Addendum LCOS 8.50 RU1

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Inhalt

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Germany

www.lancom.de

Würselen, Juli 2011

1 LCOS

1.1 Die Befehle LoadFirmware, LoadConfig, LoadScript und LoadFile

Verschiedene Anwendungen wie z. B. das Laden von Konfigurationen, Firmware-Versionen sowie Skripten oder die Prüfung einer Server-Identität mit Zertifikaten erfordern das Speichern von Dateien in einem Gerät. Sie können diese Dateien mit LANconfig oder WEBconfig in ein Gerät einspielen. Alternativ können Sie über Telnet oder SSH einen Befehl auf der Kommandozeile nutzen, um die entsprechenden Dateien direkt von einem Server (TFTP, HTTP oder HTTPS) in das Gerät zu laden. Dieses Vorgehen erleichert in größeren Installationen mit regelmäßigem Update von Firmware und/oder Konfiguration die Administration der Geräte.

Mit folgenden Befehlen laden Sie unterschiedliche Dateitypen in das Gerät:

- LoadConfig: Lädt eine Konfigurationsdatei (mit der Dateierweiterung *.lcf) in das Gerät.
- LoadFirmware: Lädt eine Firmware-Datei (mit der Dateierweiterung *.upx) in das Gerät.
- LoadScript: Lädt ein Script (mit der Dateierweiterung *.lcs) – z. B. mit Teilkonfigurationen – in das Gerät.
- LoadFile: Lädt Dateien verschiedenen Typs in das Gerät.

Die folgenden Beschreibungen verwenden 'LoadCommand' als allgemeine Bezeichnung der Load-Befehle.

Die Load-Befehle unterstützen das Laden der gewählten Datei über die Protokolle TFTP, HTTP und HTTPS. Ein TFTP-Server gleicht in der Funktionsweise einem FTP-Server, verwendet allerdings zur Datenübertragung ein anderes Protokoll. Bei der Verwendung eines HTTPS-Servers können Sie im Gerät ein Zertifikat hinterlegen, mit dem das Gerät die Identität des Servers prüft.

Der Befehl LoadFile unterstützt in der LCOS-Version 8.50 ausschließlich die Protokolle HTTP und HTTPS.

Starten Sie die Load-Befehle mit folgender Syntax in der Kommandozeile:

```
LoadCommand <Parameter>
```

Die verwendeten Parameter steuern das Verhalten der Befehle. Die Parameter können in beliebiger Kombination verwendet werden, notwendig ist ausschließlich die Angabe eines URL.

Die in der Kommandozeile übergebenen Parameter überschreiben die im Bereich /Setup/Automatisches-Laden/Netzwerk eingestellten Werte für Bedingung, URL und Minimal-Version für die Ausführung des Kommandos. Umgekehrt ergänzen die im Setup eingestellten Werte die Befehle auf der Kommandozeile, wenn keine entsprechenden Parameter übergeben werden.

Allgemeine Parameter für die Load-Befehle:

- -a: Dieser Parameter definiert die Absenderadresse, die das Gerät beim Download einer Datei an den Server übermittelt. Geben Sie die Absenderadresse in einer der folgenden Schreibweisen ein:
  - Beliebige, gültige IP-Adresse
  - INT für die Adresse des ersten Intranets
  - DMZ für die Adresse der ersten DMZ
  - LB0 bis LBF für die 16 Loopback-Adressen

  Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

- <URL>: Dieser Parameter gibt beim Download einer Datei von einem TFTP- oder HTTP(S)-Server den URL an, unter der die gewünschte Datei gespeichert ist. Geben Sie den URL in der folgenden Form an:

  ```
  LoadCommand Protokoll://Server/Verzeichnis/Dateiname.ext
  ```

  Geben Sie beim Download einer kennwortgeschützten Datei die Zugangsdaten in der folgenden Form an:

  ```
  LoadCommand
  Protokoll://Benutzername:Kennwort@Server/Verzeichnis/Dateiname.ext
  ```

- -s: Dieser Parameter gibt beim Download einer Datei von einem TFTP-Server den DNS-Namen oder die IP-Adresse des Servers an. Verwenden Sie diese Syntax alternativ zur Angabe einer URL.
- -f: Dieser Parameter gibt beim Download einer Datei von einem TFTP-Server den Namen der gewünschten Datei an. Verwenden Sie diese Syntax alternativ zur Angabe einer URL.

Werden die Parameter <URL> oder -s und -f nicht angegeben, verwendet das Gerät für die Befehle LoadFirmware, LoadConfig oder LoadScript die Standardwerte für den URL aus dem Bereich /Setup/Automatisches-Laden:

Verwenden Sie diese Standardwerte, wenn die aktuellen Konfigurationen, Skripte und Firmware-Versionen immer unter dem gleichen Namen an der gleichen Stelle gespeichert werden. In diesem Fall können Sie mit den einfachen Befehlen LoadConfig, LoadFirmware oder LoadScript automatisch die jeweils gültigen Dateien laden.

Für das automatische Laden sind folgende Parameter von besonderer Bedeutung:

-Cn: Dieser Parameter überprüft, ob die für den Befehl LoadFirmware verwendete Datei **neuer** ist im Vergleich zur im Gerät vorhandene Firmware.

- -Cd: Dieser Parameter überprüft, ob die für den Befehl LoadFirmware, LoadConfig oder LoadScript verwendete Datei **unterschiedlich** ist im Vergleich zur im Gerät vorhandenen Firmware oder Konfiguration bzw. neuer als das zuletzt ausgeführte Skript. Bei der Verwendung mit LoadScript aktualisiert dieser Parameter die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes.
- -u: Dieser Parameter deaktiviert die Versionsprüfung. Die für den Befehl LoadFirmware, LoadConfig oder LoadScript verwendete Datei wird auf jeden Fall geladen oder ausgeführt. Bei der Verwendung mit LoadScript belässt dieser Parameter die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes unverändert.
- -m: Dieser Parameter gibt die Minimalversion für eine Firmware an. Die für den Befehl verwendete Firmware muss mindestens dieser Version entsprechen, damit der Befehl LoadFirmware ausgeführt wird.

