

Benutzerhandbuch Release Notes

7.10.5

Copyright© Version 1.0, 2012 Teldat GmbH

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

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Teldat GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Teldat GmbH nicht gestattet.

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
1.1	Vorbereitung und Update mit dem FCI	1
1.2	Downgrade mit dem FCI	2
Kapitel 2	Neue Funktionen	3
2.1	Drop In	3
2.1.1	Drop-In-Gruppen	3
2.2	Special Session Handling	5
2.2.1	Special Session Handling	5
2.3	Schnittstellenbasiertes DNS-Serverkonzept	9
2.3.1	DNS-Server	9
2.4	Lastverteilung - Parameter Routenselektor und IP-Adresse zur Nachverfolgung hinzugefügt	11
2.5	IPSec over TCP	12
2.6	Wireless LAN Controller - Parameter Standort des Slave-AP hinzugefügt	12
Kapitel 3	Änderungen	13
3.1	FCI - DNS-Serverkonfiguration - geändert	13
3.2	FCI - Überwachung - Hosts geändert	13
3.3	UMTS Stick Vodafone K3806 unterstützt.	14
Kapitel 4	Behobene Fehler	15
4.1	WLAN Controller - Gefundene APs nicht gelöscht	15
4.2	RADIUS - Panic und Neustart	15
4.3	Routing - Probleme mit Erweiterter Route	15

4.4	Keepalive Monitoring - Einträge fälschlicherweise gelöscht	16
4.5	QoS - Einträge nicht korrekt angezeigt.	16
4.6	QoS - Überflüssige Meldung angezeigt	16
4.7	WLAN Controller - Falsche Kanäle verwendet	16
4.8	IPSec - Falscher Wert gespeichert	17
4.9	ISDN - Skriptfehler mit Service Tool	17
4.10	IPSec - Einrichten eines Peers fehlgeschlagen	17
4.11	Filter - Anlegen eines neuen Filters fehlgeschlagen	18
4.12	IPSec - Fehlermeldungen angezeigt.	18
4.13	ISDN - Fehlermeldung während des Bootvorgangs	18
4.14	Scheduler - Keine Aktion	18
4.15	GUI - Änderung nicht korrekt ausgeführt	19
Kapitel 5	Bekannte Probleme.	20
5.1	HTML-Konfiguration - Routenselektor nicht korrekt konfiguriert	20
5.2	Drop In - DHCP Relay	20
5.3	Setup Tool - IP-Addressänderung nicht aktiviert	20

Kapitel 1 Wichtige Informationen

1.1 Vorbereitung und Update mit dem FCI

Das Update der Systemsoftware mit dem Graphic Configuration 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 Graphic Configuration Interface ein Update auf **Systemsoftware 7.10.5** vorzubereiten und durchzuführen:

- (1) Für das Update benötigen Sie die Datei `XXXXX_b171005.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 Graphic Configuration 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 7.10.5 über das Menü **Wartung->Software & Konfiguration** durch. Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = `XXXXX_b171005.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. Success. 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 FCI

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. Success. 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_b171001.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. Success. 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 7.10.5 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 Drop In

Ab **Systemsoftware 7.10.5** ist das neue Menü **Netzwerk->Drop In** verfügbar.

Mit dem Drop-In-Modus können Sie ein Netzwerk in mehrere Segmente aufteilen, ohne das IP-Netzwerk in Subnetze teilen zu müssen. Dazu können mehrere Schnittstellen in einer Drop-In-Gruppe zusammengefasst und einem Netzwerk zugeordnet werden. Alle Schnittstellen sind dann mit der gleichen IP-Adresse konfiguriert.

Die Netzwerkkomponenten eines Segments, die an einem Anschluss angeschlossen sind, können dann gemeinsam z. B. mit einer Firewall geschützt werden. Der Datenverkehr von Netzwerkkomponenten zwischen einzelnen Segmenten, die unterschiedlichen Ports zugeordnet sind, wird dann entsprechend der konfigurierten Firewall-Regeln kontrolliert.

2.1.1 Drop-In-Gruppen

Im Menü **Netzwerk->Drop In->Drop-In-Gruppen** wird eine Liste aller **Drop-In-Gruppen** angezeigt. Eine **Drop In**-Gruppe repräsentiert jeweils ein Netzwerk.

