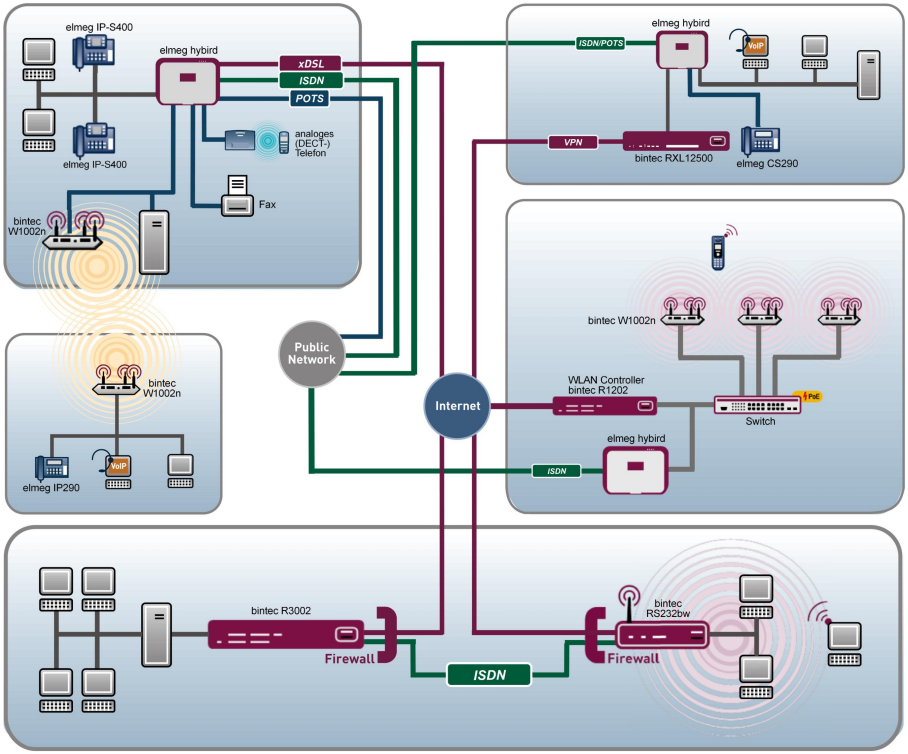

Benutzerhandbuch
Release Notes

9.1.1

Rechtlicher Hinweis

Ziel und Zweck
Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Teldat-Geräten. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind zu finden unter *www.teldat.de* .

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

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Release Notes für Teldat-Gateways finden Sie unter *www.teldat.de* .

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

Marken
Teldat und das Teldat-Logo, bintec und das bintec-Logo, artem und das artem-Logo, elmeg und das elmeg-Logo sind eingetragene Warenzeichen der Teldat GmbH.

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

Copyright

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter *www.teldat.de* .

Wie Sie Teldat GmbH erreichen
Teldat GmbH, Südwestpark 94, D-90449 Nürnberg, Deutschland, Telefon: +49 911 9673 0, Fax: +49 911 688 07 25
Teldat France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradignan, Frankreich, Telefon: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05
Internet: *www.teldat.de*

Inhaltsverzeichnis

Kapitel 1 Wichtige Informationen

1.1 Vorbereitung und Update mit dem GUI

Das Update der Systemsoftware mit dem Graphical User Interface erfolgt mit einer BLUP-Datei (Bintec Large Update), um alle notwendigen Module intelligent zu aktualisieren. Dabei werden alle diejenigen Elemente aktualisiert, die im BLUP neuer sind als auf Ihrem Gateway.

Hinweis

Die Folge eines unterbrochenen Update-Vorgangs könnte sein, dass Ihr Gateway nicht mehr bootet. Schalten Sie Ihr Gateway deshalb nicht aus, während das Update durchgeführt wird.

Gehen Sie folgendermaßen vor, um mit dem Graphical User Interface ein Update auf **Systemsoftware 9.1.1** vorzubereiten und durchzuführen:

(1) Für das Update benötigen Sie die Datei `XXXXX_bl9101.xxx`, wobei `XXXXX` für Ihr Gerät steht. Stellen Sie sicher, dass die Datei, welche Sie für das Update benötigen, auf Ihrem PC verfügbar ist. Wenn die Datei nicht auf Ihrem PC verfügbar ist, geben Sie *www.teldat.de* in Ihren Browser ein. Die Teldat-Homepage öffnet sich. Im Download-Bereich Ihres Gateways finden Sie die benötigte Datei. Speichern Sie sie auf Ihrem PC.

(2) Sichern Sie die aktuelle Boot-Konfiguration vor dem Update. Exportieren Sie die aktuelle Boot-Konfiguration über das Menü **Wartung**->**Software &Konfiguration** des Graphical User Interface. Wählen Sie dazu: **Aktion** = *Konfiguration exportieren*, **Aktueller Dateiname im Flash** = *boot*, **Zertifikate und Schlüssel einschließen** = *aktiviert*, **Verschlüsselung der Konfiguration** = *deaktiviert* Bestätigen Sie mit **Los**. Das Fenster **Öffnen von <Name des Gateways>.cf** öffnet sich. Belassen Sie die Auswahl bei *Datei speichern* und klicken Sie auf **OK**, um die Konfiguration auf Ihrem PC zu speichern. Die Datei `<Name des Gateways.cf>` wird gespeichert, das Fenster **Downloads** zeigt die gespeicherte Datei.

(3) Führen Sie das Update auf **Systemsoftware 9.1.1** über das Menü **Wartung**->**Software &Konfiguration** durch. Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = *XXXXX_bl9101.xxx*. Bestätigen Sie mit **Los**. Die Meldung „System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet.“ bzw. „System Maintenance. Please stand by. Operation in progress.“ zeigt, dass die gewählte Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung „System - Maintenance. Sucess. Operation completed success-

fully“. Klicken Sie auf **Reboot**. Sie sehen,0, die Meldung „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds“. Das Gerät startet mit der neuen Systemsoftware, das Browser-Fenster öffnet sich.

1.2 Downgrade mit dem GUI

Wenn Sie ein Downgrade durchführen wollen, gehen Sie folgendermaßen vor:

(1) Ersetzen Sie die aktuelle Boot-Konfiguration durch die zuvor gesicherte. Importieren Sie die gesicherte Boot-Konfiguration über das Menü **Wartung**->**Software &Konfiguration**. Wählen Sie dazu: **Aktion** = *Konfiguration importieren*, **Verschlüsselung der Konfiguration** = *deaktiviert*, **Dateiname** = *<Name des Geräts>.cf*. Bestätigen Sie mit **Los**. Die Meldung „System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet.“ bzw. „System Maintenance. Please stand by. Operation in progress.“ zeigt, dass die gewählte Konfiguration in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung „System - Maintenance. Sucess. Operation completed successfully.“ Klicken Sie auf **Reboot**. Sie sehen die Meldung „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ Das Gerät startet, das Browser-Fenster öffnet sich. Melden Sie sich an Ihrem Gerät an.

(2) Führen Sie das Downgrade auf die gewünschte Softwareversion über das Menü **Wartung**->**Software &Konfiguration** durch.
Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = *R3000_bl9101.r3d* (Beispiel). Bestätigen Sie mit **Los**. Die Meldung „System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet.“ bzw. „System Maintenance. Please stand by. Operation in progress.“ zeigt, dass die gewählte Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung „System - Maintenance. Sucess. Operation completed successfully.“ Klicken Sie auf **Reboot**. Sie sehen die Meldung „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ Das Gerät startet mit der neuen Systemsoftware, das Browser-Fenster öffnet sich.

Sie können sich an Ihrem Gerät anmelden und es konfigurieren.

Kapitel 2 Neue Funktionen

Systemsoftware 9.1.1 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber der letzten Version der Systemsoftware erheblich erweitern.

Hinweis

Bitte beachten Sie, dass nicht alle hier aufgeführten neuen Funktionen für alle Geräte zur Verfügung stehen. Informieren Sie sich ggf. im aktuellen Datenblatt Ihres Gerätes oder im entsprechenden Handbuch.

2.1 Assistent Telefonanschluss

Zur grundlegenden Nutzung eines Telefonanschlusses wurde ein neuer Assistent in die Benutzeroberfläche eingeführt. Mit dessen Hilfe können externe analoge, ISDN- und VoIP-Anschlüsse konfiguriert und angelegt werden.

Sie finden den PBX-Assistenten unter **Assistenten** -> **PBX** -> **Anschlüsse**. In einer Übersicht werden alle bereits existierenden Anschlüsse aufgeführt. Löschen Sie Einträge, indem Sie auf das -Symbol klicken. Wählen Sie das Symbol , um die bestehenden Anschlüsse zu bearbeiten.

Ein weiterer Anschluss kann mithilfe der Schaltfläche **Neu** angelegt werden. Anhand eines Auswahlfeldes legen Sie im nächsten Konfigurationsschritt den **Verbindungstyp** des Anschlusses fest. Dabei stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

- *ISDN*
- *Anlagenanschluss*
- *SIP-Provider*
- *SIP-Provider (Durchwahl)*
- *FXO*

Wenn Sie als **Verbindungstyp** *ISDN* auswählen und anschließend mit **Weiter** bestätigen, gelangen Sie in die ISDN-Einstellungen. Hier können Sie dem Anschluss einen **Namen** geben, die entsprechenden externen **Ports** und **Einzelrufnummer (MSN)** wählen und eine **Berechtigungsklasse** festlegen.

Bei der Option *ISDN (P-P)* wird anstatt einer Einzelrufnummer eine **Anlagenanschluss-Rufnummer** benötigt. In den **Erweiterten Einstellungen** können Sie zusätzlich eine **Durchwahlausnahme (P-P)** konfigurieren.

Bei der Verwendung eines *SIP-Providers* müssen Sie neben dem **Verbindungsnamen**, der **Einzelrufnummer** und der **Berechtigungsklasse**, die **Authentifizierungs-ID**, das **Passwort**, den **Benutzernamen** und den **Registrar** eintragen. Anschließend können Sie in den **Erweiterten Einstellungen** die Nummer des **Ports** eingeben, der für die Verbindung zum Server benutzt werden soll. Standardmäßig ist der Wert *5060* vorgegeben. Wählen Sie das **Transportprotokoll** für die Verbindung aus. Sie können **IP-Adresse** und **Port** eines STUN-Servers angeben und eine **Nationale** oder **Internationale Rufnummer erzeugen** lassen.