In der Default-Einstellung sind die Bedingungen im Bereich /Setup/Automatisches-Laden/Netzwerk auf "unbedingt" eingestellt. In der Default-Einstellung laden oder starten die Befehle LoadFirmware, LoadConfig oder LoadScript auf der Kommandozeile die entsprechende Firmware, Konfiguration oder Skriptdatei **ohne** Versionsprüfung.

Der Parameter -u hat immer Vorrang vor anderen mit den Befehlen übergebenen Parametern.

Bei der Übertragung von Dateien von einem HTTPS-Server zu einem Client-Gerät prüfen die beteiligten Netzwerkkomponenten die Identität der Gegenstelle mit Hilfe von Zertifikaten. Beim automatischen Laden von HTTPS-Servern stehen zusätzliche Parameter für den Download der Zertifikate und deren anschließende Prüfung zur Verfügung:

- -o <Pfad/Dateiname.ext>: Dieser Parameter gibt das Ziel für den Download einer Datei von einem HTTP(S)-Server mit dem Befehl LoadFile an. Verwenden Sie diese Option, um z. B. ein Zertifikat für die spätere Identitätsprüfung bei Zugriff auf einen HTTPS-Server in Ihrem Gerät zu speichern.
- -c <Pfad/Dateiname.ext>: Dieser Parameter gibt beim Download einer Datei von einem HTTPS-Server den Namen des Zertifikats an, mit dem das Gerät die Identität des Servers prüft.
- -p <Pfad/Dateiname.ext>: Dieser Parameter gibt beim Download einer Datei von einem HTTPS-Server den Namen des PKCS#12-Containers an. Der PKCS#12-Container kann mehrere CA-Zertifikate enthalten und unterstützt so die Identitätsprüfung von HTTPS-Servern mit Zertifikatsketten. Außerdem kann ein PKCS#12-Container ein Gerätezertifikat und den zugehörigen privaten Schlüssel enthalten und so die Identität des Geräts gegenüber dem HTTPS-Server bestätigen, wenn der HTTPS-Server die Authentifizierung mit einem Zertifikat erfordert.
- -d: Mit dieser Passphrase verschlüsselt das Gerät einen unverschlüsselten PKCS#12-Container.

- -n: Dieser Parameter deaktiviert die Prüfung der Server-Namen beim Download einer Datei mit dem Befehl LoadFile von einem HTTPS-Server. Wenn Sie den Server in der Download-URL als DNS-Name angeben (nicht als IP-Adresse), dann übermittelt das Gerät in seiner Anfrage an den Server zusätzlich den Server-Namen. Wenn es sich bei dem HTTPS-Server um einen virtuellen Server handelt, kann dieser Server mit den passenden Zertifikaten für den übermittelten DNS-Namen antworten. Ohne Angabe dieses Parameters prüft das Gerät, ob der DNS-Name in der Download-URL mit dem 'common name' der übermittelten Zertifikate übereinstimmt. Das Gerät startet den Download nur dann, wenn diese Prüfung erfolgreich verläuft.

Verwenden Sie für die Angabe einer Datei im Dateisystem des Geräts einer der beiden folgenden Schreibweisen:

- Geben Sie ein Ziel im internen Dateisystem des Geräts mit dem Pfad '/minifs/Dateiname.ext' an.
- Geben Sie ein Ziel auf einem externen USB-Datenträger mit dem Pfad '/mountpoint/Verzeichnis/Dateiname.ext' an. Die möglichen Einhängepunkte (Mountpoints) finden Sie unter '/Status/Dateisystem/Volumes'.

Im Dateinamen inklusive Pfad können Sie folgende allgemeine Variablen verwenden:

- `%m`: Die LAN MAC Adresse des Gerätes (Hexadezimal, kleine Buchstaben, ohne Trennzeichen)
- `%s`: Die Seriennummer des Gerätes
- `%n`: Der Gerätename
- `%l`: Der Ort des Gerätes ('Standort' - aus der Konfiguration)
- `%d`: Der Gerätetyp

Sie können diese allgemeinen Variablen in den Load-Befehlen verwenden, können die Werte für die Variablen jedoch nicht verändern.

Neben diesen allgemeinen Variablen können Sie auch die folgenden Umgebungsvariablen der Geräte nutzen, um die Ausführung der Load-Befehle flexibler zu gestalten. Alle vordefinierten Umgebungsvariablen beginnen mit zwei Unterstrichen. In den Befehlen an der Kommandozeile leiten Sie die Variablen mit einem vorangestellten Dollarzeichen ein.

- `__BLDDEVICE`: Das Sub-Projekt des Gerätes. Diese Umgebungsvariable entspricht dem zweiten Teil des Wertes für `PROJECT`, wenn Sie in der Kommandozeile den Befehl `#sysinfo#` ausführen. Das Sub-Projekt besteht in der Regel aus einer Zeichenkette ohne Leerzeichen und steht für das Hardware-Modell des aktuellen Gerätes.
- `__DEVICE`: Der Typ des Gerätes, so wie er z. B. in LANconfig oder auf dem Typenschild des Gerätes angezeigt wird.
- `__FWBUILD`: Die Build-Nummer der aktuell im Gerät verwendeten Firmware. Die Build-Nummer ist eine Zahl.
- `__FWVERSION`: Die Versionsbezeichnung der aktuell im Gerät verwendeten Firmware in der Form 'x.yy'. Die Firmware-Version besteht aus der Major-Release vor dem Punkt und der Minor-Release nach dem Punkt.
- `__LDRBUILD`: Die Build-Nummer des aktuell im Gerät installierten Loaders. Die Build-Nummer ist eine vier-stellige Zahl.
- `__LDRVERSION`: Die Versionsbezeichnung des aktuell im Gerät installierten Loaders in der Form 'x.yy'. Die Loader-Version besteht aus der Major-Release vor dem Punkt und der Minor-Release nach dem Punkt.
- `__MACADDRESS`: Der Typ des Gerätes, angegeben als 12-stellige Zeichenkette hexadezimaler Werte in Kleinschreibung ohne Trennzeichen.
- `__SERIALNO`: Die Seriennummer des Gerätes.
- `__SYSNAME`: Die Systembezeichnung des Gerätes.

Ältere Loader geben für die Anfrage der Loader-Build-Nummer eine leere Zeichenkette zurück.