2.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere **Drop-In-Gruppen** einzurichten.

Das Menü **Netzwerk->Drop In->Drop-In-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine eindeutige Bezeichnung für die Drop In -Gruppe ein.
Modus	<p>Wählen Sie, welcher Modus für die Übermittlung der MAC-Adressen von Netzwerkkomponenten verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Transparent</i> (Standardwert): ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet. • <i>Proxy</i>: ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden mit der MAC-Adresse der entsprechenden Schnittstelle weitergeleitet.
Netzwerkconfiguration	<p>Wählen Sie aus, auf welche Weise den Netzwerkkomponenten eine IP-Adresse zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert) • <i>DHCP</i>
Netzwerkadresse	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die Netzwerkadresse des Drop In-Netzwerks ein.</p>
Netzmaske	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die zugehörige Netzmaske ein.</p>
Lokale IP-Adresse	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die lokale IP-Adresse ein. Diese IP-Adresse muss für alle Ethernet-Ports eines Netzwerks identisch sein.</p>
DHCP Client an Schnittstelle	<p>Nur für Netzwerkconfiguration = <i>DHCP</i>.</p> <p>Hier können Sie eine Ethernet-Schnittstelle Ihres Routers wählen, die als DHCP-Client agieren soll.</p> <p>Diese Einstellung benötigen Sie zum Beispiel, wenn der Router Ihres Providers als DHCP-Server dient.</p>

Feld	Beschreibung
	<p>Sie können unter den Schnittstellen wählen, welche Ihr Gerät zur Verfügung stellt, die Schnittstelle muss jedoch Mitglied der Drop-In-Gruppe sein.</p>
<p>ARP Lifetime</p>	<p>Legt die Zeitspanne fest, während derer ARP-Einträge im Cache gehalten werden.</p> <p>Der Standardwert ist <i>3600</i> Sekunden.</p>
<p>DNS-Zuweisung über DHCP</p>	<p>Das Gateway kann DHCP-Pakete, die die Drop-In-Gruppe durchlaufen, modifizieren und sich selbst als angebotenen DNS-Server eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • Unverändert (Standardwert) • Eigene IP-Adresse.
<p>Vom NAT ausnehmen (DMZ)</p>	<p>Hier können Sie Datenverkehr von NAT ausnehmen.</p> <p>Verwenden Sie diese Funktion, um zum Beispiel die Erreichbarkeit bestimmter Web-Server in einer DMZ sichzustellen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>Schnittstellenauswahl</p>	<p>Wählen Sie alle Ports aus, die in der Drop In-Gruppe (im Netzwerk) enthalten sein sollen.</p> <p>Fügen Sie mit Hinzufügen weitere Einträge hinzu.</p>

2.2 Special Session Handling

Ab **Systemsoftware 7.10.5** ist das neue Menü **Netzwerk->Lastverteilung->Special Session Handling** verfügbar.

2.2.1 Special Session Handling

Special Session Handling ermöglicht Ihnen einen Teil des Datenverkehrs auf Ihrem Gerät über eine bestimmte Schnittstelle zu leiten. Dieser Datenverkehr wird von der Funktion **Lastverteilung** ausgenommen.

Die Funktion **Special Session Handling** können Sie zum Beispiel beim Online Banking verwenden, um sicherzustellen, dass der HTTPS-Datenverkehr auf einen bestimmten Link übertragen wird. Da beim Online Banking geprüft wird, ob der gesamte Datenverkehr aus derselben Quelle stammt, würde ohne **Special Session Handling** die Datenübertragung bei Verwendung von **Lastverteilung** unter Umständen abgebrochen.

Im Menü **Netzwerk->Lastverteilung->Special Session Handling** wird eine Liste mit Einträgen angezeigt. Wenn Sie noch keine Einträge konfiguriert haben, ist die Liste leer.


Jeder Eintrag enthält u.a. Parameter, welche die Eigenschaften eines Datenpakets mehr oder weniger detailliert beschreiben. Das erste Datenpaket, auf das die hier konfigurierten Eigenschaften zutreffen, legt die Route für bestimmte nachfolgende Datenpakete fest.

