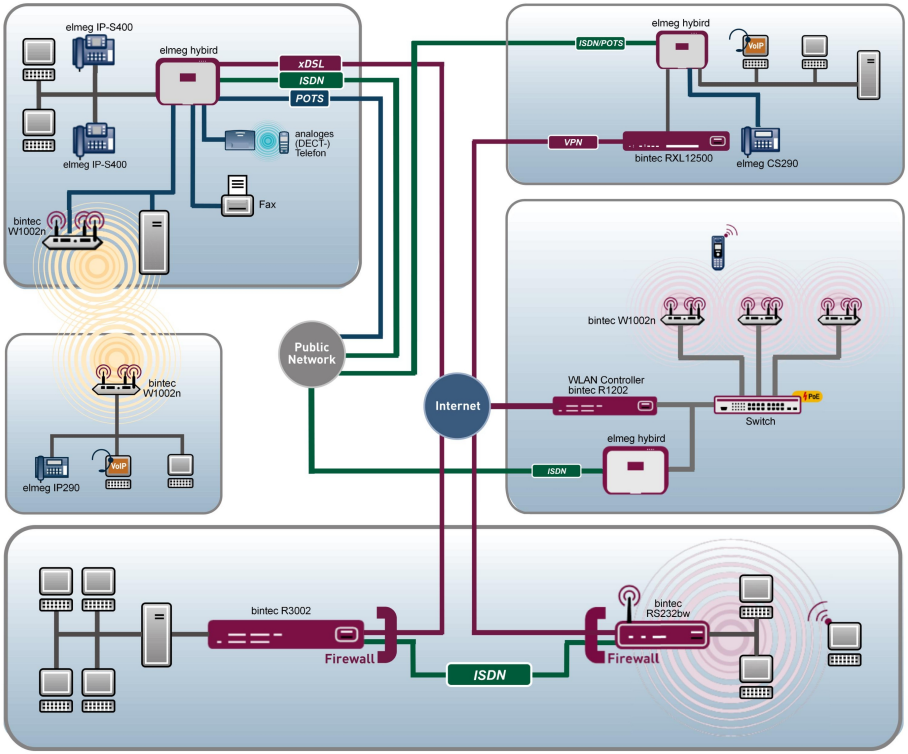

Release Notes

9.1.5

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, 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 9.1.5** vorzubereiten und durchzuführen:

(1) Für das Update benötigen Sie die Datei `XXXXX_bl9105.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 9.1.5** über das Menü **Wartung**->**Software &Konfiguration** durch. Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = *XXXXX_bl9105.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 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** = *RXL_Series_bl9105.biq* (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 9.1.5 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 Hardware: Neuer LED-Modus

Mit **Systemsoftware 9.1.5** können Sie das Leuchtverhalten der LEDs im Menü **Globale Einstellungen** und mit dem **WLAN Controller** in drei verschiedene Betriebsarten schalten.

Hinweis

Wenn Sie das LED-Verhalten über das **GUI** oder den **WLAN Controller** angepasst haben, bleibt diese Einstellung nach einem Wiederherstellen des Auslieferungszustands erhalten.

Status	Nur die Status-LED blinkt einmal in der Sekunde.
Blinkend	Die LEDs zeigen ihr Standardverhalten.
Aus	Alle LEDs sind deaktiviert.

2.2 GUI: Öffentliche Quell-IP-Adresse hinzugefügt

Mit **Systemsoftware 9.1.5** ist im Menü **VPN**->**IPSec**->**IPSec-Peers**->**Neu**->**Erweiterte Einstellungen** der Parameter **Öffentliche Quell-IP-Adresse** verfügbar.

Relevantes Feld im Menü Erweiterte IP-Optionen

Feld	Beschreibung
Öffentliche Quell-IP-Adresse	Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet wer-

Feld	Beschreibung
	den soll. Wählen Sie aus, ob die **Öffentliche Quell-IP-Adresse** aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll. Standardmäßig ist die Funktion nicht aktiv.

2.3 GUI: Parameter Standardeinstellungen wiederherstellen hinzugefügt

Mit **Systemsoftware 9.1.5** ist im Menü **Systemverwaltung**->**Administrativer Zugriff**->**Zugriff**->**Erweiterte Einstellungen** der Parameter **Standardeinstellungen wiederherstellen** verfügbar.

Im Menü **Systemverwaltung**->**Administrativer Zugriff**->**Zugriff**können Sie den Zugriff auf einzelne Schnittstellen einschränken. Jede Änderung in diesem Menü erzeugt Einträge in mehreren MIB-Tabellen. Um die konfigurierten Einschränkungen über das GUI aufheben zu können, wurde der Parameter **Standardeinstellungen wiederherstellen** eingeführt.

Relevantes Feld im Menü Erweiterte Einstellungen

Feld	Beschreibung
Standardeinstellungen wiederherstellen	Erst wenn Sie Änderungen an der Konfiguration des administrativen Zugangs vornehmen, werden entsprechende Zugangsregeln eingerichtet und aktiviert. Mithilfe des Symbols  können Sie die Standardeinstellungen wiederherstellen.

2.4 GUI: Update für die Telefone elmeg IP1x

Mit **Systemsoftware 9.1.5** können Sie mit den Geräten der **elmeg hybird**-Serien über das GUI ein Update auf den angeschlossenen **elmeg IP1x**-Telefonen durchführen.

2.4.1 elmeg IP1x-Aktualisierung

Im Menü **Wartung**->**Systemtelefone**->**elmeg IP1x-Aktualisierung** sehen Sie eine Liste der angeschlossenen **bintec**-IP-Telefone. Sie können Telefone zur sofortigen Aktualisierung der Software auswählen oder es diesen erlauben, sich grundsätzlich neue Software von der Anlage heruntzerzuladen.

Bei einer sofortigen Aktualisierung wird keine Versionskontrolle durchgeführt.

Werte in der Liste elmeg IP1x-Aktualisierung

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung an, die für das Systemtelefon eingetragen ist.
Telefontyp	Zeigt den Typ des Systemtelefons an.
MAC-Adresse	Zeigt die MAC-Adresse des Systemtelefons an.
Version der SD-Karte	Zeigt die Version der gesteckten SD-Karte.
Status/ Aktualisierungsstatus	Zeigt den Status des Systemtelefons bzw. eine Fortschrittsanzeige während eines Aktualisierungsvorgangs an. kennzeichnet ein Systemtelefon, das angeschlossen ist und dessen Systemsoftware von Ihrer **hybird** unterstützt wird. kennzeichnet ein Systemtelefon, das entweder nicht angeschlossen ist oder dessen Systemsoftware nicht von Ihrer **hybird** unterstützt wird. Für IP-Telefone gibt es keine Beschränkung gleichzeitger Aktualisierung der Systemsoftware. Falls die Systemsoftware eines Systemtelefons nicht von Ihrer **hybird** unterstützt wird, können Sie die Systemsoftware trotzdem aktualisieren. Während der Aktualisierung einer Systemsoftware sehen Sie eine Fortschrittsanzeige.
Aktualisierung erlaubt	Zeigt an, ob angschlossene Telefone sich selbstaändig neue Software von der Anlage herunterladen können. Sie können einzelne Einträge über das Kästchen in der jeweili-

Feld	Beschreibung
	gen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** bzw. **Alle deaktivieren** markieren.
Sofort aktualisieren	Zeigt an, ob die Software des Systemtelefons sofort aktualisiert werden soll. Die Funktion wird bei einem einzelnen Gerät durch Setzen eines Hakens aktiviert. Standardmäßig ist die Funktion nicht aktiv. Für alle angezeigten Geräte können Sie die Schaltflächen **Alle auswählen** bzw. **Alle deaktivieren** nutzen.