Wenn Sie einen Namen der Umgebungsvariablen schon als benutzerdefinierte Variable in einem Bereich der Konfiguration verwendet haben, nutzen sowohl die Konfiguration als auch die Befehle in der Kommandozeile vorrangig die Werte der benutzerdefinierten Variablen.

Nutzen Sie die folgenden Befehle in der Kommandozeile, um die Umgebungsvariablen anzuzeigen oder zu verändern:

- `printenv`: Zeigt alle Umgebungsvariablen und deren aktuelle Werte an. Wenn Sie einer oder mehrerne Umgebungsvariablen mit dem Befehl `setenv` einen Wert zugewiesen haben, zeigt die Ausgabe des Befehls `printenv` im oberen Teil den benutzerdefinierten Wert und im unteren Teil den Standardwert an.
- `echo __device`: Zeigt den aktuellen Werte einer einzelnen Umgebungsvariablen an, in diesem Beispiel den Wert der Variablen '__DEVICE'.
- `setenv __device MeinWert`: Setzt den Wert einer Umgebungsvariablen auf den gewünschten Wert.
- `unsetenv __device`: Setzt den Wert einer Umgebungsvariablen auf den Standardwert zurück.

Beispiele für die Load-Befehle:

- Mit dem folgenden Befehl in einer Telnet-Sitzung lädt das Gerät eine Firmwaredatei mit dem Namen 'LC-1811-8.50.0019.upx' aus dem Verzeichnis 'LCOS/850' vom TFTP-Server mit der IP-Adresse '192.168.2.200':

```
LoadFirmware -s 192.168.2.200 -f LCOS/850/LC-1811-8.50.0019.upx
```

- Mit dem folgenden Befehl in einer Telnet-Sitzung lädt das Gerät ein zur MAC-Adresse passendes Script (mit z. B. dem Namen '00a0571735da.lcs') vom TFTP-Server mit der IP-Adresse '192.168.2.200':

```
LoadScript -s 192.168.2.200 -f %m.lcs
```

- Mit dem folgenden Befehl in einer Telnet-Sitzung lädt das Gerät eine Firmwaredatei mit dem Namen 'LC-1811-8.50.0019.upx' aus dem Verzeichnis 'download' vom HTTPS-Server mit der IP-Adresse 'www.myserver.com'. Dabei wird die Identität des Servers mit dem Zertifikat 'sslroot.crt' geprüft:

```
LoadFirmware -c sslroot.crt
https://www.myserver.com/download/LC-1811-8.50.0019.upx
```

- Mit dem folgenden Befehl in einer Telnet-Sitzung lädt das Gerät ein zur Seriennummer und zur aktuellen Firmware passendes Script. Das Gerät entnimmt die Werte für Seriennummer und Firmware aus den entsprechenden Umgebungsvariablen:

```
Loadscript $__SERIALNO-$__FWVERSION.lcs
```

1.1.1 Anwendungsbeispiele

Konfiguration und Firmware regelmäßig updaten

Dieses Szenario beschreibt, wie Sie die Konfiguration und die Firmware eines Gerätes regelmäßig alle 24 Stunden updaten.

Voraussetzungen:

- Das Gerät verfügt derzeit über die Firmware der Version '8.30' und ist mit einer passenden Konfiguration ausgestattet.
- Auf dem HTTP-Server liegen die neue Firmware-Version jeweils in Form der Datei 'LCOS.upx' und die dazu passende Konfiguration jeweils in Form der Datei 'LCOS.lcf'.

Konfiguration:

1. Geben Sie den Pfad an, von dem der Befehl 'LoadFirmware' eine Firmware lädt, wenn keine anderen Parameter vorliegen. Wählen Sie für das Laden der Firmware von einem HTTP-Server z. B. folgenden Befehl:

```
set /setup/Automatisches-Laden/Netzwerk/Firmware/URL
http://www.mycompany.de/firmware/LCOS.upx
```

2. Stellen Sie die Bedingung für das Laden der Firmware so ein, dass nur eine neuere als die im Gerät vorhandene Firmware geladen wird:

```
set /setup/Automatisches-Laden/Netzwerk/Firmware/Bedingung wenn-neuer
```

3. Geben Sie den Pfad an, von dem der Befehl 'LoadConfig' eine Konfiguration lädt, wenn keine anderen Parameter vorliegen. Wählen Sie für das Laden der Konfiguration von einem HTTP-Server z. B. folgenden Befehl:

```
set /setup/Automatisches-Laden/Netzwerk/Firmware/URL
http://www.mycompany.de/configuration/LCOS.lcf
```

4. Stellen Sie die Bedingung für das Laden der Konfiguration so ein, dass nur eine andere als die im Gerät vorhandene Konfiguration geladen wird:

```
set /setup/Automatisches-Laden/Netzwerk/Konfiguration/Bedingung
wenn-unterschiedlich
```

5. Erstellen Sie einen cron-Job, der regelmäßig um 23:55 Uhr das Kommando 'LoadFirmware' ausführt:

```
cd /setup/Config/Cron-Tabelle
```

```
set 1 * * * 55 23 * * * LoadFirmware
```

6. Erstellen Sie einen cron-Job, der regelmäßig um 23:59 Uhr das Kommando 'LoadConfig' ausführt:

```
set 2 * * * 59 23 * * * LoadConfig
```

Konfiguration erst nach Firmware updaten

Dieses Szenario beschreibt, wie Sie z. B. im Rahmen eines Projektes zunächst ein Firmware-Update durchführen und erst danach die passende Konfiguration als Skript laden.

Voraussetzungen:

- Das Gerät verfügt derzeit über die Firmware der Version '8.30' und ist mit einer passenden Konfiguration ausgestattet.
- Auf dem HTTP-Server liegen die neue Firmware-Version in Form der Datei 'LCOS-850.upx' und die dazu passende Konfiguration in Form der Datei '<Seriennummer>-850.lcs'.

> Das Konfigurationsskript darf in diesem Szenario nur angewendet werden, wenn das Gerät über die passende Firmware verfügt.