Für einen *SIP-Provider (Duchwahl)* muss zusätzlich eine **Basisrufnummer** angegeben werden.

Verwenden Sie einen Standard-Telefonanschluss (*FXO*), müssen Sie neben **Name**, **Einzelrufnummer** und **Berechtigungsklasse** den entsprechenden **Externen Port** auswählen.

2.2 IKEv2 – Unterstützung für Zertifikate

Die IKEv2-Implementierung der Teldat GmbH unterstützt nun die zertifikatsbasierte Authentifizierung.

Um diese nutzen zu können, wechseln Sie zuerst ins GUI-Menü **VPN** -> **IPSec** -> **IPSec Peers** -> **Neu**.

Wählen Sie unter **IKE (Internet Key Exchange)** *IKEv2*. Daraufhin können Sie neben *Preshared Keys* auch die **Authentifizierungsmethode** *RSA-Signatur* wählen. Falls das RSA-Verfahren verwendet wird, kann unter **Lokales Zertifikat** ein eigenes Zertifikat für die Authentifizierung bestimmt werden. Das Feld zeigt die Indexnummer des Zertifikats und dessen Namen.

Unter **Lokaler ID-Typ** wählen Sie den Typ der lokalen ID aus. Folgende Werte stehen zur Auswahl:

- *Fully Qualified Domain Name (FQDN)*
- *E-Mail-Adresse*
- *IPV4-Adresse*
- *ASN.1-DN (Distinguished Name)*
- *Schlüssel-ID*

Im Feld **Lokale ID** geben Sie die ID Ihres Geräts ein. Für die Authentifizierungsmethode RSA-Signatur wird die Option **Subjektname aus Zertifikat verwenden** angezeigt. Wenn Sie diese aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet.

2.3 IPSec - Direkte Festlegung der Selektoren für Phase 2

Bei einem über die Benutzeroberfläche erstellten IPSec-Tunnel erfolgt die Aushandlung der Phase-2-SAs über konfigurierte oder dynamisch erlernte Routen. In einigen Fällen führte dies jedoch zu Problemen aufgrund konkurrierender Routen oder mangelnder Granularität von Standard-Routen, da die Filterung des Netzwerkverkehrs bis auf Protokoll- bzw. Portebene mit Standard-Routen nicht möglich ist.

Deshalb können die Selektoren nun auch manuell festgelegt werden, um die SAs abzuleiten. Wechseln Sie dazu in das Menü **VPN** -> **IPSec** -> **IPSec-Peers** -> **Neu**. Dort müssen Sie zunächst alle nötigen VPN-Parameter konfigurieren. Verwenden Sie dabei keine IPSec-Routen. Erzeugen Sie stattdessen eine oder mehrere Standardrouten und aktivieren Sie das Feld **Standardroute**. Unter **Zusätzlicher Filter des Datenverkehrs** können Sie mithilfe von **Hinzufügen** einen neuen Filter anlegen.

Im sich öffnenden Fenster sollten Sie zuerst eine **Beschreibung** des Filters angeben. Anschließend legen Sie dann das verwendete **Protokoll** fest. Schließlich müssen Sie noch bei **Quell-IP-Adresse/Netzmaske** und **Ziel-IP-Adresse/Netzmaske** das Netzwerk mit der dazugehörigen Netzmaske eintragen. Speichern Sie Ihre Einstellungen mit **Übernehmen**.

Das erweiterte Verfahren bietet weiterhin den Einsatz von NAT bzw. PAT innerhalb eines Tunnels, die Verwendung von Routing-Protokollen, wie RIP oder OSPF, sowie die Realisierung von VPN-Backup-Szenarien.

Dieses Leistungsmerkmal behebt auch ein Problem mit VPN-Business-Zugängen. Zu diesem Zweck muss die **Quell-IP-Adresse/Netzmaske** analog zu Ihrem LAN-Anschluss konfiguriert werden. Bei **Protokoll** und **Ziel-IP-Adresse/Netzmaske** können Sie die Einstellung auf `Alle` belassen.

2.4 Rogue-Access-Point-Management

2.4.1 Rogue-Access-Point-Übersicht

Rogue Access Points (Rogue APs) verwenden die SSID (Service Set IDentifier), also den Netzwerknamen, des eigenen Netzes. Obwohl sie nicht zum Netzwerk gehören, können sich Clients versehentlich an diesen fremden APs anmelden. Angreifer können diese Eigenschaft ausnutzen, um private Daten des Benutzers abzugreifen.

Im GUI können Sie inzwischen in zwei Menüs die Suche nach benachbarten APs anstoßen. Neben dem GUI-Menü **Wireless LAN Controller** -> **Monitoring** -> **Benachbarte APs** ist dies mittlerweile auch im Menü **Wireless LAN Controller** -> **Monitoring** ->**Rogue**

APs möglich.

Nach einem erfolgreichen Suchlauf werden Ihnen alle verfügbaren APs unter **Wireless LAN Controller** -> **Monitoring** -> **Benachbarte APs** angezeigt. Rogue APs, die eine vom WLAN-Controller verwaltete SSID verwenden, aber nicht von diesem administriert werden, sind hier rot hinterlegt dargestellt.

Die Rogue APs werden weiterhin im neuen Untermenü **Wireless LAN Controller** -> **Monitoring** ->**Rogue APs** separat angezeigt. Auch hier erscheinen zunächst alle Einträge rot hinterlegt. Das Untermenü **Rogue AP** besitzt eine Spalte **Akzeptiert**. Durch Aktivierung des entsprechenden Auswahlfeldes durch den Administrator wird der Rogue AP als vertrauenswürdig eingestuft. Alle eventuell definierten Alarmmeldungen werden gelöscht und nicht mehr gesendet. Außerdem werden diese APs in den Menüs **Rogue APs**s und **Benachbarte APs** nicht mehr rot hinterlegt.

2.4.2 Neue Rogue APs melden

Falls bei einer Suche nach benachbarten APs neue Rogue APs gefunden wurden, kann eine Information über E-Mail erfolgen.

Dazu muss bei der Erstellung einer neuen E-Mail-Alarmierung im Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungsempfänger**-> **Neu** unter **Ereignis** *Neuer Rogue AP gefunden* ausgewählt werden.

2.5 Verbesserte Voice-Mail-Administration

2.5.1 Automatisches Löschen von Voice-Mail-Nachrichten

Voice-Mail-Nachrichten werden nach einer festlegbaren Zeit automatisch gelöscht. Diese Zeitdauer wird im Menü **Anwendungen** -> **Voice Mail System** -> **Allgemein** -> **Erweiterte Einstellungen** unter **Lebensdauer** festgesetzt. Mögliche Werte sind 10 bis 60 Tage. Der Standardwert beträgt 60 Tage.

2.5.2 Voice-Mail-Nachrichten im Benutzerzugang löschen

Es ist nunmehr möglich einzelne oder alle Voice-Mail-Nachrichten im Benutzerzugang zu löschen. Nachrichten können weiterhin während des Abhörens über das Systemtelefon durch Betätigen der Taste "1" einzeln gelöscht werden.

Im Menü **Benutzerzugang** -> **Voice Mail System** -> **Nachrichten** finden Sie eine neue Spalte **Alle auswählen** / **Alle deaktivieren**.

Hier aktivierte Rufnummerneinträge können über die Schaltfläche **Auswahl löschen** ge-

löscht werden. Durch die entsprechenden Verweise im Kopf der Spalte können alle Einträge zur Auswahl hinzugefügt oder aus dieser herausgenommen werden.

2.5.3 Voice-Mail-Nachrichten im Benutzerzugang verwalten

Die Verwaltung von Voice-Mail-Nachrichten kann mittlerweile im Benutzerzugang durchgeführt werden. Dazu müssen Sie im GUI-Menü **Anwendungen** -> **Voice Mail System** -> **Voice Mail Boxen** unter **E-Mail-Benachrichtigung** *Benutzerdefiniert* auswählen. Anschließend kann der Benutzer im Menü **Benutzerzugang** -> **Voice Mail System** -> **Einstellungen** ->  die Art der **E-Mail-Benachrichtigung** festsetzen. Sie können für die Optionen *E-Mail* und *E-Mail mit Anhang* das **Verhalten bei E-Mail-Weiterleitung** festlegen. Dadurch bestimmen Sie, ob die Voice-Mail-Nachricht nach einer E-Mail-Benachrichtigung oder Weiterleitung gelöscht (*Nach Weiterleitung Nachricht entfernen*), auf den **Status** "Alt" (*Nach Weiterleitung Nachricht nach 'alt' verschieben*) oder "Neu" (*Nach Weiterleitung Nachricht in 'neu' behalten*) gesetzt werden soll.

2.5.4 Voice-Mail-Nachrichten im Benutzerzugang abspielen oder speichern

Auf der Benutzeroberfläche im Menü **Benutzerzugang** -> **Voice Mail System** -> **Nachrichten** besteht die Möglichkeit, Voice-Mail-Nachrichten abzuspielen oder auf den PC herunterzuladen. Zum Speichern einer Nachricht klicken Sie auf das  -Symbol. Daraufhin öffnet sich der Download-Dialog. Um die Voice-Mail-Nachricht anzuhören, klicken Sie auf das -Symbol.

2.5.5 Anzahl der gespeicherten Voice-Mail-Nachrichten festlegen

Es wurde eine Möglichkeit geschaffen, die maximale Anzahl der Voice-Mail-Nachrichten selbst festzusetzen.

Der bisher fest kodierte Wert von maximal 60 Aufzeichnungen ist für jeden Benutzer des Voice-Mail-Systems in der MIB-Tabelle **vms** -> **vmsAccountTable** ->  -> **vmsAccountMaxMessages** abgelegt und kann bei Bedarf über den SNMP-Browser verändert werden.

2.6 Schaltkontakte

Die **elmeg hybird 130j** sowie die **elmeg hybird 300** / **elmeg hybird 600** verfügen über einen bzw. zwei unabhängige Schaltkontakte, die hardwaretechnisch bereits unterstützt werden.

Ein Schaltkontakt kann als Ein-/Ausschalter oder als Taster verwendet werden, d. h. der Stromkreis wird geschlossen, geöffnet oder für eine vorgegebene Zeitdauer geschlossen. Sie können diese Eigenschaft nutzen, um einen Türöffner zu bedienen oder Ihr Außenlicht ein und wieder aus zu schalten.