Welche Datenpakete danach über diese Route geleitet werden, wird im Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu->Erweiterte Einstellungen** konfiguriert.

Wenn Sie zum Beispiel im Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu** den Parameter **Dienst** = `http (SSL)` wählen (und bei allen anderen Parametern die Standardwerte belassen), so legt das erste HTTPS-Paket die **Zieladresse** und den **Zielport** (d.h. Port 443 bei HTTPS) für später gesendete Datenpakete fest.

Wenn Sie unter **Unveränderliche Parameter** für die beide Parameter **Zieladresse** und **Zielport** die Standardeinstellung `aktiviert` belassen, so werden die HTTPS-Pakete mit derselben Quell-IP-Adresse wie das erste HTTPS-Paket über Port 443 zur selben **Zieladresse** über dieselbe Schnittstelle wie das erste HTTPS-Paket geroutet.

2.2.1.1 Bearbeiten oder Neu

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

Das Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob Special Session Handling aktiv sein soll. Mit Auswahl von <code>Aktiviert</code> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.

Feld	Beschreibung
Dienst	<p>Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>
Protokoll	<p>Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Ziel-IP-Adresse/Netzmaske	<p>Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	<p>Geben Sie, falls gewünscht, eine Zielport-Nummer bzw. einen Bereich von Zielport-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Zielport ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Zielport ein. • <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.
Quellschnittstelle	<p>Wählen Sie, falls gewünscht, die Quellschnittstelle Ihres Geräts aus.</p>

Feld	Beschreibung
Quell-IP-Adresse/Netzmaske	<p>Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port/Bereich	<p>Geben Sie, falls gewünscht, eine Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Zielport ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Zielport ein. • <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.
Special Handling Timer	<p>Geben Sie ein, während welcher Zeitspanne die spezifizierten Datenpakete über den festgelegten Weg geroutet werden sollen.</p> <p>Der Standardwert ist <i>900</i> Sekunden.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Unveränderliche Parameter	<p>Legen Sie fest, ob die beiden Parameter Zieladresse und Zielport bei später gesendeten Datenpaketen denselben Wert haben müssen wie beim ersten Datenpaket, d.h. ob die nachfolgenden Datenpakete über denselben Zielport zur selben Zieladresse geroutet werden müssen.</p> <p>Standardmäßig sind die beiden Parameter Zieladresse und Zielport aktiv.</p> <p>Belassen Sie die Voreinstellung <i>Aktiviert</i> bei einem oder bei beiden Parametern, so muss der Wert des jeweiligen Parame-</p>

Feld	Beschreibung
	<p>ters bei den später gesendeten Datenpaketen derselbe sein wie beim ersten Datenpaket.</p> <p>Sie können, falls gewünscht, einen oder beide Parameter deaktivieren.</p> <p>Der Parameter Quell-IP-Adresse muss bei später gesendeten Datenpaketen immer denselben Wert haben wie beim ersten Datenpaket. Er kann daher nicht deaktiviert werden.</p>


2.3 Schnittstellenbasiertes DNS-Serverkonzept

Ab **Systemsoftware 7.10.5** können neben dem systemweit geltenden DNS-Server auch schnittstellenspezifische DNS-Server verwaltet werden. Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern eingerichtet sind und Lastverteilung verwendet wird.

2.3.1 DNS-Server

Im Menü **Lokale Dienste->DNS->DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

2.3.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere DNS-Server einzurichten.

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<p>Wählen Sie aus, ob der DNS-Server aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.

Feld	Beschreibung
Priorität	<p>Weisen Sie dem DNS-Server eine Priorität zu.</p> <p>Sie können einer Schnittstelle (d.h. zum Beispiel einem Ethernet-Port oder einem PPPoE-WAN-Partner) mehrere Paare von DNS-Servern (Primärer DNS-Server und Sekundärer DNS-Server) zuweisen. Verwendet wird das Paar mit der höchsten Priorität, wenn die Schnittstelle im Zustand "up" ist.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 9 (niedrigste Priorität).</p> <p>Standardwert ist 5 .</p>
Schnittstelle	<p>Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll.</p> <p>Mit der Einstellung <i>Keine</i> wird ein globaler DNS-Server angelegt.</p>
Schnittstellenmodus	<p>Wählen Sie aus, ob die IP-Adressen von Name-Servern für die Namensauflösung von Internet-Adressen automatisch bezogen oder ob abhängig von der Priorität bis zu zwei feste DNS-Server-Adressen eingetragen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> • <i>Dynamisch</i> (Standardwert)
Primärer DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie die IP-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie optional die IP-Adresse eines alternativen Name-Servers ein.</p>

