Umständen wird die oben beschriebene Prozedur fehlschlagen.

Dies ist dann der Fall, wenn der im Flash ROM zusammenhängend zur Verfügung stehende Speicher nicht ausreicht, um ein größeres Software Image als das aktuell geladene zu speichern. In diesem Fall wird keine Fehlermeldung ausgegeben, so dass Sie auf der Shell lediglich Folgendes Sehen:

```
x2300ic:> update 192.168.1.10 s7104b04.x2c
Starting TFTP File Transfer .x2300ic:>
```

Dies bedeutet nicht, dass Sie Ihr Gateway nicht aktualisieren können. Bitte lesen Sie in diesem fall das **Bintec How To**, das die Vorbereitung eines Gateways der **X2000**-Familie für ein Update beschreibt. Dieses Dokument finden Sie am selben Ort, an dem sich diese Release Notes befinden.

1.4 Einschränkungen beim Downgrade

Es ist nicht möglich, direkt von **Systemsoftware 7.1.12** auf eine frühere Version der Systemsoftware zurückzukehren.

Achtung!

Konfigurationen, die unter Systemsoftware 7.1.12 erstellt werden, sind mit älterer Systemsoftware nicht kompatibel.

Sichern Sie die Konfiguration Ihres Gateways auf einem PC, bevor Sie ein Upgrade vornehmen.

Beachten Sie, dass Ihnen nach einem Downgrade bestimmte Funktionen nicht mehr zur Verfügung stehen werden.

Ein stufenweiser Downgrade ist möglich:

1. Sichern Sie die Konfiguration Ihres Gateways auf einem PC, bevor Sie auf **Systemsoftware 7.1.12** upgraden. Informationen zum externen Sichern einer Konfiguration finden Sie im Handbuch Ihres Gateways im Kapitel "Konfigurationsmanagement".
2. Nun können Sie das Upgrade vornehmen und ggf. dennoch zu Ihrer alten Systemsoftware zurückkehren. Nach dem Downgrade müssen Sie die zu dieser Systemsoftware passende Konfigurationen auf das Gateway zurückspielen. Informationen zu den notwendigen Schritten finden Sie im Handbuch Ihres Gateways.

Weitere Informationen zu Beschränkungen beim Up- oder Downgrade sowie die Dokumentation Ihres Gateways finden Sie unter www.bintec.de

1.5 BRICKware Wizard

Seit Release 7.1.1 unterstützt unsere Systemsoftware den **BRICKware** Configuration Wizard nicht mehr. Mit Systemsoftware 7.1.4 ist ein neuer, HTML-basierter Configuration Wizard eingeführt worden.

1.6 Software-Image-Namen

Die Bezeichnungen der Software-Images haben sich dahingehend geändert, dass der eigentlichen Release-Kennung die Bezeichnung des Gerätes vorangestellt wird. Werden Ihre Gateways mittels des Konfigurationswerkzeugs XAdmin konfiguriert, so müssen Sie zunächst noch die alten Image-Namen verwenden. Dazu löschen Sie lediglich die Gerätekennung aus dem Namen: "X1x00II-b7101.x2x" wird so zu "b7101.x2x".

1.7 Voraussetzungen für die Verwendung des AUX-Ports

Systemsoftware 7.1.1 und 7.1.4 unterstützen den Anschluss eines analogen oder GSM-Modems am seriellen Anschluss Ihres Gateways. Für eine erfolgreiche Verbindung müssen bestimmte Voraussetzungen erfüllt sein.

Bitte lesen Sie die Release Notes zur Systemsoftware 7.1.1, um sich über Voraussetzungen und Beschränkungen zu informieren. Insbesondere beachten Sie bitte Folgendes:

- Nur die in den Release Notes 7.1.1 angegebenen Modems sind von uns erfolgreich getestet worden und für die Verwendung am AUX-Port freigegeben. Die XON/XOFF-Flusskontrolle muss vollständig unterstützt und funktionstüchtig sein, andernfalls wird eine Verbindung zwischen Gateway und Modem unter Umständen scheitern.
- Stellen Sie sicher, dass das zur Verbindung von Gateway und Modem verwendete Kabel den im Anhang von Release Notes 7.1.1 angegebenen Spezifikationen entspricht. Um sicherzugehen, können Sie ein fertig konfektioniertes Kabel von Bintec erwerben.

1 Wichtige Informationen

2 Neue Funktionen

Mit der Systemsoftware 7.1.12 wird eine Reihe wichtiger neuer Funktionen eingeführt, dazu gehören unter anderem L2TP (Schicht 2-Tunnelprotokoll), eine Erkennungsfunktion für Artem Access Points und TACACS+.

Folgende neue Funktionen wurden hinzugefügt:

2.1 Schicht-2-Tunnelprotokoll (L2TP)

Systemsoftware 7.1.12 unterstützt das Schicht-2-Tunnelprotokoll, welches das Tunneling von PPP-Verbindungen über eine UDP-Verbindung ermöglicht.

Unsere Implementierung deckt sowohl die Funktionen des L2TP-Netzwerkservers (LNS) als auch die Funktionen eines L2TP Access Concentrator Clients

(LAC) ab. Ein LAC-Client ist in der Lage, den in L2TP verkapselten PPP-Datenstrom lokal herzustellen. Damit ist es möglich, dass Hosts in einem LAN über alle unterstützten Verbindungsarten an das Gateway angeschlossen werden und immer noch L2TP nutzen können. Gegenwärtig unterstützen unsere Gateways L2TP-Tunnels über UDP-Verbindungen.

Einstellungen beim WAN-Partner

Um einen WAN-Partner für die Nutzung von L2TP konfigurieren zu können, wurden dem Menü für das Schicht 1-Protokoll in ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** zwei neue Optionen hinzugefügt:

- *PPP over L2TP (LNS mode)*: Bei Auswahl dieser Option wird der WAN-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt.
- *PPP over L2TP (LAC mode)*: Bei Auswahl dieser Option wird der WAN-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.

Wenn ein WAN-Partner für den L2TP-LAC-Modus konfiguriert wird, ist es notwendig, ein ***L2TP TUNNEL PROFILE*** auszuwählen.

L2TP-Menüeinstellungen

Die Liste der Profile, aus denen Sie auswählen können, wird im ***L2TP***-Menü erstellt, welches über das Setup Tool-Hauptmenü erreicht werden kann.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[L2TP]: L2TP Configuration                                  MyGateway

                          Static settings
                          Tunnel profiles


                            EXIT
```

Das Untermenü ***STATIC SETTINGS*** bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
UDP port number for LNS mode	Dies ist der Port, der vom LNS auf ankommende L2TP-Tunnelverbindungen überwacht wird. Verfügbare Werte sind alle ganzen Zahlen von *1* bis *65535*, der Standardwert ist *1701,* wie es in RFC 2661 vorgegeben ist.
Port usage for LNS mode	Dieser Parameter legt fest, ob der LNS nur den überwachten Port (***UDP PORT NUMBER FOR LNS MODE***) als lokalen Quellport für den L2TP-Ruf nutzt, oder einen der verfügbaren freien Ports auswählt.

Tabelle 2-1: ***L2TP ➜ STATIC SETTINGS***

Die L2TP-Tunnelprofile werden im Untermenü ***TUNNEL PROFILES*** erstellt oder bearbeitet:

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[L2TP][TUNNEL PROFILES][ADD]: Configure L2TP tunnels          MyGateway

     Profile Name                    l2tp1
     Local IP Address
     Local UDP Port (LAC only)       0
     Local Hostname
     Remote IP Address (LAC only)
     Remote UDP Port (LAC only)      1701
     Remote Hostname
     Tunnel Password
     Hello Interval                  30
     Data Packets Sequence Numbers   disabled
     Minimum Time Between Retries    1
     Maximum Time Between Retries    16
     Maximum Retry Count             5

                          SAVE                          CANCEL
```

Das Untermenü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Profile Name	Hier können Sie eine Beschreibung für das aktuelle Profil eingeben. Das Gateway nummeriert die Profile automatisch mit "*l2tp..*", dieser Wert kann jedoch geändert werden.
Local IP Address	Hier können Sie die IP-Adresse eingeben, die als Quelladresse für alle L2TP-Rufe genutzt wird, die auf diesem Profil aufbauen. Falls dieses Feld frei gelassen wird, nutzt das Gateway die IP-Adresse der dazugehörigen Schnittstelle.
Local UDP Port (LAC only)	Hier können Sie die Portnummer eingeben, die als Quellport für alle abgehenden L2TP-Rufe genutzt wird, die auf diesem Profil aufbauen. Verfügbare Werte sind *0* bis *65535*; der Standardwert *0* bedeutet, dass den Rufen, die dieses Profil nutzen, Ports dynamisch zugeordnet werden.
Local Hostname	Hier können Sie den Hostnamen eingeben, der in abgehende Tunnelaufbaumeldungen zur Identifizierung dieses Gateways aufgenommen wird. Bei diesen Meldungen handelt es sich um die vom LAC ausgesandten SCCRQs und die vom LNS ausgesandten SCCRPs. Der LNS nutzt diesen Parameter, um die ankommenden SCCRQ einem der verfügbaren L2TP-Profile zuzuordnen. Die maximale Länge des Eintrags ist 35 Zeichen.
Remote IP Address (LAC only)	Hier geben Sie die IP-Adresse ein, die als Zieladresse für Rufe genutzt wird, die auf diesem Profil aufbauen. Das Ziel muss ein Gerät sein, welches sich wie ein LNS verhalten kann.

Feld	Beschreibung
Remote UDP Port (LAC only)	Hier geben Sie die Zielportnummer ein, die für alle Rufe genutzt wird, die auf diesem Profil aufbauen. Der entfernte LNS, der den Ruf empfängt, muss diesen Port auf L2TP-Verbindungen überwachen.
Remote Hostname	Hier geben Sie den Namen des Hosts ein, der zur Identifizierung des entfernten Gateways auf ankommende Tunnelaufbaumeldungen warten soll (vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). Die maximale Länge des Eintrags ist 35 Zeichen. Der im LAC konfigurierte ***LOCAL HOSTNAME*** muss zu dem ***REMOTE HOSTNAME*** passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. Falls das Feld ***REMOTE HOSTNAME*** auf dem LNS leer bleibt, wird das dazugehörige Profil als Standardeintrag qualifiziert, der für alle ankommenden Rufe benutzt wird, für die kein Profil mit einem passenden ***REMOTE HOSTNAME*** gefunden werden kann.
Tunnel Password	Hier geben Sie das Passwort ein, welches für die Tunnel-Authentifizierung benutzt wird. Die Authentifizierung zwischen LAC und LNS erfolgt in beiden Richtungen, d. h. der LNS prüft den ***LOCAL HOSTNAME*** und das ***TUNNEL PASSWORD***, die in der SCCRQ des LAC enthalten sind und vergleicht sie mit denen, die im relevanten Profil angegeben sind. Der LAC macht das Gleiche mit den jeweiligen Feldern der SCCRP des LNS. Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.