Konfiguration:

1. Geben Sie den Pfad an, von dem der Befehl 'LoadFirmware' eine Firmware lädt, wenn keine anderen Parameter vorliegen. Wählen Sie für das Laden der Firmware von einem HTTP-Server z. B. folgenden Befehl:

```
set /setup/Automatisches-Laden/Netzwerk/Firmware/URL
http://www.mycompany.de/firmware
```

2. Stellen Sie die Bedingung für das Laden der Firmware so ein, dass nur eine neuere als die im Gerät vorhandene Firmware geladen wird:

```
set /setup/Automatisches-Laden/Netzwerk/Firmware/Bedingung wenn-neuer
```

3. Geben Sie den Pfad an, von dem der Befehl 'LoadConfig' eine Konfiguration lädt, wenn keine anderen Parameter vorliegen. Wählen Sie für das Laden der Konfiguration von einem HTTP-Server z. B. folgenden Befehl:

```
set /setup/Automatisches-Laden/Netzwerk/Firmware/URL
http://www.mycompany.de/configuration
```

4. Stellen Sie die Bedingung für das Laden der Konfiguration so ein, dass nur eine andere als die im Gerät vorhandene Konfiguration geladen wird:

```
set /setup/Automatisches-Laden/Netzwerk/Konfiguration/Bedingung
wenn-unterschiedlich
```

5. Erstellen Sie einen cron-Job, der regelmäßig alle 10 Minuten das Kommando 'LoadFirmware' ausführt:

```
cd /setup/Config/Cron-Tabelle

set 1 * * * 10 * * * * LoadFirmware
```

6. Erstellen Sie einen cron-Job, der regelmäßig alle 10 Minuten das Kommando 'LoadScript' ausführt:

```
set 2 * * * 10 * * * * LoadScript\ $__SERIALNO-$__FWVERSION.lcs
```

Ergebnis:

Bei dieser Konfiguration lädt das Gerät in jedem Fall zuerst die aktuelle Firmware.

Wenn das Gerät nach dem Hochladen der Firmware und des Konfigurationsskriptes auf den HTTP-Server zuerst den Befehl 'LoadScript' ausführt, enthält die Umgebungsvariable '__FWVERSION' zu diesem Zeitpunkt den Wert '8.30'. Der Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` findet zu diesem Zeitpunkt also kein passendes Konfigurationsskript. Anschließend führt das Gerät den Befehl `LoadFirmware LCOS.upx` aus, nach dem Neustart enthält die Umgebungsvariable '__FWVERSION' den Wert '8.50'. Der Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` findet dann ein passendes Skript zum Updaten der Konfiguration.

Im cron-Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` ist das Leerzeichen zwischen dem LoadScript-Kommando und der Umgebungsvariablen mit einem Backslash geschützt. Eine denkbare alternative Schreibweise, bei welcher der komplette Befehl mit Anführungszeichen eingeschlossen wird, führt zu einem Fehler. LCOS behandelt Umgebungsvariablen in Anführungszeichen wie normaler Text, die Umsetzung in den Inhalt der Variablen entfällt.

1.2 Erweiterung der Sysinfo

Um Änderungen der Konfiguration feststellen und den Zeitpunkt einer Änderung nachvollziehen zu können, enthält Sysinfo im Feld CONFIG_STATUS zusätzliche Einträge.

Die Geräte speichern den Wert CONFIG_STATUS bei jeder Änderung der Konfiguration (per Kommandozeile, per SNMP oder durch das Laden von Skripten oder kompletten Konfigurationen). Der Wert CONFIG_STATUS besteht aus den folgenden Komponenten:

- Hash-Wert der Gerätekonfiguration als eindeutiges Merkmal eines Konfigurationsstandes.
- Zeitstempel der letzten Konfigurationsänderung im Format HHMMSSddmmyyyy auf Basis der koordinierten Weltzeit UTC. Der Bezug auf UTC garantiert eindeutige Werte ohne Einfluss von Standort oder Sommerzeiteinstellung.
- Zähler für die Konfigurationsänderungen, fortlaufend.

Das Feld CONFIG_STATUS enthält neben einem Wert für Statusschalter der Konfiguration und und einem Wert für den Status zum Flashen der Konfiguration die zusätzlichen Komponenten in der Form <Hash>.<Datum>.<Zähler>.

Sie können die Änderungen an der Konfiguration sowohl in entsprechenden Dateien oder Skripten (z. B. mit LCMS) als auch auf den Geräten direkt vornehmen (Kommandozeile oder WEBconfig). Der Weg der Konfigurationsänderung hat dabei teilweise Einfluss auf den Inhalt des CONFIG_STATUS.

Hash-Wert der Gerätekonfiguration

Nur LCOS – das Betriebssystem der Geräte – kann den Hash-Wert berechnen. Der Hash-Wert ist für jeden Konfigurationsstand unterschiedlich, ein veränderter Hash-Wert auf einem Gerät zeigt so eine geänderte Konfiguration an.

LCOS speichert den berechneten Hash-Wert während des Flash-Vorgangs in das Gerät.

Zeitstempel der letzten Konfigurationsänderung

Sowohl LCOS als auch LCMS können den Zeitstempel setzen, sofern sie über eine gültige Uhrzeit verfügen.

Sofern der gewählte Konfigurationsweg nicht über eine gültige Uhrzeit verfügt, setzt das Gerät den Zeitstempel auf den Wert '00:00:00 0000-00-00'.

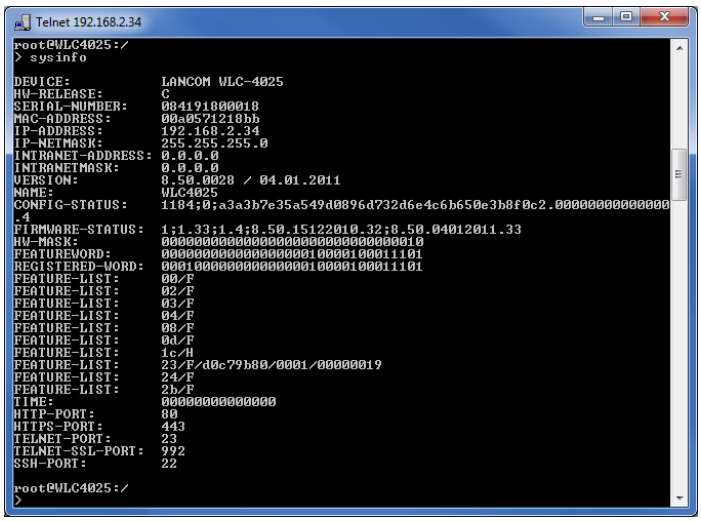
Zähler für die Konfigurationsänderungen

Bei der Auslieferung der Geräte enthält der Zähler für die Konfigurationsänderungen den Wert '0'. Danach erhöht jede Konfigurationsänderung diesen Wert um 1. Der Zähler für die Konfigurationsänderungen erlaubt die Ermittlung der aktuellen Konfigurationsversion auch dann, wenn bei der Konfiguration keine gültige Uhrzeit verfügbar war und der Zeitstempel daher den Wert '00:00:00 0000-00-00' enthält.