2.4 Lastverteilung - Parameter Routenselektor und IP-Adresse zur Nachverfolgung hinzugefügt

Im Menü **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu** können Sie durch Auswahl der Schaltfläche **Hinzufügen** die Schnittstellen der **Lastverteilungsgruppen** bearbeiten. Unter **Erweiterte Einstellungen** sind die Parameter **Routenselektor** und **IP-Adresse zur Nachverfolgung** hinzugekommen.

Routenselektor

Der Parameter **Routenselektor** ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten Anwendungsfällen notwendig, um die vom Router verwalteten IP Sessions eindeutig je Loadbalancing -Gruppe bilanzieren zu können. Für die Anwendung des Parameters gelten folgende Regeln:

- Ist eine Schnittstelle nur einer Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig.
- Ist eine Schnittstelle mehreren Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich.
- Innerhalb einer Lastverteilungsgruppen muss der Routenselector aller Schnittstelleneinträge identisch konfiguriert sein.



Wichtig

Zur Konfiguration des Routenselektors müssen die zum Loadbalancing notwendigen Routen zwingend vorher konfiguriert sein.

IP-Adresse zur Nachverfolgung

Mit dem Parameter **IP-Adresse zur Nachverfolgung** können Sie eine bestimmte Route überwachen lassen.

Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. der Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die Konfiguration von Host-Überwachungseinträgen zwingend erforderlich. Konfiguriert werden

kann dies im Menü **Lokale Dienste->Überwachung->Hosts**. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion **Überwachung** berücksichtigt werden. Über die Konfiguration der **IP-Adresse zur Nachverfolgung** im Menü **Lastverteilung->Lastverteilungsgruppen->Erweiterte Einstellungen** erfolgt die Verknüpfung zwischen der Lastverteilungsfunktion und der Host-Überwachungsfunktion. Der Lastverteilungsstatus der Schnittstelle wechselt nun in Abhängigkeit zum Status des zugewiesenen Host-Überwachungseintrages.

2.5 IPSec over TCP

Bei der IPSec-Konfiguration steht im Menü **VPN->IPSec->Optionen->Erweiterte Einstellungen** die Option **IPSec über TCP** zur Verfügung. Diese Funktion beruht auf der NCP-Pathfinder-Technologie und sorgt dafür, dass der IPSec-Datenverkehr in eine Pseudo-HTTP-Session eingebettet wird. Dies ermöglicht die Nutzung von IPSec auch in Situationen, in denen dies sonst nicht möglich wäre (z. B. wenn eine Firewall IPSec-Verkehr unterbindet).

2.6 Wireless LAN Controller - Parameter Standort des Slave-AP hinzugefügt

Im Menü **Wireless LAN Controller->Controller-Konfiguration->Allgemein** wurde der Parameter **Standort des Slave-AP** hinzugefügt.

Sie können mit diesem Parameter wählen, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden.

Die Einstellung *Entfernt (WAN)* ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die APs über VPN angebunden sind, kann es vorkommen, dass eine Verbindung unterbrochen wird. In diesem Fall behält der entsprechende AP mit der Einstellung *Entfernt (WAN)* seine Konfiguration bis die Verbindung wieder hergestellt ist. Danach bootet er und anschließend synchronisieren sich Controller und AP erneut.

Kapitel 3 Änderungen

Folgende Änderungen sind in **Systemsoftware 7.10.5** vorgenommen worden.

3.1 FCI - DNS-Serverkonfiguration - geändert

Globale DNS-Server werden nicht mehr im FCI Menü **Lokale Dienste->DNS->Globale Einstellungen** angelegt sondern im Menü **Lokale Dienste->DNS->DNS-Server->Neu**.

Deshalb wurde unter **Lokale Dienste->DNS->Globale Einstellungen** der Parameter **DNS-Serverkonfiguration** mit den Wahlmöglichkeiten *Dynamisch* und *Statisch* entfernt. Die Parameter **DNS-Server** *Primär* und *Sekundär* wurden aus demselben Grund entfernt.