Gesteuert werden diese Funktionen über die Eingabe von Kennziffern in intern oder extern angeschossene Telefone. Um den Stromkreis zu schließen, geben Sie für den ersten Schaltkontakt die Sequenz `* 531` ein und für den zweiten `* 532`.

Um den Stromkreis zu öffnen, müssen Sie die Kombination `# 53n` eingeben. Dabei können Sie für `n` die Zahlen 1 oder 2 einsetzen, für den ersten bzw. zweiten Schaltkontakt.

Wollen Sie den Stromkreis für eine bestimmte Zeit schließen, müssen Sie die Ziffernfolge `* 54n` verwenden. `n` steht dabei wieder für den ersten oder zweiten Schaltkontakt. Die Zeitdauer, für die der Stromkreis geschlossen wird, ist werksseitig auf 3 Sekunden eingestellt. Sie können diesen Wert über die Benutzeroberfläche ändern. Wechseln Sie dazu ins GUI-Menü **Physikalische Schnittstellen** -> **Relais** -> **Relaiskonfiguration**. Dort können Sie für die **Kontakte** 1 und 2 eine **Beschreibung** vergeben und unter **Signalisierungszeitraum** die Zeitspanne festlegen. Die Schaltzeit für den Taster kann zwischen einer und 999 Sekunden eingerichtet werden. Der Standardwert beträgt `3` Sekunden.

2.7 NAT Loopback

Mithilfe der NAT-Loopback-Funktion ist die Adresstranslation auch bei Anschlüssen möglich, auf denen NAT nicht aktiviert ist. Dies wird häufig verwendet, um Anfragen aus dem LAN so zu interpretieren, als ob sie aus dem WAN kämen.

Ein konkreter Anwendungsfall wäre der Test von Serverdiensten im eigenen Netzwerk. Der Client, der zum Testen verwendet werden soll, und der Server befinden sich in einem gemeinsamen LAN. Zum Verbindungsaufbau sendet der Client mit seiner LAN-IP-Adresse eine Anfrage an die WAN-IP-Adresse des Routers. Falls die NAT-Loopback-Funktion aktiv ist, leitet dieser das Datenpaket an den Server weiter. Für den Server scheint das Datenpaket aus dem WAN und nicht aus dem LAN zu kommen. Im Fall einer inaktiven NAT-Loopback-Funktion werden die Anfragen nicht an den Server weitergeleitet.

Zur Aktivierung der NAT-Loopback-Funktion wechseln Sie ins GUI-Menü **Netzwerk** -> **NAT** -> **NAT-Schnittstellen** . Auf der Übersichtsseite haben Sie die Möglichkeit in der Spalte **Loopback** durch Aktivierung des entsprechenden Auswahlfelds die Funktion einzuschalten.

2.8 SMS-Benachrichtigungsdienst

Falls Sie im Besitz eines **bintec RS120wu**, **bintec RS230au+** oder **bintec RS230bu+** sind, können Sie sich über Systemmeldungen per SMS informieren lassen. Die SMS-Implementierung funktioniert dabei analog zur Alarmierung über eine E-Mail-Mitteilung.

Sie aktivieren die Funktion im GUI-Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungsempfänger**-> **Neu** unter dem Menüpunkt **Benachrichtigungsdienst**. Hier wählen Sie *SMS* und tragen anschließend unter **Empfänger** die Telefonnummer des Empfängers der SMS-Mitteilung ein.

Anschließend müssen Sie im Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungseinstellungen** das zu verwendende **SMS-Gerät** auswählen. Ferner können Sie hier unter **Maximale SMS pro Tag** die maximale Anzahl der an einem Tag gesendeten SMS festlegen und somit Ihre Kosten regulieren. Die Aktivierung von *Uneingeschränkt* erlaubt eine beliebige SMS-Anzahl.

2.9 IPSec - Unterstützung der ISAKMP-Extended-Authentication-Methode

Bis zur **Systemsoftware 9.1.1** unterstützten die Geräte der Teldat GmbH nur die Simple-Authentication-Methode für XAuth bei der Verwendung von IPSec. Nun ist es möglich eine erweiterte Two-Factor-Authentication-Methode zu verwenden. Diese wird im RFC draft *Extended Authentication within ISAKMP/Oakley (XAUTH)* beschrieben. Dabei wird eine konventionelle Authentifizierung durch eine zweite Identitätsprüfung über einen anderen Übertragungsweg ergänzt. Konkret sendet eine Sicherheitssoftware nach erfolgreicher Authentifizierung über Benutzername und Passwort einen zusätzlichen Zugangsschlüssel per SMS an die registrierte Mobilfunknummer des Nutzers.

Dadurch wird vor allem der Einsatz der Software **SMS Passcode** der *ProSoft Software Vertriebs GmbH* ermöglicht. Das Programm läuft auf einem **Windows 2008 Radius Server** und bietet ein erweitertes Login-Verfahren für zusätzliche Sicherheit von Remote-Anwendungen in Netzwerken oder Webseiten. Die Funktionalität wurde mit dem IPSec-Client NCP getestet.

2.10 LTE-Unterstützung

Systemsoftware 9.1.1 bietet Unterstützung von LTE-USB-Sticks an der USB-Schnittstelle der RS-Serie. Folgende Sticks wurden von Teldat auf Kompatibilität geprüft:

- Telekom Speedstick LTE (Huawei/E398)

- Vodafone SurfStick (Huawei K5005)

Hinweis

Einige Funktionen wie SMS und eingehende Verbindungstypen wie ISDN Login, PPP und IPSec Callback werden bei LTE-Verbindungen aktuell nicht unterstützt.

Die Menüs zur Konfiguration der physikalischen Schnittstelle und der WAN-Verbindungen sind entsprechend angepasst worden. Darüber hinaus unterstützt auch der Assistent zur Konfiguration des Internetzugangs LTE-Verbindungen.

Im Menü **UMTS/LTE** konfigurieren Sie die Anbindung des integrierten UMTS/HSDPA/LTE-Modems (für **bintec RS232j-4G**), UMTS/HSDPA-Modems (für **bintec RS120wu** und **bintec RS230au+**) oder eines optional steckbaren UMTS/LTE-USB-Sticks.

Eine Liste der unterstützten UMTS/LTE-USB-Sticks finden Sie unter *www.teldat.de* im Bereich **Produkte**.

Wählen Sie folgenden Eintrag für das entsprechende UMTS/LTE-Modem:

- `Slot6 Unit 0`: Das integrierte Modem soll konfiguriert werden.
- `Slot6 Unit 1`: Der gesteckte UMTS/LTE-USB-Stick soll konfiguriert werden.

Hinweis

Beachten Sie, dass die verwendete Technologie nicht nur von der Verfügbarkeit und von der Einstellung im Feld **Bevorzugter Netzwerktyp** abhängt sondern auch von der Signalstärke und von der Signalqualität.

Das Menü **Physikalische Schnittstellen**->**UMTS/LTE**->**UMTS/LTE**-> besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
UMTS/LTE-Status	Wählen Sie aus, ob das gewählte UMTS/LTE-Modem aktiviert werden soll oder nicht. Mit `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Modem-Status	Nur für **UMTS/LTE-Status** = `Aktiviert` Zeigt den Status des UMTS/LTE-Modems an.

Feld	Beschreibung
	Mögliche Werte: • *Aktiv* • *Inaktiv* • *Init* • *Gerufen* • *Rufend* • *Verbinden* • *SIM Einlegen erforderlich* • *PIN Eingabe erforderlich* • *Fehler* • *Nicht verbunden*
Mobilfunk-Anbieter	Nur für **UMTS/LTE-Status** = *Aktiviert* Wird nur angezeigt, wenn sich das Modem im Zustand "up" befindet. Zeigt den aktuell verbundenen **Mobilfunk-Anbieter** an.
Aktuelles Netzwerk	Nur für **UMTS/LTE-Status** = *Aktiviert* Zeigt das aktuelle Netzwerk an, z. B. GSM oder UMTS.
Netzwerkqualität	Nur für **UMTS/LTE-Status** = *Aktiviert* Zeigt die aktuelle Qualität der UMTS/LTE-Verbindung an. Der Wert kann nicht verändert werden.
Bevorzugter Netzwerktyp	Nur für **UMTS/LTE-Status** = *Aktiviert* Wählen Sie aus, welcher Netzwerktyp bevorzugt verwendet werden soll. Mögliche Werte: • *Automatisch* (Standardwert): Für die Verbindung wird automatisch GPRS, UMTS oder LTE gewählt, je nachdem welcher Netzwerktyp örtlich zur Verfügung steht. • *Nur GPRS*: Nur GPRS wird verwendet, sollte GPRS nicht verfügbar sein, kommt keine Verbindung zustande.

Feld	Beschreibung
	• *Nur UMTS*: Nur UMTS wird verwendet, sollte UMTS nicht verfügbar sein, kommt keine Verbindung zustande. • *Bevorzugt GPRS*: Es wird bevorzugt GPRS verwendet, sollte GPRS nicht verfügbar sein, wird UMTS verwendet. • *Bevorzugt UMTS*: Es wird bevorzugt UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet. • *Nur LTE*: Nur LTE wird verwendet, sollte LTE nicht verfügbar sein, kommt keine Verbindung zustande • *LTE preferred (Priorität 4G/3G/2G)*: Es wird bevorzugt LTE verwendet, sollte LTE nicht verfügbar sein, wird UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet • *LTE/UMTS (Priorität 4G/3G)*: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird UMTS verwendet. • *LTE/GPRS (Priorität 4G/2G)*: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet. • *LTE/GPRS/UMTS (Priorität 4G/2G/3G)*: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird UMTS verwendet. • *UMTS/LTE (Priorität 3G/4G)*: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird LTE verwendet. • *UMTS/GPRS (Priorität 3G/2G)*: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird GPRS verwendet. • *UMTS/LTE/GPRS (Priorität 3G/4G/2G)*: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird LTE verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet.. • *GPRS/LTE (Priorität 2G/4G)*: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird LTE verwendet. • *GPRS/UMTS (Priorität 2G/3G)*: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von