Ein Konfigurationszähler mit dem Wert '0' nach einer Änderung der Konfiguration deutet auf einen Fehler beim Lesen oder Schreiben des Zählers im Flash hin.

Anzeige des CONFIG_STATUS

Geben Sie zur Anzeige des Wertes CONFIG_STATUS an der Kommandozeile des Gerätes den Befehl `sysinfo` ein.



Anzeige der Systeminformationen auf der Kommandozeile

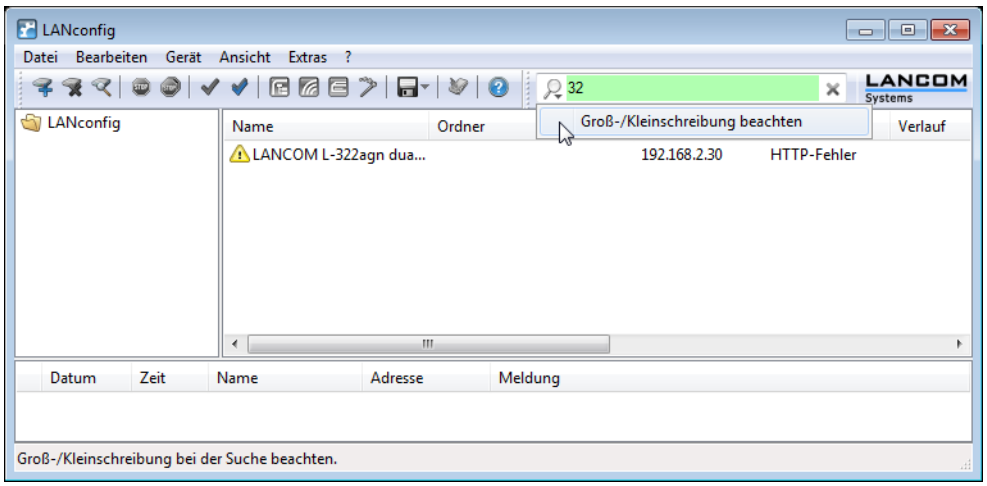
2 LCMS

2.1 LANCOM QuickFinder

Die Konfigurationsdialoge in LANconfig, LANmonitor und WLANmonitor umfassen zahlreiche Bereiche, Parameter und deren Werte sowie Tabellen. Der LANCOM Quickfinder unterstützt Sie bei der komfortablen Suche nach bestimmten Begriffen.

2.1.1 LANCOM QuickFinder in LANconfig

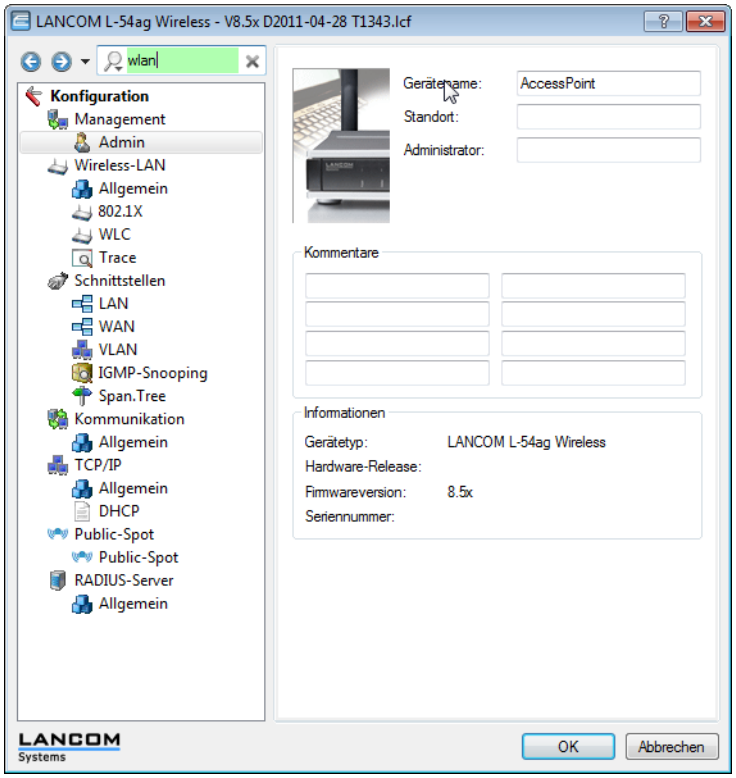
In der Hauptansicht von LANconfig finden Sie den LANCOM QuickFinder in der Symbolleiste. Geben Sie im Suchfenster einen Suchbegriff ein, um die Liste der angezeigten Geräte zu reduzieren. LANconfig durchsucht dabei alle Werte, die in den Spalten der Geräte-Liste verfügbar sind – auch die derzeit ausgeblendeten Spalten. Klicken Sie auf der Symbol neben der Lupe, um bei der Suche die Groß-/Kleinschreibung zu beachten.