2.5 IPSec: MobIKE

Mit **Systemsoftware 9.1.5** steht Ihnen die Funktion **MobIKE** zur Verfügung.

Sie finden diese Funktion im Menü **VPN**->**IPSec**->**IPSec-Peers**->**Neu** unter **Erweiterte IP-Optionen**.

Relevantes Feld im Menü Erweiterte IP-Optionen

Feld	Beschreibung
MobIKE	Nur für Peers mit IKEv2. **MobIKE** ermöglicht es, bei wechselnden öffentlichen IP-Adressen lediglich diese Adressen in den SAs zu aktualisieren, ohne die SAs selbst neu aushandeln zu müssen. Standardmäßig ist die Funktion aktiv.

2.6 IPSec: RADIUS Accounting

Wenn RADIUS Accounting konfiguriert ist, wird in Anlehnung an die RFCs 2139, 2866 und 2868 ein ausgewählter Satz von Attributen verwendet, um IPSec Phase-2-Parameter abzubilden.

2.7 WLAN: Airtime Fairness

Mit **Systemsoftware 9.1.5** steht Ihnen die Funktion **Airtime Fairness** zur Verfügung.

Sie finden diese neue Funktion im Menü **Wireless LAN**->**WLAN**->**Einstellungen Funk-**

modul-> und im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Funkmodulprofile**->.

Relevantes Feld im Menü Performance-Einstellungen

Feld	Beschreibung
Airtime Fairness	Diese Funktion ist nicht für alle Geräte verfügbar. Mit der **Airtime Fairness** -Funktion wird gewährleistet, dass Senderessourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.

2.8 WLAN: Client-Lastverteilung

Mit **Systemsoftware 9.1.5** steht Ihnen die Funktion **Client-Lastverteilung** für die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** zur Verfügung.

Die Funktion regelt die Verteilung der Clients eines Funkmoduls auf die konfigurierten Drahtlosnetzwerke sowie die Auslastung der Funkmodule und der Frequenzbänder.

Sie finden diese Funktion im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**-> und im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Drahtlosnetzwerke (VSS)**->.

Relevante Felder im Menü Client-Lastverteilung für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen. Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf die-

Feld	Beschreibung
	sem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis. Mögliche Werte sind ganze Zahlen von *1* bis *254*. Der Standardwert ist *32*.
Max. Anzahl Clients - Soft Limit	Diese Funktion wird nicht von allen Geräten unterstützt. Um eine vollständie Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehnt. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des **Max. Anzahl Clients - Hard Limit** werden Anfragen strikt abgelehnt. Der Wert der **Max. Anzahl Clients - Soft Limit** muss gleich oder kleiner sein als der **Max. Anzahl Clients - Hard Limit**. Der Standardwert ist *28*. Sie können diese Funktion deaktivieren, indem Sie **Max. Anzahl Clients - Soft Limit** und **Max. Anzahl Clients - Hard Limit** auf den gleichen Wert einstellen.
Auswahl des Client-Bands	Diese Funktion wird nicht von allen Geräten unterstützt. Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist. Die Option **Auswahl des Client-Bands** ermöglicht es, Clients von dem urspünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht. Mögliche Werte: • *Deaktiviert, optimiert für Fast Roaming*(Standardwert): Die Funktion wird für dieses VSS

Feld	Beschreibung
	nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • *2,4-GHz-Band bevorzugt*: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • *5-GHz-Band bevorzugt*: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Für das **Client-Lastverteilung** können Sie sich an zwei Stellen im GUI Statistiken ansehen.

2.8.1 Lastverteilung für Wireless LAN Controller

Im Menü **Wireless LAN Controller**->**Monitoring**+**Lastverteilung** wird eine Übersicht der **Lastverteilung** angezeigt. Sie sehen für jedes VSS u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die in vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

2.8.2 Lastverteilung für WLAN

Im Menü**Monitoring**->**WLAN**+**Lastverteilung** wird eine Übersicht der **Lastverteilung** angezeigt. Sie sehen für jedes VSS u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die in vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

Werte in der Liste Lastverteilung

Feld	Beschreibung
VSS-Beschreibung	Zeigt die eindeutige Beschreibung des Drahtlosnetzwerks (VSS) an.
Netzwerkname (SSID)	Zeigt den Namen des Wireless Netzwerks (SSID) an.
MAC-Adresse	Zeigt die MAC Adresse an, die für dieses VSS verwendet wird.
Aktive Clients	Zeigt die Anzahl der aktiven Clients.
2,4/5-GHz-Übergang	Zeigt die Anzahl der Clients, die über die Funktion **2,4/5-GHz-Übergang** in ein anderes Frequenzband verschoben worden sind.
Abgewiesene Clients soft/hard	Zeigt die Anzahl der abgewiesenen Clients, nachdem die absolute Anzahl an zulässigen Clients erreicht wurde.

2.9 WLAN: Stromsparmodus verfügbar

Bei den Geräten **W1003n**, **W2003n**, **W2003n-ext** und **W2004n** steht Ihnen im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**->**Neu** mit dem Parameter **U-APSD** ein Stromsparmodus zur Verfügung.

Relevantes Feld im Menü Service Set Parameter

Feld	Beschreibung
U-APSD	Nur für **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** Wählen Sie aus, ob der Stromsparmodus Unscheduled Automatic Power Save Delivery (U-APSD) aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

2.10 Wireless LAN Controller: Dynamische Black List

Mit **Systemsoftware 9.1.5** steht Ihnen die Funktion **Dynamische Black List** zur Verfügung.

Sie finden diese Funktion im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Drahtlosnetzwerke (VSS)**->**Neu**.

Relevantes Feld im Menü MAC-Filter

Feld	Beschreibung
Dynamische Black List	Mithilfe der Funktion **Dynamische Black List** ist es möglich, Clients, die sich möglicherweise unbefugt Zugriff auf das Netzwerk verschaffen wollen, zu erkennen und für einen bestimmten Zeitraum zu sperren. Ein Client wird dann gesperrt, wenn die Anzahl erfolgloser Anmeldeversuche innerhalb einer definierten Zeit eine bestimmte Anzahl überschreitet. Diese Grenzwerte ebenso wie die Dauer der Sperrung können konfiguriert werden. Ein gesperrter Client wird auf allen vom Wireless LAN Controller verwalteten APs für das betroffene VSS gesperrt, kann sich also auch nicht in einer anderen Funkzelle an diesem VSS anmelden. Soll ein Client permanent gesperrt bleiben, so kann dies im Menü **Wireless LAN Controller**->**Monitoring**+**Rogue Clients** erfolgen.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Im Menü **Wireless LAN Controller**->**Monitoring**+**Rogue Clients** werden die Clients angezeigt, die versucht haben, unbefugten Zugang zum Netzwerk herzustellen und sich daher auf der Blacklist befinden.

Mögliche Werte für Rogue Clients

Status	Bedeutung
MAC-Adresse des Rogue Clients	Zeigt die MAC-Adresse des Clients an, der sich auf der Blacklist befindet.
SSID	Zeigt die beteiligte SSID an.
Angegriffener Access Point	Zeigt den betroffenen AP an.
Signal dBm	Zeigt die Signalstärke des Clients während des Zugriffsversuchs an.
Art des Angriffs	Hier wird die Art des möglichen Angriffs angezeigt, z. B. eine fehlerhafte Authentifizierung.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Zugriffsversuchs an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Zugriffsversuchs an.
Statische Black List	Sie können einen Rogue Client als nicht vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte **Statische Black List** aktivieren. Die Sperrung des Clients endet dann nicht automatisch, sondern muss von Ihnen manuell wieder aufgehoben werden.
Löschen	Mithilfe des -Symbols können Sie Einträge löschen.