Feld	Beschreibung
Hello Interval	Hier geben Sie den Zeitabstand (in Sekunden) zwischen dem Senden von zwei L2TP-HELLO-Meldungen ein, um den Tunnel offen zu halten. Verfügbare Werte sind *0* bis *255*, der Standardwert ist *30*. Der Wert *0* bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.
Data Packets Sequence Numbers	Hier können Sie festlegen, ob das Gateway für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folgenummern benutzt oder nicht. Zur Auswahl stehen *disabled* (Standardwert) und *enabled*.
Minimum Time Between Retries	Hier können Sie die Mindestzeit (in Sekunden) eingeben, die das Gateway wartet, bevor es ein L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut aussendet. Die Wartezeit wird dynamisch verlängert, bis sie die ***Maximum Time Between Retries*** erreicht hat. Unabhängig von der aktuellen Wartezeit werden keine weiteren Versuche unternommen, falls der ***Maximum Retry Count*** erreicht wurde. Verfügbare Werte sind *1* bis *255*, der Standardwert ist *1*.
Maximum Time Between Retries	Hier können Sie die maximale Zeit (in Sekunden) eingeben, die das Gateway wartet, bevor es ein L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut aussendet. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *16*.

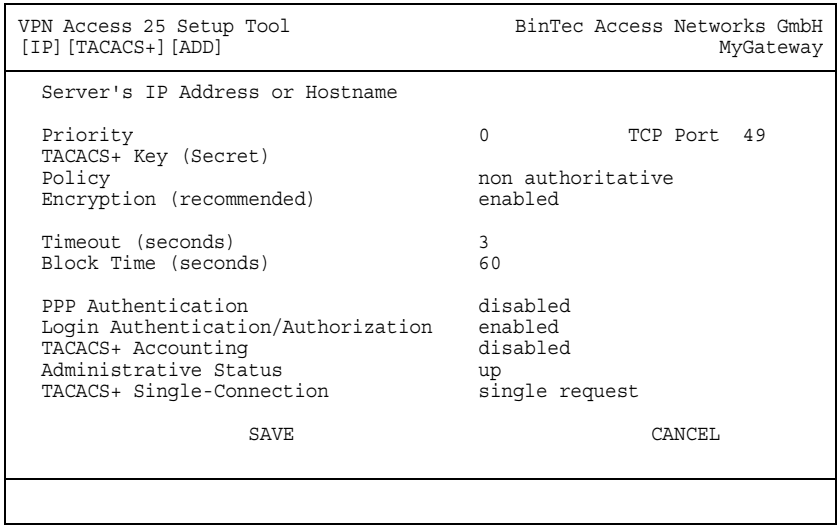
Feld	Beschreibung
Maximum Retry Count	Hier können Sie festlegen, wie oft das Gateway maximal versucht, ein L2TP-Steuerpaket erneut auszusenden, für das es keine Bestätigung erhalten hat. Wenn diese Zahl erreicht wird, ohne eine Antwort zu erhalten, erfolgt ein Timeout des Tunnels. Verfügbare Werte sind *1* bis *255*, der Standardwert ist *5*.

Tabelle 2-2: ***L2TP ➜ TUNNEL PROFILES ➜ ADD/EDIT***

2.2 TACACS+

Das TACACS+ Protokoll ermöglicht die Zugriffssteuerung von Gateways, Netzzugangsservern (NAS) und anderen Netzwerkkomponenten über einen oder mehrere zentrale Server. TACACS+ bietet Authentifizierungs-, Autorisierungs- und Abrechnungsdienste.

Die Konfiguration eines TACACS+ Servers wird über das Menü ***IP ➜ REMOTE AUTHENTICATION (RADIUS/TACACS+) ➜ TACACS+ AUTHENTICATION AND AUTHORIZATION ➜ ADD/EDIT*** vorgenommen.



Das Menü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Server's IP Address or Hostname	Hier geben Sie die IP-Adresse des TACACS+ Servers ein, der für eine AAA-Anforderung (Authentifizierung, Autorisierung, Abrechnung) abgefragt werden soll.
Priority	Hier weisen Sie dem aktuellen TACACS+ Server eine Priorität zu. Der Server mit dem niedrigsten Wert ist der erste, der für die TACACS+ AAA-Anforderung benutzt wird. Falls er keine Antwort gibt oder der Zugriff verweigert wurde (nur im nichtautoritativen Fall, siehe auch das Feld ***POLICY***), wird der Eintrag mit der nächstniedrigeren Priorität genutzt. Verfügbare Werte sind *0* bis *9*, der Standardwert ist *0*.

Feld	Beschreibung
TCP Port	Der für das TACACS+ Protokoll benutzte Standard-TCP-Port ist auf *49* eingestellt. Dieser Wert kann nicht verändert werden.
TACACS+ Key (Secret)	Hier geben Sie das Passwort ein, welches benutzt wird, um den Datenaustausch zwischen dem TACACS+ Server und dem Netzzugangsserver (Ihrem Gateway) zu authentifizieren und (falls zutreffend) zu verschlüsseln. Die maximale Länge des Eintrags ist 32 Zeichen.
Policy	Hier können Sie die Interpretation der TACACS+ Antwort auswählen. Verfügbare Werte sind *authoritative* und *non authoritative*. Wenn in diesem Feld *authoritative* eingetragen ist, wird eine negative Antwort auf eine Anfrage akzeptiert. Dies ist nicht notwendigerweise der Fall, wenn die Einstellung *non authoritative* (Standardwert) lautet. In diesem Fall wird der nächste TACACS+ Server abgefragt, bis eine autoritative Antwort kommt. Ist ***POLICY*** auf *non authoritative* gesetzt und keiner der Server liefert eine positive Antwort, oder ist keiner der Server erreichbar, werden die lokal konfigurierten SNMP Communities auf passende Zugangsinformation überprüft.

Feld	Beschreibung
Encryption (recommended)	Hier können Sie festlegen, ob der Datenaustausch zwischen dem TACACS+ Server und dem NAS verschlüsselt werden soll oder nicht. Verfügbare Werte sind *enabled* (Standardwert) und *disabled*. Falls *enabled* eingestellt wird, werden die TACACS+ Pakete mit MD5 verschlüsselt. Andernfalls - bei Einstellung auf *disabled* - werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung empfohlen.
Timeout (seconds)	Hier geben Sie die Zeit ein, wie lange der NAS auf eine Antwort von TACACS+ wartet. Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+ Server abgefragt und der aktuelle Server in einen *blocked*-Status versetzt (***TACACSPSERVEROPERSTATUS*** = *blocked*). Verfügbare Werte sind *1* bis *60*, der Standardwert ist *3*.
Block Time (seconds)	Hier geben Sie die Zeit ein, wie lange der aktuelle Server in einem blockierten Status bleibt. Nach Ende der Blockierungsdauer wird der Server in den Status versetzt, der im Feld ***ADMINISTRATIVE STATUS*** angegeben ist (siehe unten). Verfügbare Werte sind *0* bis *3600*, der Standardwert ist *60*. Der Wert *0* bedeutet, dass der Server nie in einen *blocked*-Status versetzt wird.
PPP Authentication	Diese Funktion wird von der **Systemsoftware 7.1.12** nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert.

Feld	Beschreibung
Login Authentication/Authorization	Hier können Sie festlegen, ob der aktuelle TACACS+ Server für die Login-Authentifizierung zu einem Gateway benutzt werden soll. Zur Auswahl stehen *enabled* (Standardwert) und *disabled*.
TACACS+ Accounting	Diese Funktion wird von der **Systemsoftware 7.1.12** nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert.
Administrative Status	Hier können Sie den Status auswählen, in den der Server versetzt werden soll: falls die Einstellung *up* lautet, wird der dazugehörige Server für Authentifizierung, Autorisierung und Abrechnung gemäß Priorität (siehe Feld ***PRIORITY***) und aktuellem Betriebsstatus benutzt. Andernfalls wird dieser Eintrag für TACACS+ AAA-Anforderungen nicht berücksichtigt. Zur Auswahl stehen *up* (Standardwert) und *down*.
TACACS+ Single-Connection	Hier können Sie festlegen, ob mehrere TACACS+ Sitzungen (aufeinanderfolgende TACACS+ Anforderungen) gleichzeitig über eine einzige TCP-Verbindung unterstützt werden. Falls mehrere Sitzungen nicht über eine einzige TCP-Verbindung gemultiplext werden, wird für jede TACACS+ Sitzung eine neue Verbindung aufgebaut und am Ende der jeweiligen Sitzung abgebaut. Zur Auswahl stehen *multiple requests* und *single request* (*single request* ist Standardwert und wird für die meisten Anwendungen empfohlen).

Tabelle 2-3: ***IP ➜ REMOTE AUTHENTICATION (RADIUS/TACACS+) ➜ TACACS+ AUTHENTICATION AND AUTHORIZATION ➜ ADD/EDIT***

2.3 Artem-Access-Point-Erkennung

Dem Setup Tool-Hauptmenü wurde ein neues Untermenü hinzugefügt: External Systems. Mit der Systemsoftware 7.1.12 enthält es ein Menü für die Erkennung von Artem Access Points, die sich im gleichen Netz befinden wie Ihr Gateway. Nachdem ein Access Point erkannt wurde, kann eine Anzahl bestimmter Basisparameter auf dem Access Point konfiguriert werden (vorausgesetzt, Sie kennen das Administratorpasswort).