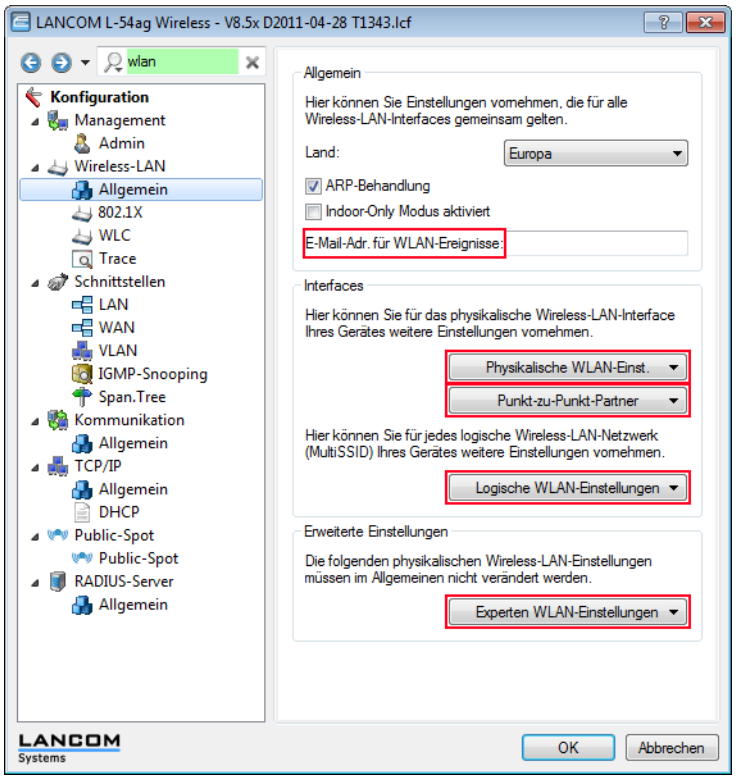
Wenn Sie einen bestimmten Wert oder Begriff in LANconfig oder der Konfiguration suchen, zeigt Ihnen der LANCOM QuickFinder in den Konfigurationsdialogen von LANconfig schnell alle Stellen, in denen der gesuchte Zeichenkette enthalten ist.

1. Starten Sie LANconfig.
2. Öffnen Sie die Konfiguration des Gerätes, welche Sie durchsuchen möchten.
3. Geben Sie im Suchfeld den gewünschten Begriff ein, z. B. 'wlan'. Die Suche unterscheidet nicht nach Groß- und Kleinschreibung. Sie können Teile von Worten oder Zahlen ebenso eingeben wie komplette Suchbegriffe. Leerzeichen in den Suchbegriffen suchen auch nur nach Zeichenketten, welche die entsprechenden Leerzeichen enthalten. Die Suchfunktion unterstützt jedoch keine Wildcards.

Der Konfigurationsbaum im linken Bereich von LANconfig ist nun reduziert auf alle Bereiche an, in denen der Suchbegriff enthalten ist:

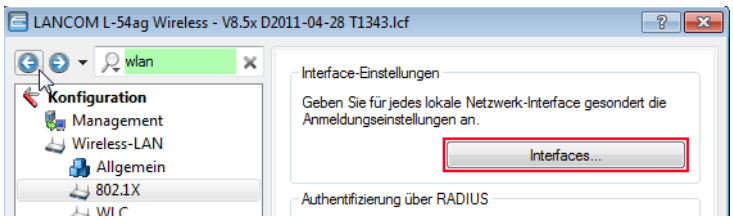


Wählen Sie einen der Bereiche im Konfigurationsbaum (z. B. 'WLAN/Allgemein'), um die entsprechenden Suchergebnisse im Konfigurationsdialog farbig eingerahmt anzuzeigen:

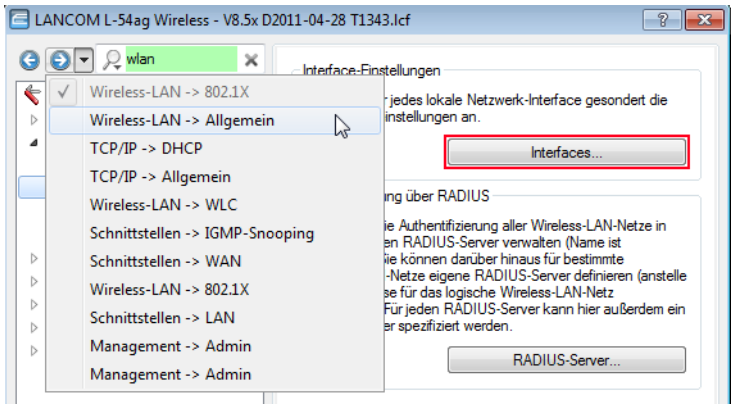


LANconfig stellt die Suchtreffer im Bereich der Firewall in der Version 8.50 nicht farbig dar.

Nutzen Sie die Navigationsschaltflächen 'Vor' und 'Zurück' links neben dem Suchfeld, um in den zuletzt besuchten Dialogen zu blättern:

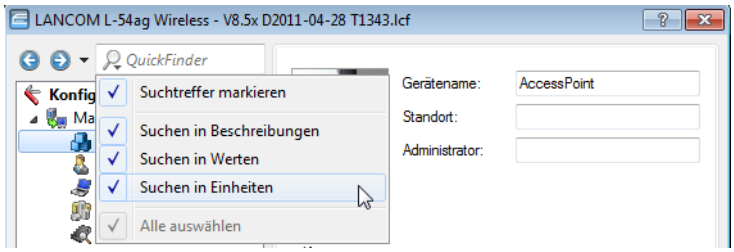


Für einen besonders schnellen Zugriff auf die letzten 10 besuchten Dialoge klicken Sie auf den Pfeil rechts neben der Schaltfläche 'Vor':



Klicken Sie auf das Kreuz rechts neben dem Suchfeld, um die Suche zu löschen und um im Konfigurationsbaum wieder alle Einträge anzuzeigen.

Um die Suchergebnisse optional zu reduzieren, wählen Sie Bereiche aus, die LANconfig in die Suche einbeziehen soll. Klicken Sie dazu auf die Lupe links neben dem Suchfeld und aktivieren oder deaktivieren Sie die gewünschten Bereiche. Legen Sie hier außerdem fest, ob die Suche die Treffer farbig markiert oder nur den Konfigurationsbaum auf die gefundenen Dialoge reduziert:



LANconfig löscht die Einstellung der Suchbereiche und die Liste der zuletzt besuchten Dialoge beim Schließen der Konfiguration.

Wenn Sie z. B. in der Konfiguration bestimmte Einstellungen für Ihren Internet-Provider vorgenommen haben, können Sie einfach mit der Eingabe des Namens alle Stellen in der Konfiguration finden, die sich auf diesen Provider beziehen.