2.11 Wireless LAN Controller: Wiederkehrender Hintergrund-Scan

Mit **Systemsoftware 9.1.5** steht Ihnen die Funktion **Wiederkehrender Hintergrund-Scan** zur Verfügung.

Sie finden diese Funktion im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Funkmodulprofile**-> **/ Neu**->**Erweiterte Einstellungen** .

Relevantes Feld im Menü Erweiterte Einstellungen

Feld	Beschreibung
Wiederkehrender Hintergrund-Scan	Diese Funktion wird nicht von allen Geräten unterstützt. Um in regelmäßigen Abständen automatisch nach benachbarten oder Rogue Access Points im Netzwerk zu suchen, können Sie die Funktion **Wiederkehrender Hintergrund-Scan** aktivieren. Diese Suche erfolgt ohne eine Beeinträchtigung der Funktion als Access Point. Aktivieren oder deaktivieren Sie die Funktion **Wiederkehrender Hintergrund-Scan**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

2.12 Wireless LAN Controller: Region

Mit **Systemsoftware 9.1.5** sind im **Wireless LAN Controller** unter **Region** folgende Länder zusätzlich verfügbar: *Argentina*, *Brazil*, *Chile*, *Colombia*, *Costa Rica*, *Equador*, *Guatemala*, *Hunduras*, *Mexico*, *Peru*, *Venezuela*.

2.13 VoIP: Durchsagen

Bei den Geräten der **elmeg hybird** Serien steht Ihnen im Menü **Endgeräte**->**elmeg-Systemtelefone**->**Systemtelefon**->**Tasten**->  unter **Tastentyp** für die Tasten Ihres Systemtelefons die neue Funktion *Durchsage Team* zur Verfügung.

Darüber hinaus können Sie Durchsagen von und zu VoIP-Telefonen nutzen. Die Funktion muss möglicherweise noch im jeweiligen Apparat konfiguriert werden.

2.14 Hotspot: Statusanzeige und Timeout hinzugefügt

Mit **Systemsoftware 9.1.5** sind im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**->**Neu**->**Erweiterte Einstellungen** die Parameter **Pop-Up-Fenster für Statusanzeige** und **Standard-Timeout bei Inaktivität** verfügbar.

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Pop-Up-Fenster für Statusanzeige	Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet. Standardmäßig ist die Funktion aktiv.
Standard-Timeout bei Inaktivität	Aktivieren oder deaktivieren Sie den **Standard-Timeout bei Inaktivität** Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet. Standardmäßig ist die Funktion aktiv. Standardwert ist *600* Sekunden.

2.15 hybird: T.38 FAX Unterstützung

Mit **Systemsoftware 9.1.5** steht Ihnen auf den Geräten **elmeg hybird 120 / 130** die Übertragung eines Faxes mittels T.38 zur Verfügung.

2.16 hybird: Meldeeingang

Die FXS-Schnittstellen können bei den Geräten der **elmeg hybird**-Serien als Meldeeingang konfiguriert werden. So kann z. B. ein Meldeknopf an eine dieser Schnittstellen angeschlossen werden: Wenn der Knopf gedrückt wird, wird ein Melderuf an bis zu acht internen oder eine von zwei externen Rufnummern ausgelöst. Während eines Melderufs kann ggf. einer der Schaltkontakte der **elmeg hybird** aktiviert werden. Optional kann die Funktion **Meldeeingang** über einen Kalender geschaltet bzw. zwischen den beiden möglichen Signalisierungsvarianten umgeschaltet werden.

Bevor Sie mit der Konfiguration der Funktion **Meldeeingang** beginnen, sollten Sie folgende Vorbereitungen treffen:

- Legen Sie im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Neu** einen Benutzer für den Melderuf an und weisen ihm interne und externe Rufnummern zu.
- Legen Sie im Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Neu** eine Berechtigungsklasse für dem Melderuf an.
- Weisen Sie dem Benutzer unter **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->  diese Berechtigungsklasse zu.
- Im Menü **Physikalische Schnittstellen**->**Relais**->**Relaiskonfiguration** können Sie den

Schaltkontakt konfigurieren, den Sie für die Funktion **Meldeeingang** verwenden wollen, um zum Beispiel Notausgänge freizuschalten.

Sie finden die Funktion **Meldeeingang** im Menü **Anwendungen**+**Meldeeingang**+**Meldeeingang**

2.16.1 Meldeeingang

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Meldeeingänge anzulegen.

2.16.1.1 Allgemein

Im Bereich **Allgemein** richten Sie grundlegende Merkmale der Meldeeingänge ein.

Das Menü **Anwendungen Meldeeingang Meldeeingang Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Status	Aktivieren oder deaktivieren Sie die Funktion. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den Melderuf ein.
Schnittstelle	Wählen Sie ggf. die Schnittstelle aus, welche für diesen Melderuf verwendet werden soll.
Interne Rufnummer	Wählen Sie eine interne Rufnummer aus, die für den Melderuf genutzt werden soll.
Variante umschalten	Legen Sie fest, wie der eingerichtete Melderuf geschaltet werden soll. Mögliche Werte: • *Kein Kalender, nur manuell*: Die manuelle Umschaltung wird aktiv. • *<Kalendereintrag>*: Wählen Sie einen der für den Melderuf konfigurierten Kalendereinträge aus.
Aktive Anrufvariante	Wählen Sie die Anrufvariante aus, die aktiv sein soll. Sie kön-

Feld	Beschreibung
	nen die Varianten konfigurieren, sobald Sie die Eingabe im Reiter **Allgemein** mit **OK** bestätigt haben.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Alarm-Signalisierungszeitraum	Geben Sie die Zeit in Sekunden ein, wie lange ein Melderuf signalisiert werden soll. Standardwert ist *30* Sekunden.
Wiederholung nach	Geben Sie die Zeit zwischen den Wiederholungen des Melderufs in Sekunden ein. Möglich ist ein Wert zwischen *1* und *600* Sekunden. Standardwert ist *10* Sekunden. Melderufwiederholungen über eine FXO-Schnittstelle sind nicht möglich.
:Anzahl der Wiederholungen	Geben Sie die Anzahl der Wiederholungen ein, wenn der Melderuf nicht angenommen wird. Möglich ist ein Wert zwischen 1 und 10 Wiederholungen. Standardwert ist *2*. Melderufwiederholungen über eine FXO-Schnittstelle sind nicht möglich.
Externer Verbindungs-Tmer	Geben Sie max. Dauer eines externen Melderuf (in Sekunden ein), nachdem dieser angenommen wurde. Möglich ist ein Wert zwischen *1* und *600* Sekunden. Standardwert ist *60* Sekunden.
Info-Meldung (UUS1)	Optional kann eine Nachricht (max. 32 Zeichen) an ISDN-Endgeräte gesendet werden.
Relaiskontakt	Wenn ein Relais während des Melderufs geschaltet werden soll: Wählen Sie das zu verwendende Relais. Die Konfiguration des Relais erfolgt im Menü **Physikalische Schnittstellen**->**Relais**.

Feld	Beschreibung
Wave-Datei	Wählen Sie aus, ob und welche gespeicherte Wave-Datei bei Annahme des Melderufs gespielt werden soll. Mögliche Werte: • *Aus* (Standardwert): Ein gehaltener Anrufer soll keine Wartemusik hören. • *<Wave-Datei>*: Der gerufene Teilnehmer soll die ausgewählte Wave-Datei hören.
Anzahl der Wiedergaben	Wählen Sie aus, wie oft die Ansage hintereinander abgespielt werden soll. Mögliche Werte: • *Endlos (Standardwert)* • *1* bis *10*

2.16.1.2 Variante 1 und 2

Sie können zwei Varianten des Melderufs konfigurieren. In der Regel wird eine Variante die Möglichkeit nutzen, interne Teilnehmer zu rufen, die andere die Möglichkeit, externe Teilnehmer zu rufen.