Erkennung

Nachdem Sie eine Access Point-Erkennung ablaufen ließen, können Sie die erkannten Geräte konfigurieren (Knotenname, IP-Adresse, Netzmaske und Gateway-Adresse). Die Erkennungsfunktion (Discovery) wird im Menü ***External Systems*** ➜ ***Artem Access Point Discovery/Configuration*** ➜ ***Initiate Discovery*** gestartet:

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[EXT][ARTEM AP][DISCOV]: Artem AP Discovery                   MyGateway

 Press 'd' to run discovery on selected interface


  Interface      Operation      Result              Last Run

  ISP            none           no Error            10/29/04 13:57:55
  en0-2          none           no Error            10/29/04 13:57:55


     ADD                DELETE              EXIT
```

Das Menü zeigt folgende Details über die konfigurierten Einträge an:

Spalte	Beschreibung
Interface	Diese Spalte zeigt den Namen der Schnittstelle an, die für Artem-Access-Point-Erkennung konfiguriert ist. Der zur Identifizierung der Schnittstelle angezeigte Name ist die ***ifDescr*** aus der Tabelle ***ifTable***.

Spalte	Beschreibung
Operation	Diese Spalte zeigt an, ob gerade eine Erkennung abläuft. Sie wird automatisch aktualisiert, um zu melden, wenn die Erkennungsoperation abgeschlossen ist. Die Spalte kann folgende (nur lesbare) Werte annehmen: ■ *none*: An dieser Schnittstelle läuft gerade keine Erkennung. ■ *discovery*: An dieser Schnittstelle läuft gerade eine Erkennungsoperation.
Result	Diese Spalte zeigt das Ergebnis der Erkennungsoperation an. Sie wird automatisch aktualisiert; die Werte können nur gelesen werden: ■ *no Error*: Keine Erkennung gestartet oder Erkennung war erfolgreich. ■ *Dest. unreachable*: Die Schnittstelle ist derzeit nicht benutzbar, d. h. die Schnittstelle ist nicht in Betrieb, hat keine IP-Adresse zugewiesen bekommen oder hat keine passende direkte Route. Die Anforderung konnte nicht abgesandt werden. Die genaue Fehlerursache ist in der Syslog zu finden.
Last Run	Diese Spalte zeigt Datum und Uhrzeit der letzten erfolgreichen Erkennung an. Falls bis zu diesem Zeitpunkt keine Erkennung durchgeführt wurde oder die erste Erkennung erfolglos war, wird hier eine leere Zeichenkette angezeigt.

Tabelle 2-4: ***External Systems ➜ Artem Access Point Discovery/Configuration ➜ Initiate Discovery***

Durch Hervorheben eines Eintrags und Drücken der **d**-Taste auf Ihrer Tastatur können Sie den Erkennungsprozess für den ausgewählten Eintrag starten.

Mit dem Menü ***External Systems*** ➜ ***Artem Access Point Discovery/Configur-ation*** ➜ ***Initiate Discovery*** ➜ ***ADD/EDIT*** können Sie der Access Point-Erkennung eine Instanz hinzufügen oder eine vorhandene bearbeiten:

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[EXT][ARTEM AP][DISCOV][ADD]: Add Interfaces for
                              Artem AP Discovery              MyGateway

  Interface                   en1-0
  Operation                   none


                    SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

Feld	Beschreibung
Interface	Hier können Sie festlegen, für welche der IP-Schnittstellen die Erkennung durchgeführt werden soll. Alle Access Points, die das Gateway über diese Schnittstelle kontaktiert, werden erkannt.

Feld	Beschreibung
Operation	Hier können Sie festlegen, ob die Erkennung unmittelbar nach der Speicherung des Eintrags gestartet werden soll, d. h. sobald Sie mit ***SAVE*** bestätigt haben. Beachten Sie, dass erkannte Access Points nicht in der MIB gespeichert werden, d. h. die Erkennung muss nach einem erneuten Booten Ihres Gateways wiederholt werden. Zur Auswahl stehen: ■ *none* (Standardwert): Nachdem der Eintrag gespeichert wurde, wird keine Operation durchgeführt. Die Erkennung kann, wie oben beschrieben, auch später gestartet werden. ■ *discovery*: Die Erkennungsoperation wird an dieser Schnittstelle unmittelbar nach Speicherung des Eintrags durchgeführt.

Tabelle 2-5: ***EXTERNAL SYSTEMS ➜ ARTEM ACCESS POINT DISCOVERY/CONFIGURATION ➜ INITIATE DISCOVERY ➜ ADD/EDIT***

Konfiguration

Nachdem Sie die Erkennung an allen vorgesehenen Schnittstellen durchgeführt haben, können Sie das Ergebnis der Erkennung mit dem Menü ***EXTERNAL SYSTEMS ➜ ARTEM ACCESS POINT DISCOVERY/CONFIGURATION ➜ VIEW/CONFIGURE*** anzeigen lassen und die erkannten Access Points konfigurieren:

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[EXT][ARTEM AP][CONF]: Discovered Artem Access Points          MyGateway

Interface   AP MAC Address      Node Name         IP Address       / Mask

en0-2       00:01:cd:0e:a5:01  XAIR AP1          192.168.0.1      / 24
en0-2       00:01:cd:0e:af:02  XAIR AP2          192.168.0.20     / 24
en0-2       00:01:cd:0f:e4:03  XAIR AP3          192.168.0.30     / 24
en0-2       00:01:cd:0f:e4:ea  XAIR 4            192.168.0.30     / 24


EXIT
```

In der Liste sind alle erkannten Access Points, die Schnittstelle, an denen sie gefunden wurden, ihre MAC-Adressen, ihre aktuellen Knotennamen und ihre aktuellen IP-Konfigurationen aufgeführt. Bestimmte Werte eines Access Points können Sie ändern, indem Sie einen Eintrag hervorheben und mit **Return** bestätigen:

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[EXT][ARTEM AP][CONF][EDIT]: Artem AP Configuration            MyGateway

  Interface          en0-2
  AP MAC Address     00:01:cd:0e:a5:01
  IP Status          unknown
  Operation          none
  Result             no Error
  Last Change        10/29/04 14:13:29

  Node Name          XAIR AP1
  IP Address         192.168.0.1
  Netmask            255.255.255.0
  Gateway Address
  Admin. Password

        SET                    REFRESH                  CANCEL
```

Das Menü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Interface	Der Wert dieses Feldes kann nur gelesen werden. Dieses Feld nennt die Schnittstelle, an die der Access Point angeschlossen ist.
AP MAC Address	Der Wert dieses Feldes kann nur gelesen werden. Dieses Feld nennt die MAC-Adresse des Access Points.
IP Status	Der Wert dieses Feldes kann nur gelesen werden. Dieses Feld zeigt an, auf welche Art der Access Point seine IP-Konfiguration erhalten hat. Mögliche Werte sind: ■ *unknown*: Die fragliche Information liegt im Access Point nicht vor. ■ *static*: Die IP-Konfiguration wurde manuell durchgeführt. ■ *DHCP Lease*: Die IP-Konfiguration wurde durch das DHCP (Dynamic Host Configuration Protocol) vorgenommen. ■ *DHCP Failed:* Die IP-Konfiguration durch das DHCP ist fehlgeschlagen und eine Rückfall-IP-Konfiguration wurde benutzt.

Feld	Beschreibung
Operation	Der Wert dieses Feldes kann nur gelesen werden. Dieses Feld zeigt die Operation an, die momentan ausgeführt wird; es wird abhängig vom Operationsstatus aktualisiert, wenn Sie ***REFRESH*** anklicken. Mögliche Werte sind: ■ *none*: Im Moment läuft keine Operation ab. ■ *set in progress*: Eine "set"-Operation läuft gerade, d. h. auf dem Access Point werden Parameter konfiguriert.

Feld	Beschreibung
Result	Der Wert dieses Feldes kann nur gelesen werden. Dieses Feld zeigt das Ergebnis einer "set"-Operation an. Mögliche Werte sind: ■ *no Error*: Der Access Point hat eine erfolgreiche Operation gemeldet oder ist noch nicht konfiguriert. ■ *no Reply*: Der Access Point hat nicht geantwortet. ■ *Access denied*: Der Access Point hat einen Autorisierungsfehler gemeldet. ■ *invalid IP parameters*: Es gibt ein Problem mit den vorgesehenen IP-Parametern (IP-Adresse, Netzmaske oder Gatewayadresse). ■ *Dest. unreachable*: Der Access Point kann aus internen Gründen nicht erreicht werden (z. B. die Schnittstelle, an die der Access Point angeschlossen ist, ist außer Betrieb). Zum Access Point kann keine Einstellanforderung gesandt werden. ■ *other AP error*: Der Access Point antwortet auf die Einstellanforderung mit einem unerwarteten oder unspezifischen Fehler. ■ *internal Error*: Ein internes Problem des Gateways hat die Einstelloperation verhindert.
Last Change	Der Wert dieses Feldes kann nur gelesen werden. Dieses Feld zeigt Datum und Uhrzeit an, zu denen der Access Point erkannt oder zuletzt konfiguriert wurde.

Feld	Beschreibung
Node Name	Hier können Sie den Namen des erkannten Access Points ändern.
IP Address	Hier können Sie die IP-Adresse des erkannten Access Points ändern.
Netmask	Hier können Sie die Netzmaske des erkannten Access Points ändern.
Gateway Address	Hier können Sie die Gatewayadresse des erkannten Access Points ändern.
Admin. Password	Hier müssen Sie das Administrator-Passwort des Access Points eingeben. Andernfalls kann die Einstelloperation nicht durchgeführt werden.

Tabelle 2-6: ***EXTERNAL SYSTEMS ➜ ARTEM ACCESS POINT DISCOVERY/CONFIGURATION ➜ VIEW/CONFIGURE ➜ EDIT***

Nachdem Sie die Einstelloperation mit der SET-Schaltfläche gestartet haben, wird in der Hilfezeile die Meldung `Set in progress...` angezeigt und der Wert von ***OPERATION*** wechselt auf *set in progress*. Um das Ergebnis der Einstellanforderung anzeigen zu lassen, klicken Sie auf ***REFRESH***: ***OPERATION*** wechselt zurück auf *none* und ***RESULT*** zeigt das Ergebnis der Einstellanforderung an.

2.4 Neuer IPSec Peer Type

Um es mehr als einem IPSec-Partner zu ermöglichen, sich mit der identischen Peer-Konfiguration mit einem IPSec-Gateway zu verbinden, führt Systemsoftware 7.1.12 einen "dynamischen Peer" ein.

Mittels einer spezifischen Konfiguration können sich mehrere Clients mit einem IPSec-Gateway verbinden und dazu ein und dieselbe Peer-Konfiguration auf dem Gateway verwenden. Ein einziger Parameter bestimmt, ob ein Peer als dynamischer Peer betrachtet wird oder nicht: ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ PEER SPECIFIC SETTINGS*** bietet dazu den Parameter ***SPECIAL***

PEER TYPE. Er kann zwei Werte annehmen: *None* (Defaultwert) und *Dynamic Client*.

Abgesehen davon, dass Sie bei der Konfiguration eines Peers als dynamischen Peer der Wert *Dynamic Client* setzen müssen, müssen Sie Folgendes Beachten:

- Die Konfiguration des dynamischen Peers darf keine Peer ID und keine Peer-IP-Adresse enthalten.
  Die CLients, die sich mit dem Gateway verbinden, müssen jedoch über eine Peer ID verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen.
- Der resultierende Peer auf dem Gateway würde nun auf alle eingehenden Tunnel-Requests zutreffen. Daher ist es notwendig, ihn an das Ende der IPSec-Peer-Liste zu stellen. Andernfalls wären alle in der Listen folgenden Peers inaktiv.

Dies bedeutet, dass ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ADD/EDIT***: ***PEER ADDRESS*** und ***PEER IDS*** bei der Konfiguration eines dynamischen Peers leer gelassen werden müssen.

Das Gateway behandelt Tunnel-Requests, auf die ein dynamische Peer zutrifft, wir folgt:

- Wenn ein eingehender IKE Request einem Peer entspricht, dessen *Special Peer Type* auf *Dynamic Client* gesetzt ist, wird der Peer-Eintrag dupliziert und ein temporärer Peer angelegt.
- Die Peer-ID des neuen Peers wird auf die ID des sich verbindenden Clients gesetzt.
- Der Peer Type des neu erstellten (temporären) Peers wird in der MIB auf "fixed" gesetzt.
- Die Peer-Priorität wird auf einen Wert gesetzt, der sicherstellt, dass der temporäre Peer mit höherer Priorität behandelt wird als andere Peers, inklusive des dynamischen "Parent"-Peers. Dies stellt sicher, dass der sich verbindende Client auch mit dem temporären Peer assoziiert wird.
- In Abhängigkeit von der Einstellung des dynamischen Peers für den Parameter Virtual Interface, werden folgende Einstellungen vorgenommen:

- Für ***VIRTUAL INTERFACE***: *yes* - Für den temporären Peer wird eine Host-Route mit der Phase-1-Adresse des Clients als Zieladresse angelegt.
- Für ***VIRTUAL INTERFACE***: *no* - Die Traffic Liste Entries, die mit dem dynamischen Peer assoziiert sind, werden in die Traffic List des temporären Peers kopiert.

Sobald der neue Peer und seine Traffic Liste bzw. seine Route erstellt worden sind, ist die weitere Handhabung die gleiche wie bei einem statischen IPSec Peer.

Achtung!

Da es in diesem Fall keinen Unterschied in der Konfiguration der Clients gibt, verwenden alle Clients die gleiche Authentisierungsinformationen.

Mit Preshared Key Authentication kann dies ein Problem bedeuten, da die Authentisierungsinformationen symmetrisch sind, d. h. beide Seiten (Client und Gateway) das gleiche Passwort verwenden. Wird die Konfiguration nur eines Clients bekannt, sind die Authentisierungsdaten der gesamten auf dem dynamischen Peer aufbauenden Infrastruktur einem potentiellen Angreifer bekannt.

Wir raten daher nachdrücklich von der Verwendung von Preshared Key Authentication mit dynamischen Peers ab.

2.5 Unterstützung von Registration-Authority-Zertifikaten im SCEP

Systemsoftware 7.1.12 unterstützt Registration-Authority-Zertifikate bei der Verwendung von SCEP. Dies erleichtert die SCEP-kontrollierte Zertifikatausstellung, da nun alle diejenigen Certificate Authorities unterstützt werden, die Zertifikatanträge über eine RA abwickeln.

Wenn eine CA Zertifikatanträge über eine eigene RA abwickelt, so muss der Client (in diesem Fall das Gateway) wissen, welche Zertifikate zur Kommunikation mit der RA verwendet werden müssen.

RA-Zertifikate werden entweder automatisch durch das Gateway erkannt (***CA-CERTIFICATE*** = *(download)*) oder manuell festgelegt (Auswahl des entsprechenden Eintrags in ***CA-CERTIFICATE***).

Die Auswahl von RA-Zertifikaten hat nur für SCEP-basierte Zertifizierung Bedeutung, daher finden sich die entsprechenden Konfigurationsoptionen im Menü ***IPSec ➜ Certificate and Key Management ➜ Key Management ➜ REQUEST CERT***:

```
VPN Access 25 Setup Tool          BinTec Access Networks GmbH
[IPSEC][CERTMGMT]..[ENROLL]: IPsec Configuration -
                          Certificate Enrollment

 Key to enroll:              1 (automatic key RSA 1024 (e 65537))

 Method:       SCEP        CA-Certificate: (download)
 Autosave:     on          CA-Domain:       myca.com
 Password:     supersecret
 Subject Name:

 Subject Alternative Names (optional):
   Type   Value
   IP     192.168.0.254
   DNS    VPN25.
   NONE

 State of Last Enrollment:   none
 Server:
 Certname:

                    Start                                Exit
```

Beachten Sie, dass *SCEP* unter ***Method*** ausgewählt sein muss, um die Optionen für die Konfiguration von RA-Zertifikaten zu sehen.

Solange das CA-Zertifikat automatisch geladen werden soll ***(download)***, ändert sich das Menü jedoch nicht, da alle möglicherweise relevanten zertifikate aus der Certificate Chain entnommen werden.

Wenn Sie jedoch ein auf dem Gateway bereits installiertes Zertifikat als CA-Zertifikat angeben, ändert sich das Menü (der Screenshot enthält Beispielwerte):

```
VPN Access 25 Setup Tool          BinTec Access Networks GmbH
[IPSEC][CERTMGMT]..[ENROLL]: IPsec Configuration -
                          Certificate Enrollment

 Key to enroll:          1 (automatic key RSA 1024 (e 65537))

 Method:        SCEP     CA-Certificate:            2 (ca@home)
 Autosave:      on       RA-Certificate (Sign):     3 (ca@home)
 Password:      secret   RA-Certificate (Encrypt): 4 (ca@home)
 Subject Name:

 Subject Alternative Names (optional):
   Type   Value
   IP     192.168.0.254
   DNS    VPN25.
   NONE

 State of Last Enrollment:   none
 Server:
 Certname:

                    Start                                Exit
```

Das menü enthält nun die folgenden zusätzlichen Felder:

Feld	Beschreibung
`RA-Certificate (Sign)`	Nur wenn ***CA-CERTIFICATE*** `nicht =` *(download)*. Hier können Sie eine Zertifikat für die Signierung der Kommunikation mit der RA auswählen. Als Standardeinstellung wird hier das CA-Zertifikat verwendet.

Feld	Beschreibung
`RA-Certificate (Encrypt)`	Nur wenn ***RA-CERTIFICATE (SIGN)*** `nicht =` *(use CA cert).* Wenn Sie ein eigenes Zertifikat zur Signierung der Kommunikation mit der RA verwenden, haben Sie hier die Möglichkeit, ein weiteres zur Verschlüsselung der Kommunikation auszuwählen. Als Standardeinstellung wird das selbe Zertifikat wie zur Signierung verwendet, aber Sie können jedes andere auf dem Gateway installierte Zertifikat auswählen.

2.6 Neue Zeitsynchronisationsoptionen

Die Optionen für die Aktualisierung der Systemzeit des Gateways von verschiedenen Quellen wurden wesentlich erweitert, um mehrere Zeitserver konfigurieren zu können.

Das Menü für die Konfiguration der Zeitabfrageoptionen wurde erweitert, es wird über das ***SYSTEM***-Menü aufgerufen (***SYSTEM*** ‹ ***TIME AND DATE***):

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SYSTEM][TIME]: Control System Time and Date          MyGateway

 Current System Time: Wed 2005/Feb/28 19:19:37  set by: None

 Change  System Time:     2005/Feb/28       19:19:17             CHANGE


Time Update Interval          :      86400     Seconds
Update System Time from ISDN :       disabled
System Time Offset from GMT   :      0         Seconds

Time Servers:

   Name/Address                                 Protocol
1:                                              SNTP
2:                                              SNTP
3:                                              SNTP

         SAVE                           CANCEL
```

Die erste Zeile im Menüfenster zeigt die aktuelle Systemzeit an. Diese kann manuell in der zweiten Zeile geändert werden. Durch Bestätigen mit ***CHANGE*** werden die Änderungen übernommen.

Da von einem Gateway ohne Hardware Real Time Clock (Liste der Gateways ohne Real Time Clock) die Systemzeit beim Neubooten zurückgesetzt wird, unterstützt die **Systemsoftware 7.1.12** die Synchronisation mit mehreren Zeitservern und über ISDN. Das Setup Tool ermöglicht die Konfiguration von drei Zeitservern, weitere können über die SNMP-Shell konfiguriert werden. Diese Optionen werden in der unteren Hälfte des Menüfensters konfiguriert. Das Menü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Time Update Interval	Hier geben Sie das Zeitintervall ein, in dem das Gateway versucht, sich auf einen der konfigurierten Zeitserver zu synchronisieren (in Sekunden). Der Standardwert ist *86400*.

Feld	Beschreibung
Update System Time from ISDN	Hier können Sie festlegen, ob die Zeitinformation, die am Ende eines ISDN-Rufs gesandt wird, zur Aktualisierung der Systemzeit benutzt wird. Diese Option wird nur solange genutzt, wie nach einem Neustart kein erfolgreiches Update von einem Zeitserver empfangen wurde Verfügbare Werte sind *enabled* (freigegeben) und *disabled* (gesperrt), der Standardwert ist *disabled*.
System Time Offset from GMT	Hier geben Sie die Abweichung zwischen der lokalen Uhrzeit und GMT ein. Die Werte werden in Sekunden eingegeben; Werte zwischen *1* und *23* werden jedoch als Stunden interpretiert und nach dem Speichern der Konfiguration in Sekunden umgewandelt. Es können positive oder negative Werte eingegeben werden, der Standardwert ist *0*.
Name/Address	Hier können Sie bis zu drei Zeitserver eingeben, entweder durch ihre Domainnamen oder durch ihre IP-Adresse. Es gibt keine vorkonfigurierten Server.