Um im neuen Menü **Lokale Dienste->DNS->DNS-Server->Neu** einen globalen DNS-Server anzulegen, belassen Sie die Standardeinstellung **Schnittstelle** *Keine*.

3.2 FCI - Überwachung - Hosts geändert

Im FCI Menü **Lokale Dienste->Überwachung->Hosts->Neu** wurde das Feld **Versuche** entfernt und stattdessen die Felder **Erfolgreiche Versuche** und **Fehlgeschlagene Versuche** hinzugefügt.

Mit **Fehlgeschlagene Versuche** können Sie angeben, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird.

Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird.

Mit **Erfolgreiche Versuche** können Sie festlegen, wieviele Pings beantwortet werden müssen, damit ein Host als erreichbar angesehen wird.

Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.

Das Feld **Regulierte Schnittstellen** wurde in **Auszuführende Aktion** umbenannt. Die Reihenfolge von **Schnittstelle** und **Schnittstellenaktion** wurde vertauscht. **Schnittstellenaktion** wurde in **Aktion** umbenannt. Unter **Aktion** steht der neue Wert *Überwachen* zur Verfügung.

Wenn Sie **Aktion** *Überwachen* wählen, können Sie die IP-Adresse überwachen, die unter **Überwachte IP-Adresse** angegeben ist.

3.3 UMTS Stick Vodafone K3806 unterstützt

Ab Systemsoftware 7.10.1 wird der UMTS Stick Vodafone K3806 (Huawei) unterstützt.

**Achtung**

Stecken oder ziehen Sie einen UMTS Stick nicht im laufenden Betrieb. Es kann dadurch zu Funktionsstörungen Ihres Gerätes kommen.

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 7.10.5** behoben worden:

4.1 WLAN Controller - Gefundene APs nicht gelöscht

(ID 15923)

Einmal gefundene aber vom WLAN Controller nicht mehr verwaltete APs (d.h. APs, die nicht mehr im Zustand managed waren) wurden nicht aus der Übersichtsseite unter **Wireless LAN Controller->Slave-AP-Konfiguraton->Slave Access Points** entfernt.

Das Problem ist gelöst.

4.2 RADIUS - Panic und Neustart

(ID 15843)

Ein RADIUS Reload verursachte eine Panic und einen Neustart des Systems.

Das Problem ist gelöst.

4.3 Routing - Probleme mit Erweiterter Route

(ID 16251)

Im Menü **Netzwerk->Routen->IP-Routen->Neu** wurde mit den Einstellungen **Erweiterte Route** *Aktiviert*, **Routentyp** = *Netzwerkroute* und **Netzwerktyp** = *Direkt* nach dem Speichern die Fehlermeldung "Eingabefehler. Der Netzwerktyp muß auf "Indirekt"

festgelegt werden." angezeigt.

Das Problem ist gelöst.

4.4 Keepalive Monitoring - Einträge fälschlicherweise gelöscht

(ID 15976)

Bei Verwendung des Setup Tools enthielt die MIB-Tabelle *ipHostsAliveTable* nach dem Speichern einer Konfiguration und einem Neustart des Systems nur elf Einträge, auch wenn mehr Einträge angelegt waren.

Das Problem ist gelöst.

4.5 QoS - Einträge nicht korrekt angezeigt

(ID 16116)

Im Menü **Netzwerk->QoS->QoS-Filter** funktionierte die Filterung für die Anzeige der Einträge nicht korrekt.

Das Problem ist gelöst.

4.6 QoS - Überflüssige Meldung angezeigt

(ID 16095)

Wenn im Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu** im Feld **Queues/Richtlinien** mit **Hinzufügen** Einträge angelegt waren und ein solcher Eintrag durch Klicken auf das Symbol Bearbeiten geöffnet wurde, wurde die Meldung "Ihre Anfrage wird bearbeitet" angezeigt.

Das Problem ist gelöst.