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Zuordnung	Sie können jedem Melderuf bis zu acht interne Rufnummern oder zwei externe Rufnummern zuordnen. Legen Sie fest, ob die Anrufe bei einem Melderuf bei den internen Teilnehmern oder bei dem externen Teilnehmer signalisiert werden sollen. Mögliche Werte: • *Extern*: Die eingetragene externe Rufnummer wird gerufen. Bei einem Melderuf können können zwei externe Nummern alternativ angerufen werden. • *Intern* (Standardwert): Die Teilnehmer, die den ausgewählten Rufnummern zugeordnet sind, werden entsprechend der eingestellten Signalisierung gerufen. Bei einem Melderuf können acht interne Teilnehmer gleichzeitig angerufen werden.
Erste Externe Rufnummer	Nur für **Zuordnung** = *Extern*Geben Sie die erste Rufnummer

Feld	Beschreibung
	des externen Teilnehmers ein.
Zweite externe Rufnummer	Nur für **Zuordnung** = *Extern*Geben Sie die zweite Rufnummer des externen Teilnehmers ein.
Interne Zuordnung	Nur für **Zuordnung** = *Intern*Wählen Sie die internen Teilnehmer aus. Fügen Sie mit **Hinzufügen** weitere interne Rufnummern hinzu.

2.17 hybird: Automatische Rufnummernübertragung verfügbar

Mit **Systemsoftware 9.1.5** wird die Rufnummer des Update Servers, die Sie auf den Geräten der `elmeg hybird` Produktlinien im Menü **Wartung**->**Systemtelefone**->**Einstellungen** als **Interne Rufnummer** konfigurieren können, automatisch an das Systemtelefon übertragen, sobald sich das Telefon an der entsprechenden **elmeg hybird** anmeldet.

Nach der Übertragung wird die Nummer am Telefon unter **Menü**->**Service**->**Software Update** angezeigt. Mit dem Drücken der OK-Taste steht die Nummer in der Wahlvorbereitung zur Verfügung.

2.18 hybird: bintec CAPI verfügbar

Mit **Systemsoftware 9.1.5** steht Ihnen auf den Geräten der **elmeg hybird 120 / 130**-Serien **bintec CAPI** zur Verfügung.

2.18.1 CAPI

Im Menü **Endgeräte**->**Andere Telefone**+**CAPI** konfigurieren Sie die angeschlossenen CAPI-Endgeräte. Sie nehmen z. B. die Zuweisung einer konfigurierten internen Rufnummer vor.

2.18.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um eine weiteres CAPI-Endgerät hinzuzufügen.

Das Menü **Endgeräte**->**Andere Telefone**+**CAPI**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das CAPI-Telefon ein.

Felder im Menü Grundlegende Telefoneinstellungen

Feld	Beschreibung
Interne Rufnummern	Mit **Hinzufügen** wählen Sie die internen Rufnummern für dieses Endgerät aus. Sie können mehrere interne Rufnummern definieren. Mögliche Werte: • *Keine freie Leitung verfügbar*: Alle konfigurierten internen Rufnummern sind schon in Verwendung. Konfigurieren Sie zunächst einen weiteren Benutzer mit internen Rufnummern. • *<Interne Rufnummer>* : Wählen Sie eine der vorhandenen Rufnummern der konfigurierten Benutzer aus.

Kapitel 3 Änderungen

Folgende Änderungen sind in **Systemsoftware 9.1.5** vorgenommen worden.

3.1 GUI: Erweiterte Einstellungen anzeigen

Beim erneuten Laden einer Seite bleibt der Zustand des Seitenbereichs **Erweiterte Einstellungen** erhalten, d.h. wenn die Parameter im Bereich **Erweiterte Einstellungen** angezeigt wurden, so werden sie nach einem Reload weiterhin angezeigt und müssen nicht erneut aufgerufen werden.

3.2 GUI: Spalten sortierbar

Im Menü **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung** ist der Inhalt der Spalten ab sofort sortierbar.

3.3 GUI: Automatische Seitenaktualisierung entfernt

Im Menü **Netzwerk**->**Lastverteilung**->**Special Session Handling** wurde die automatische Seitenaktualisierung entfernt, weil auf dieser Seite ausschließlich statische Werte verwendet werden.

3.4 GUI: SSH erweitert

Im Menü **Systemverwaltung**->**Administrativer Zugriff**->**SSH** wurden die Parameter **SSH-Port**, **Maximale Anzahl gleichzeitiger Verbindungen** und **Toleranzzeit beim Login** hinzugefügt. Die Parameter **Komprimierung**, **TCP-Keepalives** und **Protokollierungslevel** wurden in das Menü **Erweiterte Einstellungen** verschoben.

Relevante Felder im Menü SSH-Parameter (Secure Shell)

Feld	Wert
SSH-Port	Hier können Sie den Port eingeben, über den die SSH-Verbindung aufgebaut werden soll. Standardwert ist `22`.
Maximale Anzahl gleichzeitiger Verbin-	Tragen Sie die maximale Anzahl gleichzeitig aktiver SSH-Verbindungen ein.

Feld	Wert
dungen	Standardwert ist *1*.

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Wert
Toleranzzeit beim Login	Geben Sie die Zeit (in Sekunden) ein, die für den Verbindungsaufbau zur Verfügung steht. Wenn ein Client innerhalb dieser Zeit nicht erfolgreich authentifiziert werden kann, wird die Verbindung getrennt. Standardwert ist *600* Sekunden.
Komprimierung	Wählen Sie aus, ob Datenkompression verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-Keepalives	Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Protokollierungslevel	Wählen Sie den Syslog-Level für die vom SSH Daemon generierten Syslog-Messages aus. Zur Verfügung stehen: • *Informationen* (Standardwert): Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet. • *Fatal*: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet. • *Fehler*: Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet. • *Debug*: Es werden alle Meldungen aufgezeichnet.

3.5 Netzwerk: Routen überarbeitet

Das Menü **Netzwerk**->**Routen**->**IPv4-Routen**->**Neu** wurde überarbeitet und erweitert. Das Menü **Netzwerk**->**Routen**+**IPv4-Routing-Tabelle** ist neu.

Sie können jetzt auch Routen für Schnittstellen im DHCP-Client-Betrieb konfigurieren.

3.5.1 IPv4-Routen

Im Menü **Netzwerk**->**Routen**->**IPv4-Routen** wird eine Liste aller konfigurierten Routen angezeigt.

3.5.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Routen anzulegen.

Wird die Option *Erweitert* für die **Routenklasse** ausgewählt, öffnet sich ein weiterer Konfigurationsabschnitt.