Feld	Beschreibung
	GPRS wird UMTS verwendet. • *GPRS/LTE/UMTS (Priorität 2G/4G/3G)*: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird LTE verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird UMTS verwendet.  **Hinweis** Ein eingehender Datenruf (PPP-Einwahl oder ISDN-Login über V.110) kann in der Regel nur über GSM aufgebaut werden. Für UMTS/LTE ist ein Aufbau nur möglich, wenn der Provider diese Funktionalität auf Antrag freigeschaltet hat. Wenn sich ein Modem im Zustand "up" befindet und **Bevorzugter Netzwerktyp** nicht *Nur UMTS* ist, registriert sich das Modem normalerweise im GSM-Netz, damit eingehende Daten-Rufe signalisiert werden können. Wird danach eine Verbindung zum Internet hergestellt, wird in das UMTS-Netz umgeschaltet, sofern UMTS aktuell verfügbar ist.
Eingehender Diensttyp	Nur für **UMTS/LTE-Status** = *Aktiviert* Wählen Sie aus, welchem Subsystem des Gateways ein über das Modem eingehender Ruf zugewiesen werden soll. Mögliche Werte: • *Deaktiviert*: Es erfolgt keine Rufannahme (Standardwert für LTE-Verbindungen). • *ISDN-Login* : Der Ruf wird dem ISDN-Login-Subsystem zugewiesen (Standardwert für UMTS-Verbindungen). • *PPP-Einwahl*: Der Ruf wird dem PPP-Subsystem zugewiesen. • *IPSec*: Der Ruf erfolgt über IPSec. Beachten Sie für die Einstellung **Eingehender Diensttyp** *IPSec* Folgendes: IPSec-Callback wird dazu verwendet, einen IPSec-Peer zu veranlassen, eine Internetverbindung aufzubauen, um so einen IP-

Feld	Beschreibung
	Sec-Tunnel über das Internet zu ermöglichen. Mit Hilfe eines direkten Anrufs über das UMTS/LTE-Mobilfunknetz kann dem Peer signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den Anruf über Mobilfunk veranlasst, eine Verbindung aufzubauen. Im Menü **VPN**->**IPSec**->**IPSec-Peers**->  ->**Erweiterte Einstellungen** können Sie unter **Eigene IP-Adresse per ISDN/GSM übertragen** zudem auswählen, ob die IP-Adresse zum IPSec-Tunnelaufbau in dem Callback-UMTS/LTE-Ruf mitgesendet werden soll. Dieses verkürzt und erleichtert unter Umständen den Tunnelaufbau.
PUK	Wird nur angezeigt, wenn das Gerät dreimal vergeblich versucht hat, eine Verbindung aufzubauen, z. B. wenn die PIN der SIM-Karte (siehe das Feld **SIM-Karte verwendet PIN**) dreimal falsch eingegeben wurde. Geben Sie den PUK (Personal Unblocking Key) Ihrer SIM-Karte ein, um die SIM-Karte zu entsperren.
SIM-Karte verwendet PIN	Nur für **UMTS/LTE-Status** = *Aktiviert* Geben Sie die PIN Ihrer UMTS/LTE-Modemkarte ein.  **Hinweis** Die Eingabe einer falschen PIN unterbindet die Kommunikation bis der Eintrag korrigiert wird.  **Hinweis** Wenn das Gerät dreimal vergeblich versucht hat eine Verbindung aufzubauen, z. B. weil dreimal die falsche PIN eingegeben wurde, so müssen Sie zum Entsperren der SIM-Karte den **PUK** eingeben.
Fallback-Nummer	Nur für **UMTS/LTE-Status** = *Aktiviert*

Feld	Beschreibung
	Tragen Sie die Rufnummer für die Funktion GSM Fallback ein. Wenn ein Sprachruf auf diese Nummer eingeht, wird eine ggf. aktive Verbindung sofort getrennt und der Betriebsmodus des Modems auf GSM zurückgesetzt, in welchem das Modem so lange bleibt, bis wieder ein Datenruf (PPP, ISDN-Login, IPSec-Callback) erfolgt. Ist für die WAN-Verbindung der Flatrate-Modus aktiviert (Option **Immer aktiv** aktiviert in **WAN**->**Internet + Einwählen**->**UMTS/LTE**->), führt dies zu sofortigem Verbindungswiederaufbau. **Hinweis** Beachten Sie, dass die SIM-Karte diese Funktion unterstützen muss und nicht alle Mobilfunk-Anbieter Sprachrufe auf Daten-SIM-Karten weiterleiten.
APN (Access Point Name)	Nur für **UMTS/LTE-Status** = *Aktiviert* Wenn GPRS/UMTS/LTE benutzt werden soll, müssen Sie hier den sogenannten Access Point Name eintragen, den Sie von Ihrem Provider erhalten haben. Maximal können 80 Zeichen eingegeben werden. Wird hier nichts oder ein falscher APN angegeben, so funktioniert eine konfigurierte GPRS/UMTS/LTE-Verbindung nicht.

2.11 Menü WAN - UMTS/LTE

Hinweis

Beachten Sie, dass das Menü **UMTS/LTE** nur bei **bintec RS120wu** und **bintec RS230au+** (integriertes UMTS/HSDPA-Modem) bzw. **bintec RS232j-4G** (integriertes UMTS/HSDPA/LTE-Modem) oder bei Verwendung eines UMTS/HSDPA/LTE-USB-Sticks verfügbar ist!

Im Menü **WAN**->**Internet + Einwählen**->**UMTS/LTE** wird eine Liste aller konfigurierten GPRS/UMTS/LTE-Verbindungen angezeigt.

Mit den Mobilfunkstandards GPRS, UMTS und LTE kann eine Internet-Verbindung über

das Mobilfunknetz aufgebaut werden.

Das Menü **WAN**->**Internet + Einwählen**->**UMTS/LTE**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um die Internet-Verbindung eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
UMTS/ LTE-Schnittstelle	Wählen Sie die UMTS/LTE-Schnittstelle aus. Für **bintec RS120wu** ist das integrierte Modem mit Slot 6 Einheit 0 UMTS vorausgewählt, für Geräte mit optional gestecktem UMTS/ LTE-Stick der USB-Port des Geräts.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte sind *0* bis *3600* (Sekunden). *0* deaktiviert den Shorthold. Der Standardwert ist *300* .

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *IP-Adresse abrufen*(Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • *Statisch* : Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Lokale IP-Adresse	Nur bei **IP-Adressmodus** = *Statisch* Geben Sie die statische IP-Adresse des Verbindungspartners ein.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0* ... *15*). Standardwert ist *1* .

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *60* .
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte von *0* bis *100* . Der Standardwert ist *5* .
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *PAP* (Standardwert): Nur *PAP* (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur *CHAP* (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP* : Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **DNS-Server Primär** und **DNS-Server Sekundär** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

2.12 Menü Temperatur

Die Geräte der **bintec WI**-Serie sind mit einem Temperatur-Sensor ausgestattet. Dieser befindet sich auf der Hauptplatine unterhalb der ersten WLAN-Karte.

Der Sensor misst die aktuelle Temperatur. Sein Messbereich erstreckt sich von -55 °C bis +125 °C bei einer Genauigkeit von unter 1 °C.

Zusätzlich wird die erreichte Minimal- und Maximaltemperatur aufgezeichnet zusammen mit dem Zeitpunkt, an dem die jeweilige Temperatur erreicht wurde. Bei einem Neustart des Geräts werden die Werte zurückgesetzt und neu aufgezeichnet.

Standardmäßig sind untere und obere Grenzwerte für die Temperatur festgelegt, die bei Verletzung eine Alarm-Variable setzen und eine Syslog-Meldung erzeugen. Die Aktualisierung erfolgt alle 10 Sekunden.

Im Menü **Lokale Dienste**->**Überwachung**->**Temperatur** werden die Temperaturgrenzwerte konfiguriert. Sie können eine Grenzwertverletzung an eine Aktion koppeln.

Felder im Menü Basisparameter

Feld	Beschreibung
Trigger	Geben Sie hier die Temperatur ein, die nicht über- bzw. unterschritten werden soll.

Feld	Beschreibung
	Mögliche Werte: • *Temperatur über* • *Temperatur unter*
Aktion	Wählen Sie die gewünschte Aktion aus. Mögliche Werte: • *Aktivieren* (Standardwert) • *Deaktivieren*
Schnittstelle	Wählen Sie aus, über welche Schnittstelle die Aktion ausgeführt werden soll. Mögliche Werte: • *Relais* (Standardwert): Die Grenzwertverletzung wird mit dem Relais gekoppelt (siehe Menü **Physikalische Schnittstellen**->**Relais**->**Relaiskonfiguration**). • <Schnittstelle>: Bei Temperaturüberschreitung wird die gewählte Schnittstelle abgeschaltet.

Kapitel 3 Änderungen

Folgende Änderungen sind in **Systemsoftware 9.1.1** vorgenommen worden.

3.1 Neue Informationsfelder beim WLAN-Monitoring

Auf der Übersichtsseite im Menü **Wireless LAN Controller** -> **Monitoring** -> **Active Clients** wurden die drei neuen Spalten **Name**, **Client-IP-Adresse** und **Signal : Noise (dBm)** zur Verbesserung der Information und Fehlersuche eingefügt.

Unter **Wireless LAN Controller** -> **Monitoring** -> **Drahtlosnetzwerke (VSS)** wurde eine neue Spalte **Status** eingefügt. Diese zeigt an, ob die Access Points vom WLAN-Controller verwaltet werden () oder nicht ().

3.2 Signalisierung neuer Voice-Mail-Nachrichten am Systemtelefon

Bei Eingang einer neuen Voice-Mail-Nachricht wird ein Benachrichtigungstext im Display des Systemtelefons angezeigt.

3.3 Voice-Mail-Ansagen für Französisch

Es sind nun Voice-Mail-Ansagen für die Sprache Französisch verfügbar. Aktivieren Sie diese im Menü **Anwendungen** -> **Voice Mail System** ->**Voice Mail Boxen** unter **Voice Mail Sprache**.

3.4 Erweiterung des Mini-Callcenters

Das Mini-Callcenter wurde dahingehend erweitert, dass mehrere, in sich geschlossene Lösungen mit jeweils eigener Benutzeroberfläche und eigenem persönlichen Zugang entstehen. Bisher konnte das Callcenter in mehrere Bereiche aufgeteilt werden. Diese wurden allerdings nicht dargestellt. Jetzt verfügt jedes neue Mini-Callcenter über eigene Leitungen und Agenten.