Konkret erfasst die Suche dabei die folgenden Bereiche:

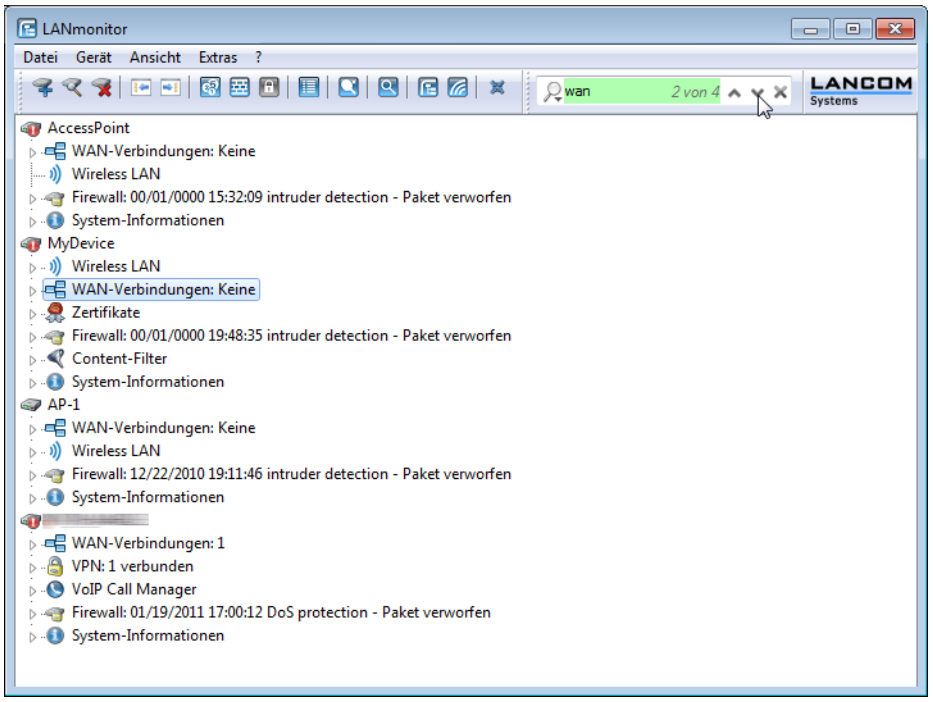
- Einträge im Konfigurationsbaum
- Bezeichnungen der Bereiche (Sektionen) in den einzelnen Konfigurationsdialogen

- Parameter
- Werte der Parameter
- Erläuternde Texte in den Dialogen
- Namen der Tabellen
- Namen der Tabellenspalten

Um die Suche in LANconfig zu nutzen gehen Sie vor wie in den folgenden Schritten beschrieben:

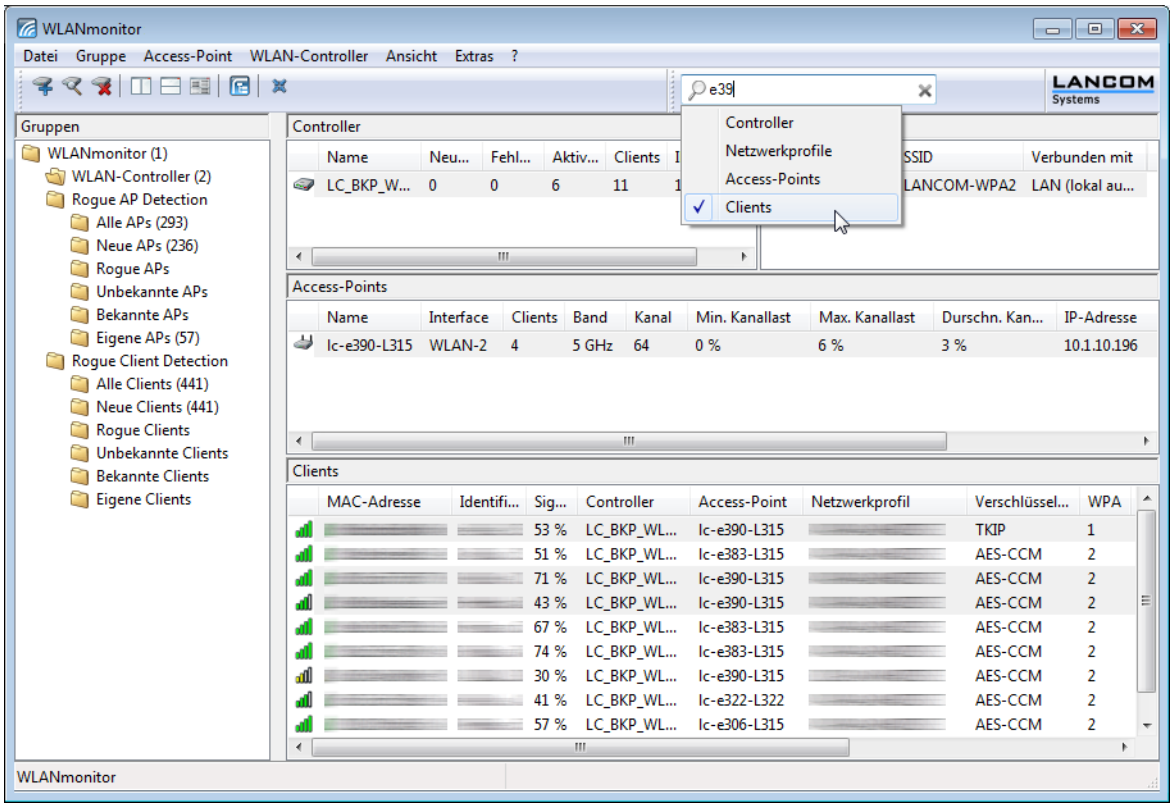
2.1.2 LANCOM QuickFinder im LANmonitor

Der LANmonitor zeigt je nach Anwendung zahlreiche Geräte, die den gesuchten Begriff enthalten können. Nach dem Start der Suche hebt LANmonitor zunächst die erste Fundstelle hervor. Wechseln Sie entweder mit den Pfeiltasten am rechten Rand des Suchfensters oder mit den der Tastenkombination Strg+F3 zur nächsten Fundstelle oder mit der Tastenkombination Strg+Shift+F3 zur vorherigen Fundstelle.