Das Menü **Netzwerk**->**Routen**->**IPv4-Routen**->**Neu** besteht aus folgenden Feldern:

Feld im Menü Grundeinstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, welche für diese Route verwendet werden soll.
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte: • *Standardroute über Schnittstelle*: Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Standardroute über Gateway*: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Host-Route über Schnittstelle*: Route zu einem einzelnen Host über eine spezifische Schnittstelle. • *Host-Route via Gateway*: Route zu einem einzelnen Host über ein spezifisches Gateway. • *Netzwerkroute via Schnittstelle* (Standardwert): Route zu einem Netzwerk über eine spezifische Schnittstelle. • *Netzwerkroute via Gateway*: Route zu einem Netzwerk über ein spzifisches Gateway. Nur für Schnittstellen, die im DHCP-Client-Modus betrieben

Feld	Beschreibung
	werden: Auch wenn eine Schnittstelle für den DHCP-Client-Betrieb konfiguriert ist, ist es möglich, Routen für den Datenverkehr über diese Schnittstelle zu konfigurieren. Die vom DHCP-Server erhaltenen Einstellungen werden dann mit den hier konfigurierten gemeinsam in die aktive Routing-Tabelle übernommen. Dadurch ist es z. B. möglich, bei dynamisch wechselnden Gateway-Adressen bestimmte Routen aufrecht zu erhalten oder Routen mit unterschiedlicher Metrik (d. h. unteschiedlicher Priorität) festzulegen. Wenn der DHCP-Server allerdings statische Routen (sog. Classless Static Routes) übermittelt, werden die hier konfigurierten Einstellungen nicht ins Routing übernommen. • *Vorlage für Standardroute per DHCP*: Die Routing-Informationen werden vollständig vom DHCP-Server übernommen. Lediglich erweiterte Parameter können zusätzlich konfiguriert werden. Diese Route bleibt von weiteren für diese Schnittstelle angelegten Routen unverändert und wird parallel mit diesen in die Routing-Tabelle übernommen. • *Vorlage für Host-Route per DHCP*: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Host ergänzt. • *Vorlage für Netzwerkroute per DHCP*: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Netzwerk ergänzt.  **Hinweis** Durch den Ablauf des DHCP Leases oder durch einen Neustart des Geräts werden die Routen, die aus der Kombination von DHCP- und hier vorgenommenen Einstellungen entstehen, zunächst wieder aus dem aktiven Routing gelöscht. Mit einer erneuten DHCP-Konfiguration werden sie dann neu generiert und wieder aktiviert.
Routenklasse	Wählen Sie die Art der **Routenklasse** aus. Mögliche Werte: • *Standard*: Definiert eine Route mit den Standardparametern.

Feld	Beschreibung
	• *Erweitert*: Wählen Sie aus, ob die Route mit erweiterten Parametern definiert werden soll. Ist die Funktion aktiv, wird eine Route mit erweiterten Routing-Parametern wie Quell-Schnittstelle und Quell-IP-Adresse sowie Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und der Status der Geräte-Schnittstelle angelegt.

Felder im Menü Routenparameter

Feld	Beschreibung
Lokale IP-Adresse	Nur für **Routentyp** = *Standardroute über Schnittstelle*, *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle* Geben Sie die IP-Adresse des Hosts ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Ziel-IP-Adresse/Netzmaske	Nur für **Routentyp** *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle* Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein. Bei **Routentyp** = *Netzwerkroute via Schnittstelle* Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.
Gateway-IP-Adresse	Nur für **Routentyp** = *Standardroute über Gateway*, *Host-Route via Gateway* oder *Netzwerkroute via Gateway* Geben Sie die IP-Adresse des Gateways ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von *0* bis *15*. Standardwert ist *1*.

Felder im Menü Erweiterte Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IP-Route ein.

Feld	Beschreibung
Quellschnittstelle	Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen. Standardwert ist *Keine*.
Neue Quell-IP-Adresse/Netzmaske	Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.
Layer 4-Protokoll	Wählen Sie ein Protokoll aus. Mögliche Werte: *ICMP*, *IGMP*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *PIM*, *L2TP*, *Beliebig*. Standardwert ist *Beliebig* .
Quell-Port	Nur für **Layer 4-Protokoll** = *TCP* oder *UDP* Geben Sie den Quellport an. Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte: • *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.

Feld	Beschreibung
Zielport	Nur für **Layer 4-Protokoll** = *TCP* oder *UDP* Geben Sie den Zielport an. Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte: • *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.
DSCP-/TOS-Wert	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der

Feld	Beschreibung
	IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F. Geben Sie für *DSCP-Binärwert*, *DSCP-Dezimalwert*, *DSCP-Hexadezimalwert*, *TOS-Binärwert*, *TOS-Dezimalwert* und *TOS-Hexadezimalwert* den entsprechenden Wert ein.
Modus	Wählen Sie aus, wann die in **Routenparameter**->**Schnittstelle** definierte Schnittstelle benutzt werden soll. Mögliche Werte: • *Wählen und warten* (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. • *Verbindlich*: Die Route ist immer benutzbar. • *Wählen und fortfahren*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist. • *Nie einwählen*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. • *Immer wählen*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

3.5.2 IPv4-Routing-Tabelle

Im Menü **Netzwerk**->**Routen**+**IPv4-Routing-Tabelle** wird eine Liste aller IPv4-Routen angezeigt. Die Routen müssen nicht alle aktiv sein, können aber durch entsprechenden Datenverkehr jederzeit aktiveirt werden.

Felder im Menü IPv4-Routing-Tabelle

Feld	Beschreibung
Ziel-IP-Adresse	Zeigt die IP-Adresse des Ziel-Hosts bzw. Zielnetzes an.
Netzmaske	Zeigt die Netzmaske des Ziel-Hosts bzw. Zielnetzes an.
Gateway	Zeigt die Gateway IP-Adresse an. Im Falle von per DHCP erhaltenen Routen wird hier nichts angezeigt.
Schnittstelle	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
Metrik	Zeigt die Priorität der Route an. Je niedriger der Wert, desto höhere Priorität besitzt die Route.
Routentyp	Zeigt den Routentyp an.
Erweiterte Route	Zeigt an, ob eine Route mit erweiterten Parametern konfiguriert worden ist.
Löschen	Mithilfe des -Symbols können Sie Einträge löschen.

3.6 DHCP: Pool-Konfiguration geändert

Die Konfiguration von DHCP-Pools im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP Pool** wurde in die beiden Menüs **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration** und **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** aufgeteilt.

Unter **Lokale Dienste**->**DHCP-Server**->**DHCP Pool** werden systemübergreifend alle IP-Pools angezeigt, auch solche, die in anderen Menüs konfiguriert wurden.

Im Folgenden sind die beiden neuen Menüs vollständig beschrieben.

3.6.1 IP-Pool-Konfiguration

Im Menü **Lokale Dienste**->**DHCP-Server**+**IP-Pool-Konfiguration** wird eine Liste aller konfigurierten IP-Pools angezeigt. Diese Liste ist global und zeigt auch die in anderen Menüs konfigurerte Pools an.

3.6.1.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adress-Pools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

3.6.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste**->**DHCP-Server**+**DHCP-Konfiguration** wird eine Liste aller konfigurierten IP-Adress-Pools angezeigt.

In dieser Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. zu deaktivieren.

Hinweis

Im Auslieferungszustand ist der DHCP-Pool mit den IP-Adressen 192.168.0.10 bis 192.168.0.49 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

3.6.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adress-Pools einzurichten. Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

Das Menü **Lokale Dienste**->**DHCP-Server**+**DHCP-Konfiguration**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, über welche die in **IP-**

Feld	Beschreibung
	Adressbereich definierten Adressen an anfragende DHCP-Clients vergeben werden. Wenn eine DHCP-Anfrage über diese **Schnittstelle** eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
Pool-Verwendung	Wählen Sie aus, ob der IP-Pool für DHCP-Anfragen im gleichen Subnetz verwendet werden soll oder für DHCP-Anfragen, die aus einem anderen Subnetz zu Ihrem Gerät weitergeleitet wurden. In diesem Fall ist es möglich, IP-Adressen aus einem anderen Netz zu definieren. Mögliche Werte: • *Lokal* (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet. • *Relais*: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetz verwendet. • *Lokal/Relais*: Der DHCP-Pool wird für DHCP-Anfragen im selben Subnetz und aus anderen Subnetzen verwendet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Gateway	Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll. Mögliche Werte: • *Router als Gateway verwenden* (Standardwert): Hier wird die für die **Schnittstelle** definierte IP-Adresse übertragen. • *Kein Gateway*: Hier wird keine IP-Adresse übermittelt. • *Angeben*: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll. Nachdem **Lease Time** abgelaufen ist, kann die Adresse durch

Feld	Beschreibung
	den Server neu vergeben werden. Standardwert ist *120*.
DHCP-Optionen	Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen. Mögliche Werte für **Option**: • *Zeitserver* (Standardwert): Geben Sie die IP-Adresse des Zeitservers ein, die dem Client übermittelt werden soll. • *DNS-Server*: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • *DNS-Domänenname*: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • *WINS/NBNS-Server*: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • *WINS/NBT Node Type*: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • *TFTP-Server*: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • *CAPWAP Controller*: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • *URL (Provisionierungsserver)*: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. Verwenden Sie diese Option, um anfragenden **IP1x0**-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form *http://<IP-Adresse des Provisionierungsservers>/eg_prov* haben. • *Herstellergruppe* (Vendor Specific Information): Mit dieser Option können Sie dem Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen übermittlen. Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche **Hinzufügen** ein.