Neue Callcenter werden zusammen mit Leitungen angelegt. Dazu wurde ein neuer Dialog im Menü **Anwendungen** -> **Mini-Callcenter** -> **Leitungen** -> **Neu** eingefügt. Die Option unter **Beschreibung des Call Centers** muss auf `Neu` eingestellt bleiben. Dadurch kann im dahinterliegenden Feld ein Name für das neue Mini-Callcenter vergeben werden. Wurde

ein Callcenter erfolgreich erzeugt, können diesem neue Leitungen hinzugefügt werden, indem im Auswahlfeld **Beschreibung des Call Centers** der Name des zuvor erzeugten Callcenters ausgewählt wird.

Die Status-Anzeige für die Callcenter im Menü **Anwendungen** -> **Mini-Callcenter** -> **Status** wurde dahingehend geändert, dass für ein Callcenter die zugeordneten Leitungen sowie den Leitungen zugeordnete Teilnehmer in einem Block zusammengefasst werden.

Im Menü **Anwendungen** -> **Mini-Callcenter** -> **Leitungen** wurde der Listenansicht der Leitungen eine zusätzliche Spalte **Zugewiesen zu** hinzugefügt, die den Namen des Callcenters enthält, zu dem die Leitung gehört.

Bei der Erzeugung neuer Agenten im Menü **Anwendungen** -> **Mini-Callcenter** -> **Agents** -> **Neu** wurde zur besseren Übersicht der Auswahl von Leitungen noch der Name des zugehörigen Callcenters hinzugefügt.

3.5 Erhöhung der Anzahl privater Telefonbucheinträge

Die Anzahl der privaten Telefonbucheinträge für jeden Benutzer wurde von 20 auf 50 erhöht.

3.6 Funktionstaste verschieben

Sie können jetzt eine konfigurierte Funktionstaste von einem Systemtelefon auf ein anderes übertragen.

Gehen Sie dazu ins GUI-Menü **Nummerierung** -> **Zuordnung der Endgeräte** -> **Systemtelefon** ->  -> **Tasten**. Wählen Sie das Symbol  , um konfigurierte Funktionstasten zu verschieben. Im Popup-Menü können Sie noch einmal **Tastenname**, **Tastentyp** und **Einstellungen** überprüfen. Wählen Sie anschleißend das **Telefon** (Telefonsystem), das **Modul** (Telefon oder Tastenerweiterung) und die **Taste** (neue Nummer der Funktionstaste im anderen Telefon) zu der die Funktion verschoben werden soll.

Sie können diese Verschiebung auch im Benutzerzugang im Menü **Benutzerzugang** -> **Systemtelefone** -> **Zugewiesene Systemtelefone** ->  -> **Tasten** durchführen. Dort können Sie Tasten allerdings nur innerhalb Ihres eigenen Telefonsystems verschieben.

3.7 Neue Profile für den Internetzugangs-Assistenten

Es wurden Standard-Profile für die Dienste **VDSL** und **Entertain VDSL** der Deutschen Telekom AG geschaffen. Damit ist es möglich, diese Anschlüsse komfortabel über den Assistenten einzurichten. Gehen Sie dazu ins GUI-Menü **Assistenten** -> **Internetzugang** -> **Neu**. Wählen Sie im Dialog *Externes xDSL-Modem* und bestätigen Sie mit **Weiter**. Verwenden Sie den passenden **physischen Ethernet-Port**, belassen Sie den **Typ** auf *Vordefiniert* und wählen Sie unter **Land** *Germany*. Nun können Sie unter **Internet Service Provider** unter anderem auch *Telekom - VDSL* oder *Telekom Entertain - VDSL* als Internetzugangsoptionen festsetzen.

3.8 BRRP: Anzeige des BRRP-Status mithilfe der Status-LED

Ab **Systemsoftware 9.1.1** können Sie anhand der Status-LED feststellen, in welchem Zustand sich der Router im BRRP-Betrieb befindet. Leuchtet die Status-LED, agiert das Gerät als Master-Router. Leuchtet die Status-LED nicht, fungiert es als Backup-Router. Wird der Router initialisiert, blinkt die Status-LED.

BRRP-Status	LED-Anzeige
Master-Router	LED leuchtet
Backup-Router	LED aus
Initialisierung	LED blinkt

3.9 Überwachung des Standard-Gateways

Mithilfe des Keep Alive Monitoring kann das Standard-Gateway überwacht werden. Falls es nicht mehr erreichbar ist, kann automatisch eine andere Schnittstelle verwendet werden.

Um diese Funktion einzurichten, gehen sie ins Konfigurationsmenü **Lokale Dienste** -> **Überwachung** -> **Hosts** -> **Neu**. Dieses Einstellungsmenü wurde neu strukturiert. Erzeugen Sie mit *Neue ID* einen neuen Eintrag. Besteht bereits eine Gruppe können Sie diese unter **Gruppen-ID** auswählen und bearbeiten.

Bei **Überwachte IP-Adresse** wählen Sie *Standard-Gateway*. Die restlichen Einstellungen für **Quell-IP-Adresse**, **Intervall**, **Erfolgreiche Versuche** und **Fehlgeschlagene Versuche** können Sie entsprechend Ihren eigenen Wünschen konfigurieren. Unter **Auszuführende Aktion** wählen Sie *Erneut wählen* und legen anschließend die Schnittstelle fest, über die die Verbindung nach einem Verlust des Standard-Gateways aufgebaut werden

soll.

3.10 Änderungen am WLAN-Controller

3.10.1 Veränderungen im Menü Benachbarte APs

Das Menü **Benachbarte APs** unter **Wireless LAN Controller** -> **Monitoring** wurde neu strukturiert. APs werden nun entsprechend ihrer SSID und BSSID zu Netzwerken gruppiert, um die Anzahl der angezeigten Tabelleneinträge zu reduzieren.

Die Aufteilung der einzelnen Tabellenspalten zeigt nun folgende Form:

Spalte	Label	Beschreibung
1	**SSID**	Alle gefundenen SSIDs alphabetisch geordnet
2	**MAC-Adresse**	MAC-Adresse oder Basic Service Set Identifier (BSSID)
3	**Signal dBm**	Signalstärke in dBm
4	**Kanal**	Verwendeter Kanal
5	**Sicherheit**	Sicherheitseinstellungen des AP
6	**Zuletzt gesehen**	Zeit, die seit der letzten Detektion des AP verstrichen ist
7	**Stärkstes Signal empfangen von**	Location und Name des Slave AP, der das stärkste Signal empfangen hat
8	**Summe der Erkennungen**	Anzahl der Detektionen mit derselben BSSID

Für eine Fehlersuche bzw. eine Optimierung des Netzwerks ist vor allem die empfangene Signalstärke entscheidend. Die Sicherheitseinstellungen geben Hinweise auf die Errichtung eines unsicheren Netzes innerhalb der eigenen WLAN-Infrastruktur.

3.10.2 Neuanordnung der Schaltflächen im Wireless LAN Controller Wizard

Die Reihenfolge der Schaltflächen **Weiter** und **Abbrechen** in allen Schritten des **Wireless LAN Controller Wizard** wurde vertauscht und an den allgemeinen Stil des GUI angepasst.

3.10.3 Wahl der Chiffre im Wireless LAN Controller Wizard

Im Assistenten für den WLAN Controller wurde im dritten Konfigurationsschritt die Auswahlmöglichkeit des **WPA Cipher** entfernt.

Falls unter **WPA-Modus** *WPA* ausgewählt wird, ist automatisch die **WPA Cipher** *TKIP* aktiviert. Falls hingegen unter **WPA-Modus** *WPA 2* ausgewählt wird, ist automatisch die **WPA Cipher** *AES* aktiviert.

3.10.4 Bezeichnungsänderung des DHCP-Servers im Wireless LAN Controller Wizard

Im ersten Konfigurationsschritt des **Wireless LAN Controller Wizard** kann nun für den **DHCP-Server** *Extern und statisch* oder *Intern* ausgewählt werden. Die Aktivierung der ersten Option bewirkt eine statische Zuordnung der IP-Adressen an die APs oder eine dynamische Zuteilung durch einen externen DHCP-Server. Falls *Intern* gewählt wurde, verhält sich das Gerät selbst wie ein DHCP-Server. In diesem Fall muss die CAPWAP-Option 138 gewählt werden, um eine Kommunikation zwischen dem Controller und den APs zu realisieren.

Hinweis

Bei einem externen DHCP-Server muss die CAPWAP-Option 138 aktiviert sein.

3.10.5 Bezeichnung eines Slave Access Points

Für einen Slave AP kann nun zusätzlich zum **Standort** ein **Name** vergeben werden. Als voreingestellter Wert wird der Gerätename verwendet.

Der Name kann einerseits im letzten Schritt des Assistenten im Menü **Wireless LAN Controller** -> **Wizard** konfiguriert werden. Auf der Übersichtsseite für die **Slave Access Points** kann der Wert im Feld **Name** verändert werden. Andererseits kann im Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** -> unter **Name** eine andere Bezeichnung eingetragen werden.

3.10.6 Vereinfachung der Firmware-Wartung

Im Menü **Wireless LAN Controller** -> **Wartung** -> **Firmware-Wartung** wurde die Möglichkeit geschaffen, alle Access Points gleichzeitig auszuwählen bzw. aus der Auswahl zu entfernen. Durch Betätigen des Verweises **Alle auswählen** bzw. **Alle deaktivieren** werden alle APs ausgewählt bzw. für alle APs die Auswahl aufgehoben. Somit kann ein großer Bestand an Access Points leichter verwaltet werden.

3.10.7 Warnung im Fall einer Einstellungsänderung des DHCP-Servers

Für den Fall, dass ein Anwender den **Wireless LAN Controller Wizard** startet und der DHCP-Server bereits an der gewünschten LAN-Schnittstelle ausgeführt wird, kann der DHCP-Server nur durch die Aktivierung der DHCP-Option **CAPWAP Adresse** aktualisiert werden. Dabei erhalten allerdings bereits verbundene Access Points keine neue CAPWAP-Adresse. Dadurch werden sie auch nicht im vierten Schritt des Konfigurationsprozesses angezeigt. Da keine technische Lösung dieses Problems existiert, muss für diejenigen Access Points, die schon mit dem WLAN-Controller verbunden waren, ein Reset durchgeführt werden. Eine entsprechende Warnmitteilung wurde im ersten Konfigurationsschritt des **Wireless LAN Controller Wizard** eingefügt.