Feld	Beschreibung
Protocol	Hier können Sie das Protokoll auswählen, welches für die Abfrage der Zeitserver benutzt wird. Zu Auswahl stehen: ■ *SNTP* - Dieser Server nutzt das Simple Network Time Protocol. ■ *disabled* - Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt. ■ *TIME/UDP* - Dieser Server nutzt das Time/UDP-Protokoll. ■ *TIME/TCP* - Dieser Server nutzt das Time/TCP-Protokoll.

Tabelle 2-7: ***SYSTEM → TIME AND DATE***

Liste der Gateways ohne Real Time Clock

Die folgenden Gateways verfügen nicht über eine Real Time Clock:

- **X1000 II**
- **X1200 II**
- **X2250**
- **X2300** compact with serial numbers equal to or higher than "X2C25...."
- **X2300s**
- **X2300i** compact with serial numbers equal to or higher than "X2I25..."
- **X2300is** compact with serial numbers equal to or higher than "X2Y25..."
- **X2404** comopact with serial numbers equal to or higher than "X2D21..."
- **X2500**
- **VPN Access 5**, **25** and **100**
- **X2301**
- **X2302**.

2.7 Kontinuierlicher Ping

Vor der Systemsoftware 7.1.12 konnte der Ping-Daemon nur für eine beschränkte Zahl von Echoanforderungen eingesetzt werden (zwischen 1 und 65535). Dies wurde geändert, so dass an den entfernten Host ein kontinuierlicher Ping gesandt werden kann.

Hinweis

Beachten Sie, dass der Ping-Daemon nicht mit dem Ping-Befehl identisch ist, den Sie von der SNMP-Shell aus nutzen können. Der Ping-Daemon wird durch Einträge in die ***biboPingTable*** konfiguriert und läuft nur im Hintergrund ab.

Um den Ping-Daemon so zu konfigurieren, dass er einen kontinuierlichen Ping aussendet, kann die Variable ***biboPingPacketCount*** jetzt den Wert *0* annehmen. Damit wird der Pingzähler auf unbegrenzt ("unlimited") gesetzt.

2.8 Jitter-Daemon

Die Systemsoftware 7.1.12 beinhaltet einen Jitter-Daemon.

Um den "Jitter" zu berechnen (die Abweichungen des Antwortzeitverhaltens (Round Trip Time) zwischen zwei Hosts), werden vom Gateway ICMP-Echoanforderungen an einen bestimmten entfernten Host gesandt.

Die Konfiguration dieser Funktion wird vom Setup Tool nicht unterstützt. Informationen über die verfügbaren Konfigurationsparameter finden Sie in der **MIB-Referenz** für **Systemsoftware 7.1.12**, Abschnitt **IP**: ***biboJitterAdminTable***, ***biboJitterCtrlTable*** und ***biboJitterStatsTable***.

2.9 ATM QoS - VBR 3

ATM QoS (Quality of Service) bietet eine Anzahl von Dienstklassen an; aufgrund dieser Klassen wird eine Priorisierung des Datenverkehrs durch Traffic Shaping durchgeführt. Mit der Systemsoftware 7.1.12 wird die Unterstützung der Kategorie VBR.3 eingeführt.

VBR.3 verändert das ursprüngliche Verhalten von VBR.1 in der Weise, dass es "Best Effort Scheduling" durch CLP-Kennzeichnung (Cell Loss Priority, Zellverlustpriorität) nutzt.

Hinweis

Informationen über die ATM QoS-Dienstklassen sind in den **Release Notes 7.1.1** enthalten, die unter www.bintec.net zum Download zur Verfügung stehen.

VBR.3 bringt folgendes Verhalten mit sich:

Unter Berücksichtigung der Verkehrsparameter PCR (Peak Cell Rate, Spitzenzellenrate), SCR (Sustainable Cell Rate, Dauerzellrate) und MBS (Maximum Burst Size, maximale ununterbrochene Sendedauer mit PCR) als begrenzende Faktoren überträgt das Gateway den gesamten Verkehr, der innerhalb der Grenzen des "Traffic Contracts" liegt, mit auf *0* gesetztem CLP-Flag, d. h. die ATM-Zellen werden nicht für ein potentielles Verwerfen durch das an das Gateway angeschlossene ATM-Netz gekennzeichnet. Jeglicher Datenverkehr, der die PCR überschreitet, wird vom Gateway selbst verworfen, während bei Datenverkehr, der <SCR+MBS> überschreitet, das CLP-Flag auf *1* gesetzt wird, d. h. diese Zellen können durch das an das Gateway angeschlossene ATM-Netz verworfen werden.

Um VBR.3 auf ein ATM-Profil anzuwenden (das Profil wird durch eine Kombination aus VCI und VPI festgelegt) können Sie bei ***ATM*** ➜ ***ATM QoS*** ➜ ***ADD/EDIT***: ***ATM SERVICE CATEGORY*** die Option *Variable Bit Rate (VBR.3)* wählen.

2.10 DHCP-Hostname

Manche ISPs fordern, dass DHCP-Meldungen, die vom Client ausgesandt werden, einen Hostnamen enthalten (DHCP Option 12). Wenn dieser Hostname nicht übertragen wird, wird dem Client keine IP-Adresse zugeteilt. Systemsoftware 7.1.12 erfüllt diese Anforderung.

Das Setup Tool-Menü für die Konfiguration einer Ethernet-Schnittstelle wurde dementsprechend geändert. Falls die ***IP-CONFIGURATION*** auf *DHCP* eingestellt

ist, wird das Feld ***DHCP HOSTNAME*** angezeigt (der Screenshot zeigt Beispielwerte):

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[LAN]: Configure LAN Interface                                MyGateway

      IP-Configuration            DHCP
           local IP-Number        192.168.0.254
           local Netmask          255.255.255.0
           DHCP MAC Address
           DHCP Hostname          Client_1
           Encapsulation          Ethernet II
           Mode                   Auto


      Bridging                    disabled

      Virtual Interfaces >

                SAVE                                CANCEL
```

In diesem Feld können Sie den Hostnamen eingeben, der vom ISP gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.

2.11 Wiederholung einer HTML-Wizard-Konfiguration

Bisher war es nicht möglich, eine Wizard-Konfiguration, die bereits auf dem Gateway gespeichert war, als Grundlage für einen Neuablauf des HTML-Wizard zu nutzen. Bei jedem erneuten Ablauf des HTML-Wizard ignorierte dieser die Parameter einer bereits vorhandenen Konfiguration. Die Systemsoftware 7.1.12 führt einen Neuablauf ("Rerun") des HTML-Wizard ein, der es ermöglicht, bestimmte Parameter einer früheren Wizardkonfiguration beizubehalten und gleichzeitig andere zu ändern.

Am Ende eines jeden Wizardablaufs werden Sie jetzt aufgefordert, eine Erweiterung für die Datei einzugeben, mit der die alte Wizardkonfiguration im Flash-ROM gespeichert werden soll. Damit ist es theoretisch möglich, eine beliebige

Zahl von Wizardkonfigurationen zu speichern - bedenken Sie aber, dass der Speicherplatz auf dem Flash-ROM begrenzt ist. Da der Wizard nur die zuletzt gespeicherte Konfiguration als Basis für einen Neuablauf nutzt (es gibt keine Möglichkeit, zwischen den Konfigurationen auszuwählen), ist es wenig sinnvoll, eine größere Zahl von Konfigurationen zu speichern.

Hinweis

Beachten Sie, dass die von Ihnen für eine bestimmte Konfiguration eingegebene Dateierweiterung keinen Einfluß darauf hat, welche Konfiguration der Wizard als Basis für einen Neuablauf nutzt. Der Wizard wählt immer die zuletzt gespeicherte Konfiguration.

Die Eingabeaufforderung für die Speicherung der vorherigen Konfiguration sieht folgendermaßen aus:

Abbildung 2-1: Eingabeaufforderung des HTML-Wizard für Konfigurationsspeicheroptionen

Wenn Sie jetzt den HTML-Wizard neu starten, werden Sie aufgefordert, einzugeben, ob der Wizard auf Basis der Werkseinstellungen starten soll oder ob er

die Einstellungen nutzen soll, die während der letzten Wizardkonfiguration vorgenommen wurden:

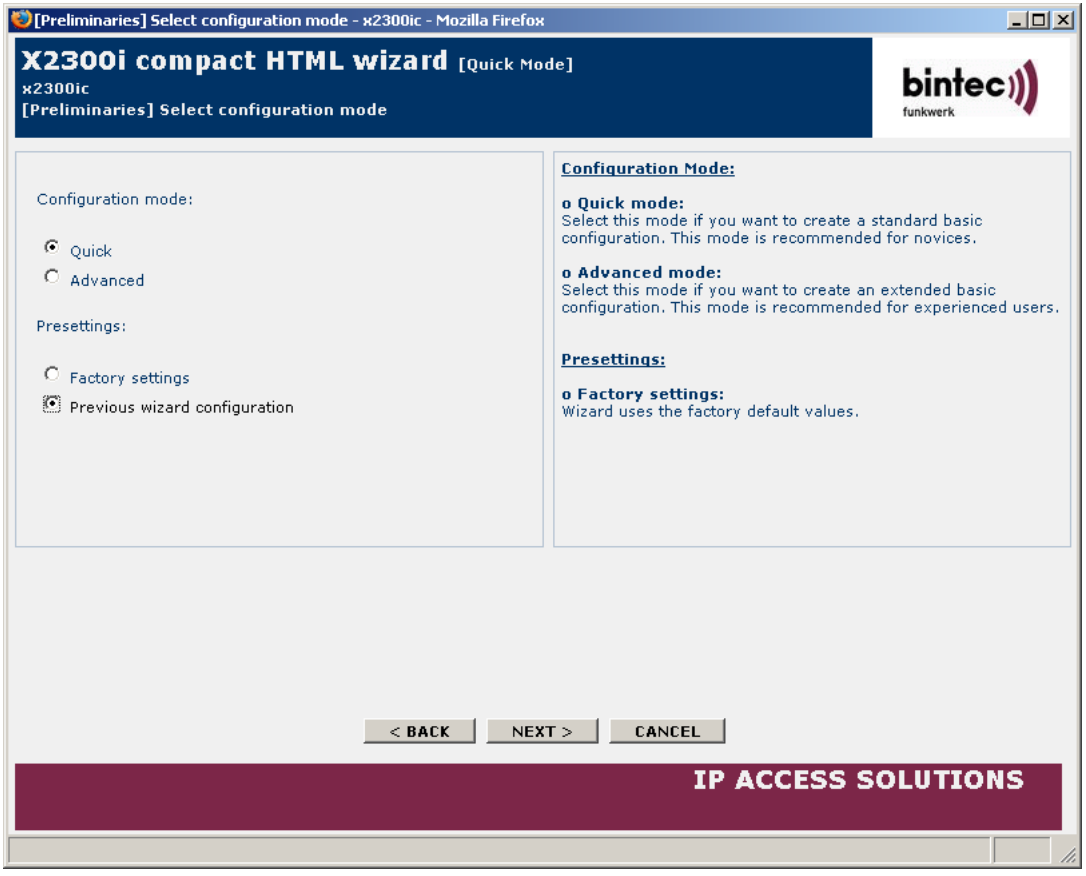


Abbildung 2-2: Konfigurationsauswahl für den HTML-Wizard

2.12 IPSec-Peer-Überwachung

Die IPSec-Menüs wurden durch detailierte Überwachungsfunktionen verbessert.

Das Überwachungsmenü (***IPSEC*** ➜ ***CONFIGURE PEERS***) wird durch Hervorheben eines Peers in der Peerliste und Eingabe von "M" aufgerufen (es muss der Großbuchstabe M sein). Das Überwachungsmenü sieht folgendermaßen aus:

```
VPN Access 25 Setup Tool                                        Bintec
[IPSEC][PEERS]: IPsec Configuration - Configure Peer List     MyGateway

 Description:    Peer_1

 Admin Status:   up           Oper Status:       dormant
 Local Address:               Remote Address:

 SAs Phase 1>    0    /0           Phase 2>     0    /0




 Messages >

 EXIT                ACTION: enable      START
```

Das Menü enthält folgende Felder:

Feld	Beschreibung
Description	Hier wird die Beschreibung des überwachten Peers angezeigt.
Admin Status	Hier wird der ***ADMIN STATUS*** des überwachten Peers angezeigt.
Oper Status	Hier wird der ***OPER STATUS*** des überwachten Peers angezeigt. Dies ist der aktuelle Betriebsstatus des Peers.
Local Address	Die lokale IP-Adresse des IPSec-Tunnels wird nur dann angezeigt, wenn sie aktuell zur Verfügung steht, d. h. wenn sie entweder statisch konfiguriert ist oder wenn der IPSec-Tunnel bereits aktiv ist.
Remote Address	Die IP-Adresse des fernen Peers wird nur dann angezeigt, wenn sie aktuell zur Verfügung steht, d.h. wenn sie entweder statisch konfiguriert ist oder wenn der IPSec-Tunnel bereits aktiv ist.
SAs Phase 1	Hier wird die Zahl der Phase-1-SAs angezeigt (*<established>*/*<total>*). Durch Hervorheben von ***PHASE 1*** und Drücken der Eingabetaste kann man auf ein detailierteres Phase-1-Überwachungsmenü zugreifen.
SAs Phase 2	Hier wird die Zahl der Phase-2-SAs angezeigt (*<established>*/*<total>*). Durch Hervorheben von ***PHASE 2*** und Drücken der Eingabetaste kann man auf ein detailierteres Phase-2-Überwachungsmenü zugreifen.

Feld	Beschreibung
ACTION	Hier können Sie einige Aktionen ausführen, die den Verbindungsstatus des Peers beeinflussen. Folgende Aktionen sind möglich: ■ *reset* - Setzt den Admin Status des Peers auf *down;* wartet, bis der Oper Status des Peer den Status *down* erreicht hat und setzt den Admin Status des Peers wieder auf *up*. ■ *enable* - Setzt den Admin Status des Peers auf *up.* ■ *disable* - Setzt den Admin Status des Peers auf *down*. ■ *set up* - Setzt den Admin Status des Peers auf *dialup*, was die Einrichtung eines Phase-1-SA für den Tunnel auslöst.

Tabelle 2-8: ***IPSec ➜ Configure Peers ➜ Monitoring Menu***

Die ***Phase 1>***-Untermenüverknüpfung führt zum IKE-SA-Überwachungslistenmenü, welches nur die IKE SAs für den aktuell überwachten Peer anzeigt. SAs für andere Peers können in der Liste auftauchen, solange die ferne ID für diese SAs noch nicht bekannt ist. Sobald die ferne ID bekannt ist, werden dieses SAs aus der Peeransicht gelöscht.

Die ***Phase 2>***-Untermenüverknüpfung führt zum IPSec-Bündellisten-Überwachungsmenü, welches dann nur die Bündel des aktuell überwachten Peers anzeigt.

Die ***Messages >-***Untermenüverknüpfung führt zum Meldungsüberwachungsmenü. Es wird mit einem Filter mit der Funktion "*peer {0}{<idx>}* "initialisiert, wobei <*idx*> der Index des aktuell überwachten Peers ist. Beachten Sie, dass das Leerzeichen am Ende der Filterfunktion wichtig ist, da ansonsten alle Peers die Filterfunktion erfüllen. Dies bedeutet, dass alle Meldungen in Bezug auf diesen

Peer und alle Meldungen für unbekannte Peers (index *0*) angezeigt werden. Um die Meldungen für unbekannte Peers zu unterdrücken, ersetzen Sie die Filterfunktion durch "*peer <idx>*".

2.13 Neue X.25-Funktionen

Unsere X.25-Implementierung wurde um einige Funktionen erweitert, wie beispielsweise die Konvertierung von X.25-Rufen in TCP-Rufe (X.25 über TCP-Gateway) oder die Übertragung von X.25-Daten über TCP-Netze (XoT).

Informationen über die neu implementierten Funktionen finden Sie im Bereich "Lösungen" unter www.bintec.de.

Bitte beachten Sie die Änderungen der Lizenzpolitik bezüglich X.25, die in “Lizenz für X.25 benötigt” auf Seite 52 beschrieben sind.

3 Änderungen

Folgende Änderungen wurden vorgenommen, um die Funktionalität Ihres Gateways zu erweitern:

3.1 Änderungen bei IPSec

3.1.1 Lizenz für IP-Adressenübertragung über ISDN

In Release 7.1.10 unserer Systemsoftware musste die Funktion, dynamisch zugewiesene IP-Adressen von IPSec Peers über den ISDN-B- oder D-Kanal zu übetragen, entfernt werden. Nach sorgfältiger Untersuchung der zugrundeliegenden Patentangelegenheiten können wir diese Funktion nun wieder anbieten.

Um den IP-Adresse-Transfer im ISDN-B -oder D-Kanal zu aktivieren, benötigen Sie eine kostenfreie Lizenz, die Sie auf den Service/Support-Seiten von www.bintec.de erhalten können. Der Lizenzmechanismus wird dort bald zur Verfügung stehen. Er wird in gleicher Weise funktionieren wie der zur Vergabe von STAC/MPPC-Lizenzen verwendete.

Informationen zur Installation der Lizenz finden Sie im Kapitel "Licenses" Ihres **Bintec Benutzerhandbuchs**.

3.1.2 Filter im Messages-Menü

Das Menü ***Monitoring and Debugging*** ➜ ***Messages*** bietet jetzt die Möglichkeit an, die angezeigten Syslog-Meldungen zu filtern. Sie können in das Feld ***Filter*** eine beliebige Zeichenkette eingeben; dann werden im darüberliegenden Meldungsanzeigebereich nur solche Meldungen angezeigt, die auch diese Zeichenkette enthalten. Zur Vereinfachung wird ein Wildcard (*) angenommen, damit auch solche Meldungen angezeigt werden, die die vorgegebene Zeichenkette als Teilkette enthalten.

3.1.3 Wildcards und leere Rufnummern im IPSec-Rückruf

Vor der **Systemsoftware 7.1.12** war es nicht möglich, Wildcards für die ISDN-Rufnummer eines IPSec-Rückrufs einzugeben. Es war auch nicht möglich, das Feld ***IPSec*** ➜ ***Configure Peers*** ➜ ***IPSec Callback***: ***Incoming ISDN Number*** völlig leer zu lassen.

3.2 Lizenz für X.25 benötigt

Bei Gateways der X-Generation-Familie stand X.25 zur Verfügung, ohne dass dafür eine Softwarelizenz erforderlich war. Dies hat sich geändert und ab der

Systemsoftware 7.1.12 muss für die Nutzung von X.25 eine Softwarelizenz gekauft und installiert werden.

Hinweis

Falls Sie einen Update von einer älternen Softwareversion auf die **Systemsoftware 7.1.12** durchführen möchten und die entsprechende Lizenz erworben haben, empfehlen wir, die Lizenz zu installieren, bevor Sie den Update vornehmen. Damit wird sichergestellt, dass alle X.25-Funktionen unmittelbar nach dem Update wieder zur Verfügung stehen.

3.3 Ping-Daemon in allen Produkten verfügbar

Mit der **Systemsoftware 7.1.12**, steht der Ping-Daemon in allen unseren Produkten zur Verfügung, die auf diesen Softwarerelease upgedated werden können.

Hinweis

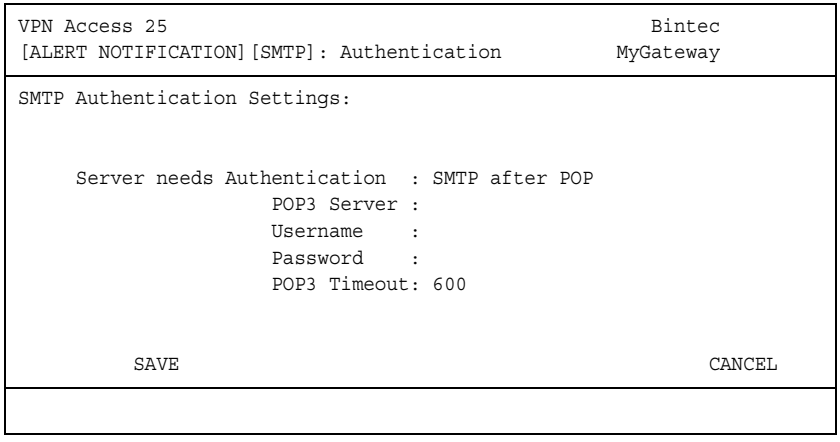
Beachten Sie, dass der Ping-Dämon nicht mit dem Ping-Befehl identisch ist, den Sie in der SNMP-Shell eingeben können. Der Ping-Dämon wird durch Einträge in die ***BIBOPINGTABLE*** konfiguriert und läuft nur im Hintergrund.

3.4 TAF-Support beendet

Die Unterstützung der TAF (Token Authentication Firewall) wird ab **Systemsoftware 7.1.12** eingestellt.

3.5 SMTP-Authentifizierungssupport für Email-Alarm

Vor der **Systemsoftware 7.1.12** wurde die SMTP-Authentifizierung durch den Email-Alarm nicht unterstützt. Dies wurde geändert und die Authentifizierung kann im neu geschaffenen Untermenü (***MONITORING AND DEBUGGING*** ➜ ***EMAIL ALERT*** ➜ ***AUTHENTICATION SETTINGS***, siehe folgenden Screenshot) konfiguriert werden:



Das Menü bietet folgende Optionen an:

Feld	Wert
Server needs Authentication	Hier können Sie die gewünschte SMTP-Authentifizierung auswählen. Zur Auswahl stehen: ■ *none* (Standardwert)) ■ *Enhanced SMTP* ■ *SMTP after POP.*
Username	Bei *Enhanced SMTP*-Authentifizierung: dies ist der Benutzername, den Sie benutzen, um sich direkt beim SMTP-Server einzuloggen. Bei *SMTP after POP*: dies ist der Benutzername, den Sie benutzen, um sich beim POP3-Server einzuloggen.
Password	Bei *Enhanced SMTP*-Authentifizierung: dies ist das Passwort, welches Sie benutzen, um sich direkt beim SMTP-Server einzuloggen. Bei *SMTP after POP:* dies ist das Passwort, welches Sie benutzen, um sich beim POP3-Server einzuloggen.