Bearbeiten

Im Menü **Lokale Dienste** -> **DHCP-Server** +**DHCP-Konfiguration**->**Erweiterte Einstel-**

lungen können Sie einen Eintrag im Feld **DHCP-Optionen** bearbeiten, wenn **Option** = *Herstellergruppe* gewählt ist.

Wählen Sie das Symbol , um einen vorhandenen Eintrag zu bearbeiten. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server für bestimmte Telefone.

Felder im Menü Basisparameter

Feld	Beschreibung
Hersteller auswählen	Dieser Parameter wird von Ihrem Gerät aktuell nicht verwendet. Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen. Mögliche Werte: • *Siemens* (Standardwert) • *Sonstige*
Provisioning-Server (code 3)	Dieser Parameter wird von Ihrem Gerät aktuell nicht verwendet. Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll. Für die Einstellung **Hersteller auswählen** = *Siemens* wird der Standardwert *sdlp* angezeigt. Sie können die IP-Adresse des gewünschten Servers ergänzen.

3.7 NAT/SIF: Standard-Anzahl von Sessions geändert

Die Standardeinstellung für die Anzahl verfügbarer NAT bzw. SIF Sessions wurde abhängig vom jeweiligen Gerät geändert.

Die Einstellungen sind wie folgt:

Produkt	Anzahl der NAT Sessions	Anzahl der SIF Sessions
bintec RXL-Serie	16000	16000
bintec R(T)-Serie	8000	8000
Andere bintec-Geräte	4000	4000

3.8 X.25-über-ISDN: Einträge in der MIB-Tabelle biboDialTable modifiziert

Bei X.25 über ISDN muss für den ISDN-Verbindungsaufbau eine Rufnummer angegeben werden, über die der X.25 Server erreicht werden kann. Sie können die Rufnummer entweder mit Hilfe einer Regel mit der MIB-Variable **x25RTDstLinkAddrRule** erzeugen oder Sie können die entsprechenden Einträge der MIB-Tabelle **biboDialTable** dafür nutzen.

Bisher konnten die Einträge der **biboDialTable** für ausgehende Rufe auf X25-über-ISDN-Schnittstellen nur dann genutzt werden, wenn die Rufnummer nicht über die obige Regel erzeugt wurde.

Ab **Systemsoftware 9.1.5** werden die Einträge der**biboDialTable** auch dann benutzt, wenn die ISDN-Rufnummer über die **x25RTDstLinkAddrRule** erzeugt wurde, sofern die MIB-Variable **biboDialNumber** leer oder "*" ist.

Nach wie vor wird eine bereits geänderte Rufnummer durch den Eintrag in der **biboDialTable** nicht überschrieben.

Durch die vorliegende Änderung können z. B. Einträge in der **biboDialTable** mit verschiedenen Stack-Masken verwendet werden.

3.9 UMTS: Stick TP-Link MA-180

Beim UMTS Stick TP-Link MA-180 wird ab sofort der AT-Befehl `AT+CRSM` unterstützt.

3.10 UMTS: ISDN-Login-Unterstützung

Ein ISDN-Login ist nun auch bei LTE-Verbindungen möglich. Beim Sierra Wireless MC7710 wird die Systemsoftwareversion 3.5.19.4 benötigt.

3.11 UMTS: Systemmeldungen per SMS

Mit **Systemsoftware 9.1.5** sind Systemmeldungen per SMS für QMI/LTE- Modems verfügbar.

3.12 UMTS: Closed User Groups

Sie können sich jetzt über LTE-Verbindungen in geschlossene Benutzergruppen einwählen und authentifizieren.

3.13 Systemtelefone: Einrichten der Umschalttaste geändert

Für die Systemtelefone **elmeg S530** und **elmeg S560** konnten Sie bisher auf jeder Funktionstaste in beiden Ebenen je eine Umschalttaste (Shift-Taste) über das GUI einer **elmeg hybird** einrichten.

Wenn eine Umschalttaste auf der ersten Ebene eingerichtet war, so wurde auf der zweiten Ebene im GUI "keine Funktion" angezeigt. Wenn auf dieser Taste in der zweiten Ebene eine andere Funktionstaste eingerichtet wurde, so funktionierte diese nur fehlerhaft, sofern es sich um eine Funktionstaste mit LED-Anzeige handelte.

Ab sofort wird die Umschalttasten-Funktion der ersten Ebene gelöscht, wenn auf der entsprechenden Taste in der zweiten Ebene eine andere Funktion eingerichtet wird.

Auf der zweiten Ebene konnten Sie ebenfalls eine Umschalttaste einrichten. Diese Einrichtungsvariante wurde aus der Software entfernt.

3.14 MIB: SNMP Discovery geändert

Die SNMP-Discovery-Funktion können Sie jetzt in der MIB-Tabelle **snmpAdmin** mit der MIB-Variablen *McDiscovery* aus- und einschalten. Standardmäßig ist sie eingeschaltet.

Kapitel 4 Behobene Fehler

Hinweis

Beachten Sie, dass die im Folgenden 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 9.1.5** behoben worden:

4.1 Probleme mit neuen Browserversionen

(ID 17542, 17578, 17698, 17759)

Bei Verwendung der neuesten Versionen der Browser Chrome, Internet Explorer oder Safari gab es Probleme mit dem Dateityp. Die Probleme traten zum Beispiel auf, wenn in einer Liste ein Eintrag ausgewählt werden sollte. Es konnte vorkommen, dass die gewünschte Auswahl grau dargestellt und nicht wählbar war oder dass der erwartete Eintrag nicht angezeigt wurde.

Das Problem wurde gelöst.

4.2 Speicherproblem mit Absturz

(ID 17573)

Es konnte in seltenen Fällen vorkommen, dass bei **bintec RXL12500** in Zusammenarbeit mit einem Gerät eines anderen Herstellers umfangreicher Speicherverbrauch gefolgt von einem Absturz auftrat.

Das Problem wurde gelöst.

4.3 Ethernet: Port-Separation nicht wirksam

ID 17877

Beim Start des Geräts konnte es dazu kommen, dass die Auftrennung der Ethernet-Schnittstellen nicht schnell genug aktiviert wurde und der Switch kurzfristig alle Ports zusammenfasste. Dies konnte in ungünstigen Fällen z. B. zu nicht funktionstüchtigen WAN-Verbindungen führen.

Das Problem wurde gelöst.

4.4 USB: Probleme mit T-Mobile Speedstick LTE II

(ID 17685)

Der von der Deutschen Telekom neu eingeführte T-Mobile Speedstick LTE II wurde von Geräten der RS-Serie nicht erkannt.

Das Problem wurde gelöst.

4.5 USB: Probleme mit UMTS Stick HUAWEI E352s-5

(ID 17518)

Der UMTS Stick HUAWEI E352s-5 wurde von Geräten der RS-Serie nicht erkannt.

Das Problem wurde gelöst.

4.6 System: Gerät in Endlosschleife

(ID n/a)

Wenn eine A-MPDU (Aggregated MAC Protocol Data Unit) an Ihr Gerät gesendet wurde und einer ihrer Frames fehlerhaft war, konnte es vorkommen, dass das Gerät in eine Endlosschleife geriet und dadurch blockiert wurde.