3.10.8 Assistent für die E-Mail-Benachrichtigung

Nach Abschluss des vierten Konfigurationsschrittes im Assistenten des WLAN-Controllers kann nun sofort eine E-Mail-Benachrichtigung eingerichtet werden. Durch Betätigen der Schaltfläche **START** neben **Benachrichtigungsdienst für WLAN-Überwachung konfigurieren** wird man ins Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungsempfänger** geleitet und kann dort die Berichterstellung für WLAN-Ereignisse konfigurieren.

3.10.9 LED-Verhalten der Slave-APs

Sie können nun das Leuchtverhalten der Slave-APs festlegen.

Wechseln Sie dazu in das Menü **Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**. Hier können sie unter **Slave-AP-LED-Modus** die Konfiguration vornehmen. Wählen Sie die Standardeinstellung *Status* blinkt nur die Status-LED des APs einmal in der Sekunde. Bei *Blinkend* zeigen die LEDs des APs ihr bisheriges Standardverhalten und mit der Einstellung *Aus* können Sie alle LEDs deaktivieren.

3.11 HotSpot - Walled Garden Pages aus unterschiedlichen IP-Adressbereichen

HotSpot-Betreiber können nun den Zugriff auf frei zugängliche Webseiten aus verschiedenen IP-Adressbereichen erlauben. Aktivieren Sie dazu unter **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu Walled Garden**. Geben Sie die **Walled Garden URL** des Intranet-Servers ein. Webseiten sind nun über diese Adresse und alle Adressen erreichbar, die unter **Zusätzliche, frei zugängliche Domänennamen** mithilfe von **Hinzufügen** eingetragen wurden.

3.12 VoIP-Wahlverhalten

Bei der Einwahl über VoIP wird der Wahlvorgang durch Eingabe von # oder nach einer voreingestellten Zeitspanne abgeschlossen. Beide Wählmethoden werden von der **elmeg hybird** nun gleichwertig behandelt. Das Raute-Zeichen wird intern nicht mehr verwendet. Dadurch werden Konflikte mit den von der **elmeg hybird** verwalteten Datenbanken (Telefonbuch, Anruferliste, usw.) vermieden.

Hinweis: Eine Anpassung der Systemtelefone ist ebenfalls notwendig.

3.13 Durchsage und Wechselsprechen in der Benutzeroberfläche aktivieren

Die Funktionen Durchsage und Wechselsprechen können jetzt direkt in der Benutzeroberfläche der **elmeg hybird** freigegeben werden. Es ist nicht mehr notwendig, die Funktionstaste Durchsage erlauben bzw. Wechselsprechen erlauben am Systemtelefon zu konfigurieren.

Um das automatische Annehmen einer Durchsage bzw. einer Wechselsprech-Anfrage zu erlauben, gehen Sie in das Menü **Nummerierung** -> **Zuordnung der Endgeräte** -> **Systemtelefon** ->  -> **Einstellungen** -> **Erweiterte Einstellungen**. Hier können Sie **Durchsage** oder das **Wechselsprechen empfangen** für jedes Gerät separat genehmigen.

Hat ein Systemtelefon mehrere Rufnummern, so werden die Einstellungen ausschließlich für die erste MSN übernommen.

Ist bereits eine Funktionstaste am Systemtelefon programmiert, so wird außerdem die Leuchtdiode entsprechend des GUI-Zustands gesteuert.

Die Einstellung kann auch im Benutzerzugang im Menü **Benutzerzugang** -> **Systemtelefone** -> **Zugewiesene Systemtelefone** ->  -> **Einstellungen** -> **Erweiterte Einstellun-**

gen vorgenommen werden.

3.14 Team ein-/ ausloggen

Es ist lediglich mit Systemtelefonen möglich, sich aus einem Team über die Funktionstaste "Ein-/ Ausloggen Team" abzumelden. Bei Standard-Telefonen kann diese Funktion nun über den **Benutzerzugang** erreicht werden.

Wechseln Sie dazu auf die Benutzeroberfläche in das neue Menü **Benutzerzugang** -> **Einstellungen** -> **Einstellungen von Features** ->  ->**Einloggen/Ausloggen**. Hier können Sie sich durch die Aktivierung bzw. Deaktivierung des Auswahlfeldes in der Spalte **Status** in den verschiedenen Teams an- oder abmelden. Die Veränderungen müssen Sie anschließend noch mit **Übernehmen** bestätigen.

An einem angeschlossenen Systemtelefon programmierte Funktionstasten werden entsprechend synchronisiert.

3.15 Funktionstaste Leitungstaste

Unter einer Funktionstaste "Leitungstaste" wird ein Kanal eines externen POTS- , ISDN- oder VoIP-Anschlusses eingerichtet. Wird diese Taste am Systemtelefon betätigt, wird automatisch Freisprechen eingeschaltet und der erste freie Kanal des Anschlusses belegt (Bsp.: Es sind vier Leitungstasten konfiguriert. Falls die dritte Taste im Ruhezustand gedrückt wird, wird der Zustand auf der ersten Leitungstaste signalisiert.). Sie hören dann den externen Wählton und die LED der Leitungstaste des entsprechenden Kanals leuchtet.

Wird ein externer Anruf an einem anderen internen Systemtelefon signalisiert, blinkt die LED der nächsten freien Leitungstaste an Ihrem Telefon. Sie können diesen durch Betätigen der Leitungstaste heranholen.

Eine Leitungstaste kann beliebig oft an einem Systemtelefon vergeben bzw. auf mehreren Tasten konfiguriert werden.

Hinweis: Für das neue Prinzip der Leitungstastensteuerung wird eine aktuelle Firmware-Version der Systemtelefone benötigt.

3.16 Erweiterung der Anrufvarianten

Bis zur **Systemsoftware 9.1.1** konnten die Anrufvarianten 1 bis 4 nur für alle Teams simultan geändert werden. Dazu wird die Sequenz ** 91 n* im Telefon eingegeben. *n* steht dabei für eine Zahl von 1 bis 4. Diese repräsentiert die Anrufvarianten. Nun können die Anrufvarianten für jedes Team separat umgeschaltet werden. Hierfür muss die Abfolge nur um die entsprechende Teamnummer (MSN) ergänzt werden. Die Sequenz hat dann die folgende Form: ** 91 tm n . tm* bezeichnet hier die Teamnummer (MSN).

Diese neue Kennziffernprozedur kann nur von Teilnehmern verwendet werden, die über eine dem Benutzer zugeordnete Berechtigungsklasse hierfür freigeschaltet sind.

3.17 Verbesserung der Displayanzeige bei den Modellen elmeg CS 4x0x und elmeg IP-S 400

Bei einem Amtsruf wurde im Display der Modelle **elmeg CS 4x0x** und **elmeg IP-S 400** abwechselnd die Bezeichnung des Amtes und der Name der Rufnummer angezeigt.

Dieses Verhalten kann jetzt genauer konfiguriert werden. Im Menü **Nummerierung** ->**Benutzereinstellungen** -> **Berechtigungsklassen** ->  -> **Grundeinstellungen** -> **Erweiterte Einstellungen** können Sie im Feld **Zusätzliche Information für externen Anruf** die Anzeigearten *Nur Name der Nummer* (Standardwert), *Namen des Anschlusses und der Nummer*, *Nur Name des Anschlusses* und *Keine* auswählen.

3.18 Hold am externen S_0-Anschluss abschalten

Es besteht nun die Möglichkeit die ISDN-Information "Hold" am externen S_0-Anschluss abzuschalten. Dies ist notwendig, da mehrere Provider aufgrund der ISDN-Information "Hold" die Verbindung stumm schalten oder eine eigene Melodie (meist nur Ton oder Text) einspielen.

Aktivieren oder deaktivieren Sie dazu die Funktion im Menü **Nummerierung** -> **Externe Anschlüsse** -> **Anschlüsse** ->  -> **Erweitere Einstellungen** bei **Halten im System**. Standardmäßig ist Funktion nicht aktiv.

3.19 Wave-Datei abspielen und von der SD-Karte auf den PC kopieren

Wave-Dateien der Voice-Applikationen, wie die Ansage vor einer Abfrage, MoH, Infotext, Weckansagen, usw. aber auch Voice-Mail-Ansagen, Mitschnitte und Sprachnachrichten, können von Ihnen abgehört oder von der SD-Karte auf den PC kopiert werden, um sie dort abzuspielen.

Gehen Sie dazu ins Menü **Anwendungen** -> **Voice-Applikationen** -> **Wave-Dateien**. Zum Speichern einer Nachricht klicken Sie auf das -Symbol. Daraufhin öffnet sich der Download-Dialog. Um die Voice-Mail-Nachricht anzuhören, klicken Sie auf das -Symbol.

3.20 Berechtigungsklassen unter Monitoring sowie im Benutzerzugang anzeigen

Sie haben nun die Möglichkeit, sich die für einen Benutzer vergebenen Berechtigungsklassen im Monitoring anzeigen zu lassen.

Wechseln Sie hierzu ins Menü **Monitoring** -> **Statusinformationen** -> **Benutzer** -> . Hier werden Ihnen unter **Aktuelle Berechtigungsklasse** alle vergebenen Klassen angezeigt. Die aktuell Aktive ist entsprechend gekennzeichnet ( ).

Die **Aktuelle Berechtigungsklasse** wird ebenfalls im Benutzerzugang unter **Benutzerzugang** -> **Status** angezeigt.

3.21 Benachrichtigung im Fall einer E-Mail-Weiterleitung

Während des Abhörens einer Sprachnachricht am Telefon kann diese mithilfe der Taste "5" an eine E-Mail-Adresse weitergeleitet werden. Bisher wurde die Nachricht ohne Rückmeldung bis zum Ende abgespielt. Mit der neuen Firmware-Version wird die Wiedergabe der Nachricht bei Betätigen der Taste "5" abgebrochen und per E-Mail versandt. Eine Bestätigungsansage informiert über Erfolg bzw. Misserfolge der Weiterleitung. Diese neuen Ansagen stehen in deutsch, englisch und französisch zur Verfügung.

3.22 DSP-Nutzungsanzeige auf der GUI-Statusseite

Im GUI-Menü **Systemverwaltung** -> **Status** werden unter **Module** neben den eingesetzten DSP-Modulen die aktuell belegten DSP-Kanäle angezeigt (belegt / vorhanden).