Feld	Wert
POP3 Server	Hier geben Sie den Domainnamen des POP3-Servers ein, der die Authentifizierung zum SMTP-Server weitergibt.
POP3 Timeout	Hier geben Sie eine Zeitsperre (Timeout) ein, nach deren Ablauf die Authentifizierung als ungültig betrachtet und wiederholt wird. Mögliche Werte sind *60* bis *3600* Sekunden, der Standardwert ist *600*.

Tabelle 3-1: ***MONITORING AND DEBUGGING → EMAIL ALERT → AUTHENTICATION SETTINGS***

3.6 LOCAL-Schnittstelle für OSPF und Routing freigegeben

Routen, die an die LOCAL-Schnittstelle angebunden waren, wurden weder beim Routing berücksichtigt, noch wurden sie durch OSPF verteilt. Dies wurde geändert, und die LOCAL-Schnittstelle steht damit sowohl für die Routen-Definition als auch für OSPF zur Verfügung.

3.7 SDSL-Firmware als eigenständige Datei

Bisher war die SDSL-Firmware für den Anschluss eines **X2400**-Gateway an ein SDSL-Netzwerk Teil der Systemsoftware aller Gateways der **X2000**-Familie. Dies wurde geändert und analog der ADSL-Firmware steht die SDSL-Firmware jetzt als eigenständige Datei zur Verfügung, die unabhängig von der Systemsoftware benutzt werden kann.

Durch das Herausnehmen der SDSL-Firmware aus der Systemsoftware ist es jetzt möglich, diese unabhängig von der Systemsoftware upzudaten und Risiken zu vermeiden, wie beispielsweise inkompatible Konfigurationen, die bei einem Update der Systemsoftware auftreten könnten. Darüber hinaus spart diese Änderung wertvollen Speicherplatz im Flash-ROM der Gateways der **X2300**-

Familie, da dort die SDSL-Firmware nicht mehr benötigt wird. Mit der wachsenden Funktionsvielfalt, die durch unsere Software unterstützt wird, wird damit die Möglichkeit späterer Upgrades für Gateways der **X2300**-Familie offengehalten.

Beachten Sie bitte, dass Ihr **X2400-**Gateway nach einem Update auf **Systemsoftware 7.1.12** nicht mehr über die SDSL-Firmware verfügt, wenn Sie diese nicht extra installiert haben. Ohne diese Firmware sind keine SDSL-Verbindungen möglich. Die Installation der notwendigen SDSL-Firmware wird in einer Anleitung beschrieben, die Sie in der gleichen ZIP-Datei wie die **Systemsoftware 7.1.12** finden, und die auch von der gleichen Adresse heruntergeladen werden kann, wie die **Systemsoftware 7.1.12**.

3.8 Konfigurierbare Zeitsperre für HTML-Wizard-Sitzungen

Bisher wurde eine HTML-Wizard-Sitzung nach einer vergleichsweise kurzen Zeit der Inaktivität abgebrochen. Mit der **Systemsoftware 7.1.12** wird eine konfigurierbare Inaktivitätszeit eingeführt.

Nach Aufruf des HTML-Wizard über die URL http://<gateway IP address>/wizard?inactivity=<timeout in seconds> können Sie jetzt die Inaktivitäts-Zeitsperre nach Ihren Bedürfnissen konfigurieren.

3.9 HTML-Wizard NAT-Einstellungen

Bisher erzeugte der HTML-Wizard einen Internet-WAN-Partner, bei dem die Silent-Deny-Option für die Netzwerk-Adress-Übersetzung (Network Address Translation, NAT) deaktiviert war. Dies wurde geändert.

Der HTML-Wizard erzeugt jetzt einen Internet-WAN-Partner, bei dem die Silent-Deny-Option aktiviert ist, da dies einen zusätzlichen Schutz gegen Angriffe aus dem Internet bietet.

3.10 SSHD-Überwachung hinzugefügt

Das SSHD-Überwachungsmenü fehlte bisher im Menü ***MONITORING AND DEBUGGING***. Es wurde hinzugefügt, um den Zugriff auf die Überwachungsoptionen zu vereinheitlichen.

3.11 Standardeinstellung für Klassifizierung und Signalisierung

Der in ***QOS ➜ IP CLASSIFICATION AND SIGNALLING ➜ ADD*** vorgeschlagene Standardwert wurde von *classify & set TOS M* auf *classify (keep TOS) M* geändert, da dies die am häufigsten benutzte Einstellung ist.

3.12 Latenzzeit für fehlgeschlagene PPP-Netzauswahl verkürzt

Vor der **Systemsoftware 7.1.12** wurde eine PPP-Schnittstelle nicht sofort nach ***BIBOPPPMAXRETRIES*** +1 aufeinanderfolgenden fehlgeschlagenen Netzauswahlversuchen in den "Blockiert"-Status versetzt. Darüber hinaus gab es eine kurze Verzögerung, die vom Wiederanwahltimer verursachte wurde, der nach jedem Versuch neu gestartet wurde.

Dieses Verhalten wurde geändert, um die Latenzzeit bis zum Blockieren einer Schnittstelle zu minimieren. Dies verbessert das Reaktionsverhalten auf Bedingungen, die eine Umleitung des Datenverkehrs über eine Backup-Schnittstelle erfordern.

3.13 DOVB 64 kbps wird unterstützt

DOVB 64 kbps kann jetzt als ***LAYER 1 PROTOCOL*** ausgewählt werden, wenn ein WAN-Partner konfiguriert wird.

3 Änderungen

4 Gelöste Probleme

Folgende Probleme, die bei früheren Versionen unserer Systemsoftware auftreten konnten, wurden mit der Systemsoftware 7.1.12 gelöst:

■ “ARP - Falsche ARP-Meldung” auf Seite 70

4.1 HTML-Wizard - Verschiedene Verbesserungen

4.1.1 Missverständliche Fehlermeldung

ID 3360

Bei der Konfiguration des Internetzugangs mit dem Internetprovider "T-Online" (dies trifft nur für Deutschland zu) werden Sie nach Ihrer "Anschlusskennung" gefragt. Falls Sie Ihren Eintrag nicht korrekt bestätigt haben, wird eine Fehlermeldung angezeigt, die Ihnen meldet, dass Sie Ihr "Passwort" nicht korrekt bestätigt haben, obwohl es sich bei der "Anschlusskennung" nicht um ein Passwort handelt.

Dieses Problem wurde gelöst.

4.1.2 CLID-Konfiguration

(Keine ID)

Wenn in einer LAN-LAN-Verbindung CLID (Calling Line Identification, Identifizierung des Anrufers) aktiviert wurde, blieb das Feld für die Angabe der MSN des WAN-Partners zunächst leer. Die Konfiguration konnte trotzdem abgespeichert werden, was zu einer nicht funktionierenden CLID-Konfiguration führte.

Dieses Verhalten wurde dahingehend geändert, dass der HTML-Wizard jetzt automatisch die zuvor konfigurierte Rufnummer des WAN-Partners einträgt, wobei führende Nullen weggelassen werden. Der Benutzer kann diese Einstellung ändern, aber es ist nicht mehr möglich, die Konfiguration ohne CLID-Rufnummer abzuspeichern.

4.1.3 Nutzlose Option entfernt

Bei der Konfiguration eines DSL-WAN-Partners mit T-Online-Voreinstellung konnten die Benutzer zwischen einer PPPoE- und einer PPTP-Verbindung wählen. Diese Auswahl ist unnötig, da T-Online gegenwärtig keine DSL-über-PPTP-Verbindungen unterstützt.

Dieses Problem wurde gelöst.

4.2 IPSec - Verschiedene Verbesserungen

4.2.1 QoS-Klassifizierung schlägt fehl

ID 3401

Die Klassifizierung "High Priority" einer QoS-Konfiguration schlug fehl, falls die Hardwarebeschleunigung aktiviert war.

Dieses Problem wurde gelöst.

4.2.2 Tote IPSec-Peers

ID 3469

Falls für einen Interface Peer weder eine IP-Adresse noch IPSec-Rückruf (Callback) konfiguriert wurden, wurde aktuell kein Tunnel aufgebaut. Der Wert des ***IPSECPEEROPERSTATUS*** änderte sich nie von *dormant* auf *up*.

Dieses Problem wurde gelöst.

4.2.3 IPSec-Rückruf kann nicht deaktiviert werden

ID 3528

Falls für einen Peer der ISDN-Rückruf konfiguriert wurde, war es unmöglich, diesen mit Hilfe des Setup Tools wieder zu deaktivieren. Darüber hinaus setzte

der IPSec-Wizard des Setup Tools die Rückrufeinstellungen eines Peers auf *passive,* wenn im dazugehörigen Untermenü *both* gewählt wurde.

Dieses Problem wurde gelöst.

4.2.4 Hardwareverschlüsselung zu langsam

(Keine ID)

Die Gesamtperformance der hardwareunterstützten Verschlüsselung bei **VPN Access100** wurde optimiert.

4.2.5 IPSec-Debugausgabe führt zu einem Gatewayabsturz

(Keine ID)

Wenn die IPSec-Debugausgabe aktiviert wurde oder der IPSec-Cache oder Verkehrslisteneinträge ausgelesen wurden, hat das Gateway neu gebootet.

Dieses Problem wurde gelöst.

4.3 BRRP - Verschiedene Verbesserungen

(Keine ID)

Eine Feinabstimmung der BRRP-Implementierung hat zu einer wesentlichen Verbesserung der Performance und zu einer vereinfachten Benutzung geführt:

- Die Konfiguration von Funktionen für den synchronen Betrieb mehrerer virtueller Router wurde vereinfacht.