Das Problem wurde gelöst.

4.7 LAN: Anlegen einer virtuellen Schnittstelle misslang

(ID 17598, 17622)

Wenn im Menü **LAN**->**IP-Konfiguration**->**Neu** bereits mehrere virtuelle Schnittstellen angelegt waren, konnte keine weitere virtuelle Schnittstelle angelegt werden.

Das Problem wurde gelöst.

4.8 LAN: Identische MAC-Adresse für verschiedene Geräte

(ID 17645)

Wenn im Menü **LAN**->**IP-Konfiguration** unter **en1-4**  gewählt war, **Adressmodus** = *DHCP* gesetzt war und unter **MAC-Adresse** die Einstellung **Voreingestellte verwenden** und unter **Erweiterte Einstellungen** unter **DHCP-MAC-Adresse** ebenfalls **Voreingestellte verwenden** aktiviert war und diese Einstellungen mit **OK** gespeichert waren, so wurde in der MIB-Tabelle **ipDhcpClientTable** in der MIB-Variablen **PhysAddress** ein fester Wert gespeichert. Für jedes Gerät wurde bei identischer Konfiguration ein identischer Wert für **PhysAddress**, d.h. dieselbe MAC-Adresse, gespeichert.

Das Problem wurde gelöst.

4.9 LAN: Panic and Stacktrace

(ID 17672)

Wenn *en1-0* eine IP-Adresse zugewiesen war und Switch Port 5 *en1-0* zugeordnet war, diese Konfiguration als Boot-Konfiguraton gespeichert war, in Port ETH 5 ein LAN-Kabel eingesteckt war, LAN-Datenverkehr an den Router geschickt wurde und ein Reboot auf dem Gerät durchgeführt wurde, so wurde eine Panic mit Stacktrace und ein Reboot ausgelöst.

Das Problem wurde gelöst.

4.10 PPP: Übermittlung von Name-Server-Adressen funktionierte nicht

(ID 17689)

Es konnte vorkommen, dass die Übermittlung von Name-Server-Adressen mit Hilfe von IP-CP nicht funktionierte..

Das Problem wurde gelöst.

4.11 ISDN: Falsches Format für Rufnummer

(ID 17757)

Im Menü **WAN**->**Internet + Einwählen**->**ISDN**->**Neu**->**Erweiterte Einstellungen** konnten im Abschnitt **Wahlnummern** unter **Einträge** mit **Hinzufügen** im Feld **Rufnummer** beliebige Zeichen eingegeben werden.

Das Problem wurde gelöst.

4.12 DNS/NAT: Gelöschte DNS-Einträge

(ID 17355)

Wenn im Menü **Netzwerk**->**NAT**->**NAT-Konfiguration** ->**Neu** ein Eintrag angelegt und mit **OK** gespeichert wurde sowie danach wieder gelöscht wurde, so wurde im Menü **Lokale Dienste**->**DSN**->**DNS-Server** der DNS-Server-Eintrag der entsprechenden Schnittstelle ebenfalls gelöscht.

Das Problem wurde gelöst.

4.13 Hadware-Verschlüsselung: Panic

ID 17593

Bei hardware-verschlüsselten PPP-Verbindungen konnte es zu einer Panic kommen.

Das Problem wurde gelöst.

4.14 IPSec: Zertifikate fehlerhaft angezeigt

(ID 17565)

Bei Verwendung mehrerer CA-Zertifikate wurde im Menü **VPN**->**IPSec**->**Phase-1-Profile**->**Neu**->**Erweiterte Einstellungen** nur das erste Zertifikat angezeigt.

Das Problem wurde gelöst.

4.15 IPSec: Proposals fehlerhaft angezeigt

(ID 17715)

Im Menü **VPN**->**IPSec**->**Phase-1-Profile** und im Menü **VPN**->**IPSec**->**Phase-2-Profile** wurde jeweils in der Spalte **Proposals** ein falscher Wert angezeigt,

Wenn zum Beispiel als **Verschlüsselung** *AES-128* und als **Authentifizierung** *SHA1* gewählt war, wurde *[AES/SHA1]* angezeigt, d.h. die Anzeige der Verschlüsselung wurde nach drei Zeichen abgeschnitten. Dasselbe Problem trat mit *AES-192* und *AES-256* auf.

Das Problem wurde gelöst.

4.16 Netzwerk: Falscher Wert für Special Session Handling

(ID 17483)

Wenn im Menü **Netzwerk**->**Lastverteilung**->**Special Session Handling**->**Neu** z. B. **Dienst** = *http (SSL)* gewählt wurde und die Einstellung mit **OK** gespeichert wurde, so wurde in der MIB-Tabelle **ipLoadBExtHandlingTable** die MIB-Variable **SrcIfIndex** = *0* gesetzt statt **SrcIfIndex** = *-1*.

Das Problem wurde gelöst.

4.17 CAPI: Falsche Anzeige im Remote CAPI Client

(ID 17591)

In der **Remote Multi CAPI Client Konfiguration** wurden im Bereich **Information über Leistungsmerkmale** fälschlicherweise auch Modem-Leistungsmerkmale angezeigt.

Das Problem wurde gelöst.

4.18 WLAN: Sporadische Panic

(ID 17262)

Im Menü **Wireless LAN**->**Verwaltung** wurde im Dropdown-Menü **Region** der Eintrag *Invalid Reference* angezeigt. Mehrmaliges Öffnen dieses Menüs konnte eine Panic auslösen.

Das Problem wurde gelöst.

4.19 WLAN: Falsche Anzeige

(ID 17353)

Bei Geräten mit zwei Funkmodulen wurde bei Konfiguration des 5GHz-Bandes im Dropdown-Menü **Frequenzband** der Wert *Invalid Reference* angezeigt.

Das Problem wurde gelöst.

4.20 WLAN: WDS-Links irrtümlich angezeigt

(ID 17292)

Bei den Geräten **bintec W1003n**, **W2003n**, **W2003n-ext** und **W2004n** wurden die Menüs **Wireless LAN**->**WLAN**->**WDS-Links** und **Monitoring**->**WLAN**->**WDS** angezeigt, obwohl bei diesen Geräten aktuell keine WDS-Links verfügbar sind.

Das Problem wurde gelöst.

4.21 WLAN: TKIP nicht verfügbar

(ID 17522)

Bei den Geräten **bintec W1003n**, **W2003n**, **W2003n-ext** und **W2004n** war in den Menüs **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)** und **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Drahtlosnetzwerke**->  für die Parameter **WPA Cipher** und **WPA2 Cipher** die Einstellung *TKIP* nicht verfügbar.

Das Problem wurde gelöst.

4.22 WLAN: Drahtlosnetzwerk (VSS) unbeabsichtigt gelöscht

(ID 17510)

Wenn im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)** unter **Erlaubte Adressen** Adressen eingetragen waren und davon eine Adresse gelöscht wurde, so wurde das gesamte Drahtlosnetzwerk gelöscht.

Das Problem wurde gelöst.

4.23 WLAN: Scanabbruch fehlerhaft

(ID n/a)

Wenn während eines Scans das WLAN ausgeschaltet wurde, so verblieb das System im Scanning-Modus.

Das Problem wurde gelöst.

4.24 WLAN: Panic bei automatischer Kanalauswahl

(ID n/a)

Wenn ein Drahtlosnetzwerk (VSS) während der automatischen Kanalauswahl deaktiviert wurde, kam es zu einer Panic des Geräts.

Das Problem wurde gelöst.

4.25 WLAN: DFS Typ 4 nicht funktionsfähig

(ID n/a)

Radarerkennung für Kanäle konnte nicht verwendet werden, da DFS (Dynamic Frequency Selection) Typ 4 nicht funktionierte.