3.23 TAPI: Anzeige der Rufnummer bei einem externen Anruf

Die Telefonnummer des Anrufers (Caller-ID) wird jetzt über das TAPI-Feld "connected-ID" übertragen. Somit kann dessen Rufnummer schon vor Annahme des Anrufs oder bei weitervermittelten Gesprächen registriert werden.

3.24 Änderung der Standardeinstellungen

Es wurden für mehrere Werte die Standardeinstellungen geändert:

Im Menü **Nummerierung** -> **Benutzereinstellungen** -> **Benutzer** -> **Neu** -> **Grundeinstellungen** wurden die voreingestellten Werte für die **Berechtigungsklassen Standard**, **Optional** und **Nacht** von *Nicht erlaubt* auf *Default CoS* geändert.

Im Menü **Nummerierung** -> **Benutzereinstellungen** -> **Benutzer** -> **Neu** -> **Rufnummern** sind jetzt **System-Telefonbuch** und **Besetztlampenfeld** standardmäßig aktiviert.

Im Menü **Nummerierung** -> **Benutzereinstellungen** -> **Berechtigungsklassen** -> 
sind auf den Karteikarten **Leistungsmerkmale** und **Anwendungen** folgende Auswahlfelder standardmäßig aktiviert:

- **Anklopfen**
- **Call Through**
- **Wechselsprechen empfangen**
- **Durchsage**
- **MWI-Informationen empfangen**
- **Verbindungsdaten speichern**
- **Gebührenübermittlung**

Im Menü **Nummerierung** -> **Zuordnung der Endgeräte** -> **Analog** sind unter den **Erweiterten Einstellungen** die Funktionen **Rufnummer anzeigen (CLIP)** und **Neue Nachrichten anzeigen (MWI)** standardmäßig aktiviert. Der Standardwert für die **FXS-Rufwechselspannung** beträgt mittlerweile *50 Hz*.

3.25 Benutzer nach internen Rufnummern filtern

Im Menü **Nummerierung** -> **Benutzereinstellungen** -> **Benutzer** kann unter **Filtern in** nun auch nach der **Internen Rufnummer** gefiltert werden.

3.26 Änderung der Sortierreihenfolge bei ISDN-Slots

Im Menü **Nummerierung** -> **Zuordnung der Endgeräte** -> **ISDN** werden die Slots unter **Schnittstelle** nun entsprechend ihrer Nummerierung sortiert.

3.27 System-Telefonbuch

3.27.1 System-Telefonbuch löschen

Um das System-Telefonbuch komplett zu löschen, gehen Sie in das Menü **Anwendungen** -> **System-Telefonbuch** -> **Allgemein**. Hier aktivieren Sie unter **Telefonbuch löschen** die Schaltfläche **Löschen**. Daraufhin erscheint eine Sicherheitswarnung. Mit **OK** bestätigen Sie Ihre Entscheidung.

3.27.2 System-Telefonbuch mit LDAP bereitstellen

Die **elmeg hybird** unterstützt nun LDAP (Lightweight Directory Access Protocol), um Einträge des System-Telefonbuchs anderen Geräten bzw. Anlagen, wie OpenStage 40/60, bereitzustellen. Name, Rufnummer (MSN) sowie mobile und private Rufnummer können auf diese Weise transferiert werden.

LDAP ist werksseitig aktiviert und benötigt keine Konfiguration. Der Client kann sich anonym oder über Benutzername und Passwort mit der Telefonanlage verbinden.

Die LDAB-Parameter für Name, MSN, mobile und private Rufnummer (sn, telephoneNumber, mobile, homePhone) werden dabei in den zwei MIB-Tabellen **mpsPhonebookTable** und **mpsExtensionAdmin** abgelegt.

mpsPhonebookTable

LDAP	MIB
sn	mpsPhonebookName
telephoneNumber	mpsPhonebookNumber
mobile	-
homePhone	-

mpsExtensionAdmin

LDAP	MIB
sn	mpsUserName
telephoneNumber	mpsExtensionNumber
mobile	mpsUserMobileNumber
homePhone	mpsUserHomeNumber

Über den Debug-Mechanismus "debug ldap" können Sie detaillierte Informationen auslesen.

3.28 Im Kalender die Feiertage nach Datum sortieren

Die Feiertage im Menü **Anwendungen** -> **Kalender** -> **Feiertage** werden nach Datum und nicht mehr alphabetisch sortiert.

3.29 Offene Rückfrage für SIP-Telefone

Die Kennziffernprozeduren zum Einleiten der "Offenen Rückfrage" sind mittlerweile für Standard-SIP-Telefone freigeschaltet.

3.30 Telefonsperre / Externwahlberechtigung mit PIN

Über eine spezielle Kennziffernprozedur kann ein beliebiges Telefon temporär zur Externwahl mit den eigenen, persönlichen Berechtigungen verwendet werden. Dazu ist die Eingabe der MSN und zugehörigen PIN des Benutzers erforderlich.

Für eine Einzelwahl gehen Sie dabei folgendermaßen vor:

(1) Wählen Sie die Sequenz `*5*` an einem beliebigen Telefon.

(2) Geben Sie Ihre eigene MSN ein.

(3) Betätigen Sie die Stern-Taste.

(4) Geben Sie ihre eigene 4-stellige PIN ein.

(5) Sie hören den externen Wählton.

(6) Geben Sie eine externe Rufnummer ein.

Die folgenden Benutzer-spezifischen Eigenschaften werden daraufhin temporär für diesen Einzelruf verwendet:

- Typ des Teilnehmers

- Amtsberechtigung (CoS)
- Amtsbelegungsreihenfolge (CoS)
- Externe MSN / DDI-Signalisierung
- Weitere Legitimationen der Berechtigungsklasse

Einige Korrelationen der Leistungsmerkmale bzw. Einschränkungen sind bei dieser Art der Externwahl zu berücksichtigen:

- Der Besetztzustand einer überwachten (vorhergehenden) MSN muss nach Eingabe der neuen MSN geändert werden.
- Das Besetztlampenfeld (LED) der Systemtelefone muss aktualisiert werden.
- Wenn TAPI-Monitoring aktiv ist, ändert sich zwar der Leitungszustand, dieser wird der PC-Applikation aber nicht signalisiert.
- Beim Einleiten einer Rückfrage-Verbindung muss die zuvor eingegebene Benutzer-MSN ebenfalls signalisiert werden.
- Wird eine Rückfrageverbindung im Wahlzustand durch das Auflegen des Hörers beendet, erfolgt kein Wiederanruf, da die eingegebene Benutzer-MSN nicht mit dem Gerät übereinstimmt.
- Wird eine Rückfrageverbindung über einen Blind Transfer (Transfer ohne Ankündigung) übergeben, erfolgt ebenfalls kein Wiederanruf nach Zeit.
- Die gleichen o. g. Beschränkungen gelten für Rückfrage-Rufe in Teams.
- Ein Wiederanruf nach Zeit einer Offenen Rückfrage wird beim Original-Gerät signalisiert.
- Automatische Rückrufe (CCBS and CCNR) werden nicht zugelassen.
- Die Telefon-Entsperrprozedur kann nicht in einer normalen Rückfrage-Verbindung gewählt werden.

3.31 Zusammenfassung der ADSL- und VDSL-Menüs

Für die Geräte **bintec R3002** und **bintec RT3002** bzw. **bintec R3502** sind die Menüs **ADSL**- bzw. **VDSL-Modem** unter **Physikalische Einstellungen** entfallen. Die entsprechenden Einstellung befinden sich nun unter **Physikalische Einstellungen** -> **DSL-Modem**.

3.32 Alphabetische Sortierung der Wartungsfunktionen

Die Parameter unter **Aktion** im Menü **Wartung** ->**Software & Konfiguration** -> **Optionen** sind mittlerweile alphabetisch angeordnet.

3.33 biboAdmConfig: Syntax-Änderung

Die Syntax zur Konfiguration von biboAdmConfigHostUrl hat sich geändert. Im Folgenden sind die Kommandos für SNMP und configd aufgeführt.

SNMP:

```
cmd=put hosturl="xmodem:1k"
```

configd:

```
configd put all xmodem:1k
```

3.34 hybird 120 / 130: ISDN-LED

Das Leuchtverhalten der ISDN-LEDs wurde erweitert. Zusätzlich kann nun auch die Belegung der B-Kanäle abgelesen werden.

ISDN-LED-Anzeige

Farbe	Status	Information
Gelb	an	Schicht 1 ist aktiv
Gelb	aus	Ruhezustand bzw. außer Betrieb
Gelb	langsam blinkend (einmal pro Sekunde)	ein B-Kanal ist aktiv
Gelb	schnell blinkend (zweimal pro Sekunde)	zwei B-Kanäle sind aktiv

Kapitel 4 Behobene Fehler

Hinweis

Beachten Sie, dass die im Folgenden speziell erwähnten Änderungen nicht den gesamten Umfang der Fehlerbehebungen darstellen. Insbesondere müssen sie nicht für alle Produkte zutreffen. Selbst wenn die folgenden Korrekturen für Ihr Gerät nicht relevant sein sollten, profitiert es dennoch von den allgemeinen Verbesserungen des Patches.

Folgende Fehler sind in **Systemsoftware 9.1.1** behoben worden:

4.1 System - Validierung der Softwareversion

(ID 12594)

Zur Vermeidung unnötiger Downloads wird die Versionsnummer der Firmware mittlerweile vor dem Herunterladen der Datei überprüft. Bisher fand eine Kontrolle der Versionsnummer erst nach dem Herunterladen vom Server und einer anschließenden CRC-Verifikation statt.

Dies behebt die Update-Problematik bei Telekom VPN-Business-Anschlüssen.

Das Problem wurde gelöst.

4.2 GUI - Internet-Assistent

(ID 14701)

Der Assistent für den Internetzugang des **bintec R3502** war nicht in der Lage, einen ADSL- oder ADSL2-Anschluss einzurichten. Dieses Fehlverhalten wurde beseitigt, sodass es nun möglich ist, eine solche Verbindung komfortabel über den Assistenten zu erzeugen.

Das Problem wurde gelöst.

4.3 Telefonie - Aufbau einer Konferenz

(ID 14230)

Der Aufbau einer Konferenz von einem IP-Systemtelefon zu einem ISDN-Systemtelefon war nicht möglich.

Das Problem wurde gelöst.