4.7 WLAN Controller - Falsche Kanäle verwendet

(ID 16026)

Wenn im Menü **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile->Neu->Erweiterte Einstellungen** das Feld **Kanalplan** = *Benutzerdefiniert* gesetzt war und unter **Wireless LAN Controller->**

Slave-AP-Konfiguration->Funkmodulprofile->Neu der Wert im Feld **Frequenzband** geändert wurde, wurden die Werte im Feld **Benutzerdefinierter Kanalplan** nicht angepasst.

Das Problem ist gelöst, die Werte werden entsprechend der Einstellung **Kanalplan** = *Auto* voreingestellt.

4.8 IPSec - Falscher Wert gespeichert

(ID 15990)

Wenn im Menü **VPN->IPSec->Phase-1-Profile->Neu** das Feld **Lokaler ID-Typ** = *ASN.1-DN (Distinguished Name)* gesetzt war, das Feld **Lokaler ID-Wert** leer gelassen wurde und diese Konfiguration gespeichert wurde, wurde beim erneuten Aufrufen dieses Eintrags **Lokaler ID-Typ** = *Fully Qualified Domain Name (FQDN)* angezeigt.

Das Problem ist gelöst.

4.9 ISDN - Skriptfehler mit Service Tool

(ID 15804)

Bei Verwendung des ISDN Service-Einwahl-Tools **SvcCfgMgr** konnte es vorkommen, dass ein Skriptfehler auftrat.

Das Problem ist gelöst.

4.10 IPSec - Einrichten eines Peers fehlgeschlagen

(ID 16271)

Beim Einrichten eines Peers konnte es vorkommen, dass auf dem System ein Stacktrace ausgelöst wurde.

Das Problem ist gelöst.

4.11 Filter - Anlegen eines neuen Filters fehlgeschlagen

(ID 16180)

Wenn im Menü **Netzwerk->QoS->QoS-Filter->Neu** das Feld **Dienst** = *any* gesetzt war, misslang das Anlegen eines neuen Filters mit der Meldung "Eingabefehler. Ungültiger Wert für Attribut".

Das Problem ist gelöst.

4.12 IPSec - Fehlermeldungen angezeigt

(ID 15708)

Nach dem Aufbau einer IPSec-Verbindung erschien die Fehlermeldung "NCI Alert ... failed to add attrib for ipsecStatPeerDPD" mehrmals.

Das Problem ist gelöst.

4.13 ISDN - Fehlermeldung während des Bootvorgangs

(ID 18973)

Bei Geräten mit nur einem ISDN BRI Port konnte es vorkommen, dass während des Bootvorgangs die Fehlermeldung "!!!no masterenable for [2:0] !!!" ausgegeben wurde.

Das Problem ist gelöst.

4.14 Scheduler - Keine Aktion

ID 15997

Wenn der eingestellte Timer-Bereich abließ, erfolgte keine Aktion für den Aktionstyp *Schnittstellenstatus*.

Das Problem ist gelöst.

4.15 GUI - Änderung nicht korrekt ausgeführt

ID 15970

Die Änderung der Netzmaske einer bestehenden IP-Adresse führte nicht zu einer korrekten Anpassung der Zielnetzwerkadresse.

Das Problem ist gelöst.

Kapitel 5 Bekannte Probleme

Folgende Probleme waren bei Veröffentlichung dieses Releases noch nicht behoben:

5.1 HTML-Konfiguration - Routenselektor nicht korrekt konfiguriert

ID 16536

In der grafischen Konfigurationsoberfläche kommt es zu einem Fehler bei der Konfiguration des Routenselektors im Menü

Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu. Beim Schreiben der Konfiguration wird nicht korrekt zwischen normalen und erweiterten Routen unterschieden, und es kann zu einer nicht funktionsfähigen Konfiguration kommen. Die Konfiguration über das Setup Tool umgeht diesen Fehler

5.2 Drop In - DHCP Relay

ID n/a

Die Funktion DHCP Relay ist für Schnittstellen, die mehreren Drop-In-Gruppen zugewiesen sind, nicht funktionsfähig.

5.3 Setup Tool - IP-Addressänderung nicht aktiviert

ID 16290

Ändert man die IP-Adresse einer Schnittstelle mit dem Setup Tool, so wird die Änderung nicht aktiv, bevor nicht die Konfiguration gesichert und das Gateway neu gestartet worden ist. Die Konfiguration mittels der grafischen Konfigurationsoberfläche umgeht dieses Problem.