Das Problem wurde gelöst.

4.26 WLAN: Land nicht änderbar

(ID n/a)

Bei Verwendung bestimmter Module konnte die Ländereinstellung nicht geändert werden.

Das Problem wurde gelöst.

4.27 WLAN: Maximale Sendeleistung falsch

(ID n/a)

Beim Festlegen der maximalen Sendeleistung wurde unter anderem die Antennenverstärkung nicht berücksichtigt

Das Problem wurde gelöst.

4.28 WLAN: Probleme mit unverschlüsselter Kommunikation

(ID 17168)

Es konnte vorkommen, dass bei unverschlüsselter Kommunikation zwischen 802.11n-fähigen bintec WLAN-Geräten und bintec WLAN-Geräten, die mit anderen Standards arbeiteten, Probleme auftraten.

Die Probleme wurden gelöst.

4.29 Wireless LAN Controller Wizard: Problem bei Initialisierung der Access Points

(ID 17658)

Bei Verwendung des Wireless LAN Controller Wizards konte es vorkommen, dass die Initialisierung des ersten gefundenen Access Points in einer Liste von mehreren gefundenen Access Points mit der Debug-Meldung "WTP is offline (unexpected restart detected)" misslang und der Wizard in einer Endlosschleife versuchte, diesen Access Point zu initialisieren.

Das Problem wurde gelöst.

4.30 Wireless LAN Controller: Kanalanzeige fehlerhaft

(ID 17659)

Wenn Sie im Wireless LAN Controller mehere Access Points konfiguriert hatten, wurde im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Slave Access Points** in der Spalte **Kanal** jeweils *0* angezeigt.

Das Problem wurde gelöst.

4.31 Wireless LAN Controller: Stacktrace

(ID n/a)

Bei Nutzung des Wireless LAN Controllers konnte es vorkommen, dass eine Panic gefolgt von einem Stacktrace auftrat.

Das Problem wurde gelöst.

4.32 Wireless LAN Controller: Probleme mit Remote Access Points

(ID 17727)

Wenn über einen Wireless LAN Controller sowohl lokale als auch entfernte Access Points gesteuert wurden, konnte es zu Problemen mit den entfernten APs kommen (z. B. bei Verwendung einer Firewall oder einer VPN-Verbindung), weil der Wireless LAN Controller für das Senden der Antwortpakete auf die CAPWAP Requests der APs eine falsche IP-Adresse / einen falschen Port verwendete.

Das Problem wurde gelöst.

4.33 Wireless LAN Controller: CAPWAP Daemon

(ID 17657)

Es konnte vorkommen, dass nach dem Start des Wireless LAN Controller Wizards der CAPWAP Daemon eine CPU-Last von 99 % verursachte und der Wireless LAN Controller blockiert war.

Das Problem wurde gelöst.

4.34 Wireless LAN Controller: Inaktive Einträge nicht löschbar

ID 17844

Es konnte vorkommen, dass inaktive Einträge für Slave Access Points im WLAN Controller nicht gelöscht werden konnten.

Das Problem wurde gelöst.

4.35 Wireless LAN Controller: Spatial Streams

ID 17867

Bei der Konfiguration der Radioprofile war es nicht möglich, ein Profil mit der Nutzung von drei Spatial Streams zu erstellen. Diese werden aber von **W2004n** unterstützt.

Das Problem wurde gelöst.

4.36 VoIP: Systemabsturz

(ID n/a)

Es konnte vorkommen, dass die erste VoIP-Verbindung einen Systemabsturz verursachte.

Das Problem wurde gelöst.

4.37 VoIP: Gestörte Verbindung

(ID 17729)

Eine falsche Codec-Auswahl bei IP-Systemtelefonen zerstörte die Audio-Verbindung. Es waren ausschließlich Störgeräusche zu hören.

Das Problem wurde gelöst.

4.38 VoIP: Syslog-Meldung angezeigt

(ID 17782)

Wenn bei einem Gerät der **bintec RS-Serie** im Menü **VoIP**->**SIP** ein **SIP-Proxy** konfiguriert wurde, wurde auf dem **Level** *Debug* für das **Subsystem** *Configuration* die Syslog-Meldung " NCI: outputErrorVals errorId INT_0_65535 not defined" angezeigt.

Das Problem wurde gelöst.

4.39 VoIP: IP-Telefon IP1x0 nicht funktionsfähig

(ID n/a)

Wenn vier MSNs über ein Gerät der **hybird**-Serien an vier **IP1x0**-Telefone vergeben wurden, eine fünfte (oder weitere) MSN an einem Telefon direkt vergeben wurde, so wurde

dieses Telefon durch die Provisionierung mittels **hybird** lahmgelegt, d.h. der Provisionierungsvorgang startete alle 30 Sekunden, sodass das Telefon nicht mehr verwendet werden konnte.

Das Problem wurde gelöst.

4.40 VoIP: Probleme mit Audio-Verbindung

(ID n/a)

Bei VoIP-Verbindungen konnte es vorkommen, dass die Audio-Verbindung nur in einer Richtung oder gar nicht funktionierte.

Das Problem wurde gelöst.

4.41 VoIP: FAX-Probleme

(ID 17594)

Bei AudioCodes DSP-Modulen konnten Probleme bei einem eingehenden Fax auftreten.

Das Problem wurde gelöst.

4.42 VoIP: Audio-Verbindungen nicht funktionsfähig

(ID 17762)

Bei den Geräten **elmeg hybird 120 / hybird 130** konnte es vorkommen, dass die Audio-Verbindungen nicht funktionierten.

Das Problem wurde gelöst.

4.43 VoIP: Falsche Meldung bei SIP-Verbindungen

(ID 17707)

Wenn bei SIP-SIP-Verbindungen die verwendeten Codecs nicht zusammenpassten, wurde bei den Geräten der **hybird**-Serien die irritierende Fehlermeldung "Bandwith limitation reached. Call rejected!" angezeigt.

Das Problem wurde gelöst.

4.44 hybird: Wartemusik nicht verfügbar

(ID n/a)

Wenn die Wartemusik (Music on hold, MoH) ein zweites Mal abgerufen wurde, funktionierte sie nicht mehr.

Das Problem wurde gelöst.

4.45 hybird: Zeicheninterpretation fehlerhaft

(ID 17734)

In Geräten der **elmeg hybird**-Serien konnte es zu Fehlinterpretationen von Zeichen kommen und in der Folge davon zu einer fehlerhaften Anzeige dieser Zeichen auf angeschlossenen Systemtelefonen **elmeg S560** / **elmeg S530**.

Das Problem wurde gelöst.

4.46 hybird: Undefinierter Zustand

(ID 17702)

Bei Geräten der **elmeg hybird**-Serien konnte es vorkommen, dass sie unter Last in einen undefinierten Zustand gerieten..

Das Problem wurde gelöst.

4.47 hybird: Schnittstellen nicht nutzbar

ID 17899

Bei Ausstattung einer modularen elmeg hybird mit einer großen Anzahl von ISDN-Schnittstellen konnten nicht alle Schnittstellen genutzt werden.

Das Problem wurde gelöst.

Kapitel 5 Bekannte Probleme

5.1 WLAN Controller - Konfiguration der Radiomodule

Wenn über den WLAN Controller den Geräten **W2003n** bzw. **W2004n** Funkmodulprofile zugewiesen werden, muss dem WLAN-Modul 1 ein Profil für das 2,4-GHz-Band zugewiesen werden, dem WLAN-Modul 2 eines für das 5-GHz-Band. Bei einer anderen Zuordnung der Funkbänder zu den Modulen bleiben die Module nach dem Laden der Konfiguration vom WLAN Controller inaktiv.