4.4 Telefonie - Fälschlich ausgelöste Konferenz

(ID 14229)

Nach einer Rückfrage bzw. beim Mitschneiden aus einer ESTOS-Anwendung wurde eine 3er-Konferenz ausgelöst. Dieses Fehlverhalten wurde beseitigt.

Das Problem wurde gelöst.

4.5 System - Tracing-Fehler bei GSM/UMTS/LTE

(ID 16957)

Tracing funktionierte nicht in Verbindung mit GSM-, UMTS- oder LTE-basierten PPP-Schnittstellen.

Das Problem wurde gelöst.

4.6 IPSec - Panik bei Openswan bzw. strongSwan

(ID 12125)

Falls die Linux-IPSec-Implementierungen Openswan oder strongSwan einen IPSec-Tunnel initiierten und in diesen die Phase-2-Konfiguration weder ein lokales noch ein Remote-Subnetz aufwies, kam es beim Responder zu einer Panik.

Das Problem wurde gelöst.

4.7 IP - Stacktrace in Verbindung mit der Schnittstelle "LOCAL"

(ID 16970)

Falls sich die IP-Adresse der Schnittstelle "LOCAL" sowie die Zieladresse eines IP-Pakets im gleichen Subnetz befanden, stürzte die Anlage mit einem Stacktrace ab.

Das Problem wurde gelöst.

4.8 IPsec - Dormant IPSec-Peers

(ID 14518)

Ein IPSec-Peer, der mittels eines RADIUS-Servers angelegt wird, soll zusammen mit allen abhängigen Einträgen gelöscht werden, sobald sein Status auf "down", "blocked" oder "dormant" wechselt. Peers im Zustand "dormant" wurden aber nicht immer entfernt.

Das Problem wurde gelöst.

4.9 DNS - Zeitüberschreitung in der Initialisierungsphase

(ID 16909)

Die Bearbeitung eines DNS-Requests benötigte bis zu 5 Sekunden, falls sich kein passender Eintrag im DNS-Cache befand. Dadurch wurde auch die Funktion des DynDNS-Service beeinträchtigt.

Das Problem wurde gelöst.

4.10 GUI - Konfigurationssicherung während der Suche nach benachbarten APs

(ID 16037, 16771, 16776, 16782, 16871)

Eine Sicherung der Konfiguration während eines Scans nach benachbarten APs führte zu unbrauchbaren MIB-Tabellen.

Der Sicherungsmechanismus wurde diesbezüglich angepasst. Die Veränderungen des Scan-Prozesses werden in die gespeicherten Tabellen übernommen.

4.11 IPSec - Panik beim Shrew Soft VPN Client

(ID 16823)

Im Fall eines Tunnelaufbaus zu einem Teldat-Gateway durch den Shrew Soft VPN Client konnte es zu einer Panik kommen. Dazu musste der **IKE Config Mode** im Shrew Soft VPN Client auf *Auto Configuration* gesetzt sein, WINS oder DNS aktiviert sein oder die IKE Config-Mode Reply Message zwei Adressen für den WINS- und DNS-Server enthalten.

Das Problem wurde gelöst.

4.12 DHCP - Fehler im DHCP-Relay-Mechanismus

(ID 15915)

Falls beim DHCP-Client mehrere Schnittstellen auf einem physischen Ethernet-Kabel konfiguriert waren und das Broadcast Flag nicht gesetzt wurde, versagte das DHCP-Relay-System.

Das Problem wurde gelöst.

4.13 QoS - Automatische Erstellung einer Standard-QoS-Richtlinie

(ID 16561)

Beim Anlegen einer neuen QoS-Richtlinie im Menü **Netzwerk** -> **QoS** -> **QoS-Schnittstellen/Richtlinien** -> **Neu** unter dem Menüpunkt **Queues/Richtlinien** wird automatisch ein Standard-Eintrag mit der kleinsten Priorität (= 255) angelegt. Dieser wird bereits durch Anklicken von **Hinzufügen** erzeugt, ist für den Benutzer aber erst nach einer Bestätigung mit **OK** zu erkennen.

Der Anwender wird in der Benutzeroberfläche auf diesen Umstand jetzt explizit hingewiesen.

4.14 Lastverteilung - Fehler bei der Konfiguration des Routenselektors

(ID 16536)

Beim Anlegen einer neuen Lastverteilungsgruppe im Menü **Netzwerk** -> **Lastverteilung** -> **Lastverteilungsgruppen** -> **Neu** führte die Konfiguration des **Routenselektors** unter **Schnittstellenauswahl für Verteilung** -> **Hinzufügen** -> **Erweiterte Einstellungen** zu korrupten MIB-Einträgen.

Das Problem wurde gelöst.

4.15 DHCP - Panik des DHCP-Servers

(ID 16567)

Falls keine "freien" IP-Adressen im dynamischen IP-Adress-Pool mehr zur Verfügung standen, kam es beim DHCP-Server zu einer Panik mit Nullzeiger-Zugriff.

Das Problem wurde gelöst.

4.16 hybird - Anrufvarianten für TFE schalten

(ID 16787)

Für alle TFEs können nur die Anrufvarianten 1 und 2 simultan mithilfe der Kennziffernprozedur **92x* (x = 1, 2) umgeschaltet werden.

4.17 SIP - Unterdrückung der Rufnummer

(ID 19709)

Es war nicht möglich einen anonymen Anruf von einem SIP-Telefon aus zu initiieren.

Das Problem wurde gelöst.

4.18 UMTS - Reaktivierung des UMTS-Modems

(ID 16758)

Falls ein UMTS-Modem deaktiviert und die Konfiguration gesichert wurde, war es über die Benutzeroberfläche nicht möglich das Modem zu reaktivieren.

Das Modem kann nun im Menü **Physikalische Schnittstellen** -> **UMTS/LTE** unter **Aktion** aktiviert und deaktiviert werden.

Das Problem wurde gelöst.

4.19 System - Erzeugung von Standard-Systemlizenzen

(ID 13960)

Um die Standardlizenzen eines Geräts wiederherstellen zu können, wird die Schaltfläche **Stdrd. Lizenzen** im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen** betätigt. Dabei wurde nicht überprüft, ob die Lizenz bereits angelegt war. Somit konnten über diese Prozedur immer neue Einträge angelegt werden.

Das Problem wurde gelöst.

4.20 SNMP - Dienst abschalten

(ID 16173)

Falls **snmpAdminPort** = *0* war, wurde der SNMP-Dienst nicht wie vorgesehen deaktiviert.

Das Problem wurde gelöst.

4.21 PPTP - Panik bei PPTP in Verbindung mit MPPE

(ID 16662)

Bei der Verwendung von PPTP mit MPPE kam es zu einer Panik.

Das Problem wurde gelöst.

4.22 bintec R3802: Status der SHDSL-Schnittstelle

(ID 11187)

Auf der Status-Seite der **bintec R3802** im GUI-Menü unter **Systemverwaltung** -> **Status** der Status des SHDSL-Schnittstelle nicht akkurat wiedergegeben (z. B. die möglichen Wire Modes).

Das Problem wurde gelöst: Die Bezeichnung der Schnittstelle wird nun wie im Menü **Physikalische Schnittstellen** -> **SHDSL** ->**SHDSL-Konfiguration** angezeigt. Ebenso kann nun der Konfigurationsstatus korrekt abgelesen werden.

4.23 System - Tracing auf PPP-Schnittstellen

(ID 14607)

Es war nicht möglich Tracing auf allen PPP-Schnittstellen durchzuführen.

Das Problem wurde gelöst.

4.24 DynDNS - Rekursive Schleife

(ID 9899)

Im DynDNS-Mechanismus bildete sich eine Schleife, falls sich die Systemzeit änderte. Dadurch wurde eine große Anzahl an Syslog-Meldungen erzeugt.

Das Problem wurde gelöst.

4.25 Systemtelefonbuch - Anzeigeproblem

(ID 15132)

Falls das Telefonbuch der Anlage ohne Eingrenzung auf einen Anfangsbuchstaben vom Systemtelefon aus aufgerufen wurde, wurde der erste Telefonbucheintrag angezeigt und es war nicht möglich, nach weiteren Einträgen zu suchen.

Das Problem wurde gelöst.

4.26 OSPF - Routen nicht propagiert

(ID 14333)

Die direkten Routen der Schnittstelle "LOCAL" wurden nicht propagiert.

Das Problem wurde gelöst: Diese Funktion kann nun im Setup Tool aktiviert werden. Setzen Sie dazu im Menü **IP** -> **Routing Protocols** -> **OSPF** -> **OSPF Static Settings** den Parameter **Propagate Routes bound on local interfaces** auf *yes*.

4.27 IPSec - Falsche Proposals

(ID 15148)

Ein im Menü **VPN** -> **IPSec** -> **Phase-1-Profile** -> **Neu** erstelltes IKE-Profil wurde in einigen Fällen mit nicht ausgewählten Proposals angelegt.

Das Problem wurde gelöst.

4.28 CAPI - T.30-Fax-Support

(ID 14810)

T.30-Faxe wurden über CAPI nicht registriert und die entsprechenden LEDs funktionierten nicht.

Das Problem wurde gelöst.

4.29 IPSec - Verlust von Phase-2-Heartbeats

(ID 14380)

Phase-2-Heartbeats gingen bei hoher CPU-Last verloren. Dieses Problem war selbstverstärkend, da die Reinitialisierung der Heartbeats die Systemauslastung weiter erhöhte.

Das Problem wurde gelöst.

Kapitel 5 Bekannte Probleme

5.1 UMTS-Sticks Huawei E372 und Huawei E367u-2

(ID 16951)

Ab **Systemsoftware 9.1.1** funktioniert bei den UMTS-Sticks **Huawei E372** und **Huawei E367u-2** kein ISDN-Login, keine PPP-Einwahl und kein SMS-Versand mehr.

5.2 Konifguration von Gigabit-Ethernet

(ID 19990)

Für die Konfiguration eines Gigabit-Ethernet-Anschlusses sollten Sie im Menü **Physikalische Schnittstellen** -> **Ethernet-Ports** -> **Portkonfiguration** immer *Vollständige automatische Aushandlung* wählen.

Sollten Sie die Ethernet-Schnittstellen manuell fest eingestellt haben, kann es nach dem Update auf Systemsoftware 9.1.1 zu Problemen kommen, wenn das Gateway an einen Switch angeschlossen ist, da unter Umständen beide Geräte als Clock Master agieren. Stellen Sie in diesem Fall das Gateway auf autmomatische Aushandlunug um.