- Interne Statusunterschiede zwischen den Routern, die durch Funktionsdefinitionen verknüpft sind, werden vermieden.
- BRRP verfügt jetzt über einen eigenen syslog-Bereich ("BRRP").

4.4 VLAN - Verschiedene Verbesserungen

4.4.1 Setup Tool - Das Löschen einer Schnittstelle führt nicht zur Löschung in der Routing-Tabelle

ID 2720

Bei der Einrichtung einer virtuellen Schnittstelle mit dem Setup Tool wurde auch ein Netzwerkroute in der ***IPROUTETABLE*** erstellt. Beim Löschen einer virtuellen Schnittstelle (wieder mit dem Setup Tool) wurde auch der Eintrag in der ***IFTABLE*** wieder gelöscht, der dazugehörige Routingeintrag wurde jedoch nicht entfernt.

Dieses Problem wurde gelöst.

4.4.2 Setup Tool - Löschung der IP-Adressen von virtuellen Schnittstellen

ID 2908 und 3397

Bei der Bestätigung der Konfiguration einer Ethernet-Schnittstelle mit ***SAVE*** wurden die IP-Adressen aller virtuellen Schnittstellen gelöscht, die für diese Ethernet-Schnittstelle konfiguriert waren.

Dieses Problem wurde gelöst.

4.4.3 Setup Tool - VLAN-Konfiguration für physikalische Schnittstelle kann nicht gespeichert werden

ID 2909

Das Konfigurationsfenster für eine physikalische Ethernet-Schnittstelle bot die Optionen *VLAN* für das Feld IP-Konfiguration und dementsprechend die Spezifikation einer VLAN ID an. Wenn eine Ethernet-Schnittstelle auf diese Weise

konfiguriert wurde, gingen die Einstellungen nach Bestätigung der Konfiguration mit ***SAVE*** wieder verloren.

Wenn die gleichen Konfigurationsparameter auf der SNMP-Shell an die MIB weitergeleitet wurden, führte dies zu einer Panic des Routers und einem erneuten Booten.

Dieses Problem wurde gelöst.

4.4.4 Setup Tool - MAC-Adresse nicht gespeichert

ID 2910

Falls Sie während der Ethernet-Konfiguration eine MAC-Adresse eingegeben hatten, schien es, als ob die MAC-Adresse nach der Bestätigung mit ***SAVE*** abgespeichert würde (nach erneutem Aufruf des entsprechenden Menüs wurde die MAC-Adresse immer noch angezeigt). Sie wurde jedoch nie in der MIB gespeichert, so dass nach dem Verlassen des Setup Tools und erneutem Aufruf des entsprechenden Menüs die MAC-Adresse nicht mehr vorhanden war und in der ***IFTABLE*** keine neu konfigurierte MAC-Adresse enthalten war.

Dieses Problem wurde gelöst.

4.4.5 Setup Tool - Panic nach VLAN-Konfiguration

ID 3392

Nach einer VLAN-Konfiguration hat das Gateway gelegentlich eine Panic gezeigt und neu gebootet.

Dieses Problem wurde gelöst.

4.5 DHCP - Verschiedene Verbesserungen

Unsere DHCP-Implementierung wurde sorgfältig überarbeitet, wodurch die Leistungsfähigkeit und die Fehlervermeidung verbessert wurden. Darüber hinaus wurde folgendes Problem gelöst:

4.5.1 Stack Trace nach fehlgeschlagener IP-Adressenprüfung

ID 2586 und 2824

Bevor der DHCP-Server einem Client eine temporäre IP-Adresse zuweist, prüft er mit Hilfe eines Ping, ob diese IP-Adresse nicht schon von einem anderen Host benutzt wird. Falls es auf den Ping eine Antwort gibt, d. h. falls die Prüfung negativ ausfällt, wird ein Stack Trace erstellt. Die gleiche Situation kann durch Erzwingung einer erneuten DHCP-Zuweisung von Seiten des Hosts verursacht werden.

4.6 QoS - Stack Trace mit WFQ

(Keine ID)

Wenn in einer QoS-Konfiguration WFQ (Weighted Fair Queuing) benutzt wird, konnte dies sporadisch zu Stack Traces führen.

Dieses Problem wurde gelöst.

4.7 Setup Tool - PPP-Blockierungszeit nimmt unerwünschte Werte an

ID 2987

Die SNMP-Shell sowie das Setup Tool ermöglichten es, der Variablen ***BIBOPPPBLOCKTIME*** sehr niedrige und sogar negative Werte zuzuweisen. Negative Werte haben (abhängig vom eingegebenen Wert) eine sehr lange Blockierungszeit zur Folge, und sehr kleine Werte (z.B. < 5 Sek.) können zu Problemen führen, falls ein Rückruf aktiviert wurde.

Dies wurde geändert: problematische Werte können nicht mehr eingegeben werden.

4.8 Setup Tool - Organisation des QoS-Menüs

ID 3001

Der Aufbau des QoS-Menüs ***IP CLASSIFICATION AND SIGNALLING*** wurde geändert, um einen besseren Überblick über die bereits konfigurierten Filter zu bieten. Früher waren einige der Filterparameter unter Umständen nicht sichtbar.

4.9 Setup Tool - Falsch angeordnete Beschreibung im Lastausgleichs-Menü

ID 3176

In der Listendarstellung des Menüs ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➜ ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** waren Einträge in der Beschreibungsspalte unbeabsichtigt eingerückt.

Dieses Problem wurde gelöst.

4.10 LCP - Zweiphasige Verhandlung führt zu falscher Verkapselung

ID 3303

Die Kanalbündelung konnte fehlschlagen (keine Daten wurden übertragen), wenn die ferne Seite eine zweiphasige Authentifizierungsprozedur genutzt hat, bei der die fernen Endpunkte verschiedene Optionen für die Adressfeldkomprimierung während der LCP-Protokollverhandlung (Link Control Protocol) anboten.

Dieses Problem wurde gelöst.

4.11 Setup Tool - Druckfehler korrigiert

ID 3405

Im Menü ***WAN PARTNER ADVANCED SETTINGS*** gab es bei den verfügbaren Optionen für den Parameter ***CALLBACK*** einen Druckfehler.

Dieses Problem wurde gelöst.

4.12 QoS - Probleme mit X8E-SYNC

ID 3412

Bei der Verarbeitung großer Datenmengen arbeitete eine QoS-Konfiguration für Prioritätswarteschlangen mit Bandbreitenbeschränkung nicht richtig.

Dieses Problem wurde gelöst.

4.13 SNMP-Community gelöscht

ID 3474

Jeder Anmeldeversuch für einen in der ***BIBOADMLOGINTABLE*** definierten Account führte dazu, dass die ***BIBOADMREADCOMMUNITY*** in eine leere Zeichenkette verwandelt wurde, d. h. die Community wurde gelöscht.

Dieses Problem wurde gelöst.

4.14 Lastausgleich - Falsche Sitzungszählung an den IPSec-Schnittstellen

ID 3487

Die Nutzung der IP-Lastausgleichsfunktion für IPSec-Schnittstellen konnte zu einer falschen Sitzungszählung führen (die in der ***IPLOADBIFTABLE***: ***ACTASSIGNEDSESSIONS*** angegeben ist).

Dieses Problem wurde gelöst.

4.15 RIP - TOS-Kennzeichnung nicht möglich

ID 3491

Bei lokal erzeugten RIP-Paketen war keine TOS-Signalisierung möglich.

Dieses Problem wurde gelöst.

4.16 PPP - Überflüssige Einträge in der pppSessionTable

ID 3515

Nach der Trennung eines PPP-Rufes mit Inband-Authentifizierung wurde der dazugehörige Eintrag in der ***PPPSESSIONTABLE*** nicht gelöscht. Dies konnte zu einem Speicherleck führen.

Dieses Problem wurde gelöst.

4.17 X8500 - PCI-Fehler

ID 3562

Beim Booten eines X8A-SYS-VPN wurde eine PCI-Fehlermeldung angezeigt, falls ein X8E-2SYNC-Modul vorhanden war. Mit einer X8A-SYS-Platine bootete der Router während des Bootprozesses neu.

Dieses Problem wurde gelöst.

4.18 PPP - Verbindungszurückweisung

ID 3582

Durch einen unkomprimierten Adressprotokoll-Header in der CHAP- oder PAP-Authentifizierungsantwort, die vom Bintec-Gateway ausgesandt wurde, wurde eine LCP-Protokollzurückweisung verursacht. Dies war nicht RFC-kompatibel.

Dieses Problem wurde gelöst.

4.19 IP-Filter - Portspezifikation ungenau

ID 3601

In vielen Fällen, bei denen IP-Filter angewandt wurden, konnten Ports für andere Protokolle als TCP oder UDP konfiguriert werden, obwohl die fraglichen Ports nur für diese Protokolle vorgesehen waren. Es gab keinen Hinweis darauf, dass Filtereinträge mit den Protokollen *any* und *any port* nur zu TCP- oder UDP-Paketen passen.

Dieses Problem wurde gelöst: Die portbezogenen Felder werden jetzt bei allen Protokollen ausgeblendet, die keine Portspezifikation unterstützen.

4.20 ARP - Falsche ARP-Meldung

ID 3671

Wenn ein Gateway über mehrere Schnittstellen verfügte (z. B. eine physikalische und eine virtuelle), konnte es falsche ARP-Meldungen erzeugen, wobei die IP-Adresse der einen Schnittstelle und die MAC-Adresse der anderen Schnittstelle benutzt wurden.

Dieses Problem wurde gelöst.