2.1.3 LANCOM QuickFinder im WLANmonitor

Der WLANmonitor erfasst sowohl Access Points als auch WLAN-Clients. Mit einem Klick auf die Lupe am linken Rand des Suchfensters öffnen Sie ein Kontextmenü zur Auswahl des Suchumfangs. Wählen Sie je nach Anwendung nur die Access Points, nur die Clients oder alle Einträge aus.



2.2 LANtracer: Tracen mit LANconfig und LANmonitor

Die Abfrage von Traces kann sehr komfortabel über LANconfig oder LANmonitor vorgenommen werden. Klicken Sie dazu mit der rechten Maustaste auf den Geräteeintrag und wählen Sie im Kontextmenü den Eintrag Traces.

Zur Abfrage von Traces über LANconfig oder LANmonitor muss ein Telnet-Zugriff auf das Gerät erlaubt sein. Beim Starten des Trace-Dialogs versuchen LANconfig oder LANmonitor zunächst eine SSL-verschlüsselte Telnet-Verbindung zum Gerät aufzubauen. Falls das Gerät keine SSL-Verbindungen unterstützt, wechseln LANconfig oder LANmonitor automatisch auf unverschlüsseltes Telnet. Wenn der Konfigurationszugriff auf das Gerät passwortgeschützt ist, sind zudem die Zugangsdaten für einen Administrator mit Trace-Rechten erforderlich.

2.2.1 Einleitung

Mit der Trace-Funktion in LANconfig und LANmonitor können Sie über die normalen Trace-Funktionen hinaus, wie sie von der Telnet-Oberfläche bekannt sind, weitere Funktionen nutzen, die eine Erstellung und Auswertung der Traces erleichtern. So kann z. B. die aktuelle Trace-Konfiguration, mit der die benötigten Trace-Befehle aktiviert werden, in einer Konfigurationsdatei gespeichert werden. Eine solche Trace-Konfiguration kann ein erfahrener Service-Techniker vorbereiten und einem weniger erfahrenen Anwender zur Verfügung stellen, der damit die gewünschte Trace-Ausgabe eines Gerätes

erzeugen kann. Auch die Trace-Ergebnisse können komfortabel in einer Datei gespeichert werden und an den Techniker zur Auswertung zurückgegeben werden.

Um das Trace-Fenster für ein Gerät zu öffnen, klicken Sie in LANconfig oder LANmonitor mit der rechten Maustaste auf den Eintrag des Gerätes und wählen im Kontext-Menü den Eintrag “Trace-Ausgabe erstellen”.

Der LANmonitor bietet die folgenden Schaltflächen zur Bedienung des Trace-Moduls:

Öffnet eine vordefinierte Konfiguration für die Trace-Ausgabe. Damit können Sie eine Trace-Ausgabe genau so erstellen, wie Sie z. B. von einem Service-Techniker benötigt wird.

Speichert die aktuelle Trace-Konfiguration oder die Trace-Daten, um diese an einen Anwender weiterzugeben.

Löscht die aktuelle Anzeige der Trace-Ergebnisse.

Startet die Ausgabe der Trace-Ergebnisse gemäß der aktuellen Konfiguration und wechselt automatisch in den Anzeige-Modus der Trace-Ergebnisse. Solange die Ausgabe der Trace-Ergebnisse läuft, sind alle anderen Schaltflächen deaktiviert.

Hält die Ausgabe der Trace-Ergebnisse an.

Wechselt in den Modus zur Konfiguration der Trace-Ausgabe.

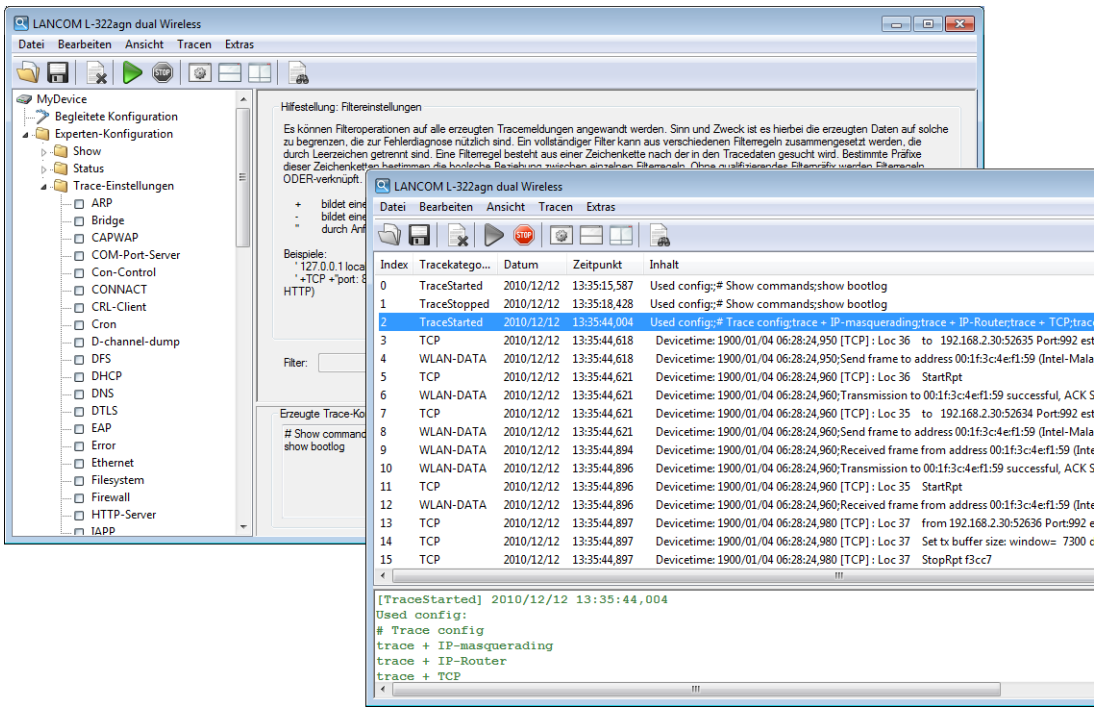
Wechselt in den Modus zur Anzeige der Trace-Ergebnisse.

Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern.

Öffnet das Fenster zur Suche in den Trace-Ergebnissen.

Startet die Synchronisation der beiden Traces in der geteilten Anzeige anhand des Zeitstempels.

Beendet die Synchronisation der beiden Traces in der geteilten Anzeige.



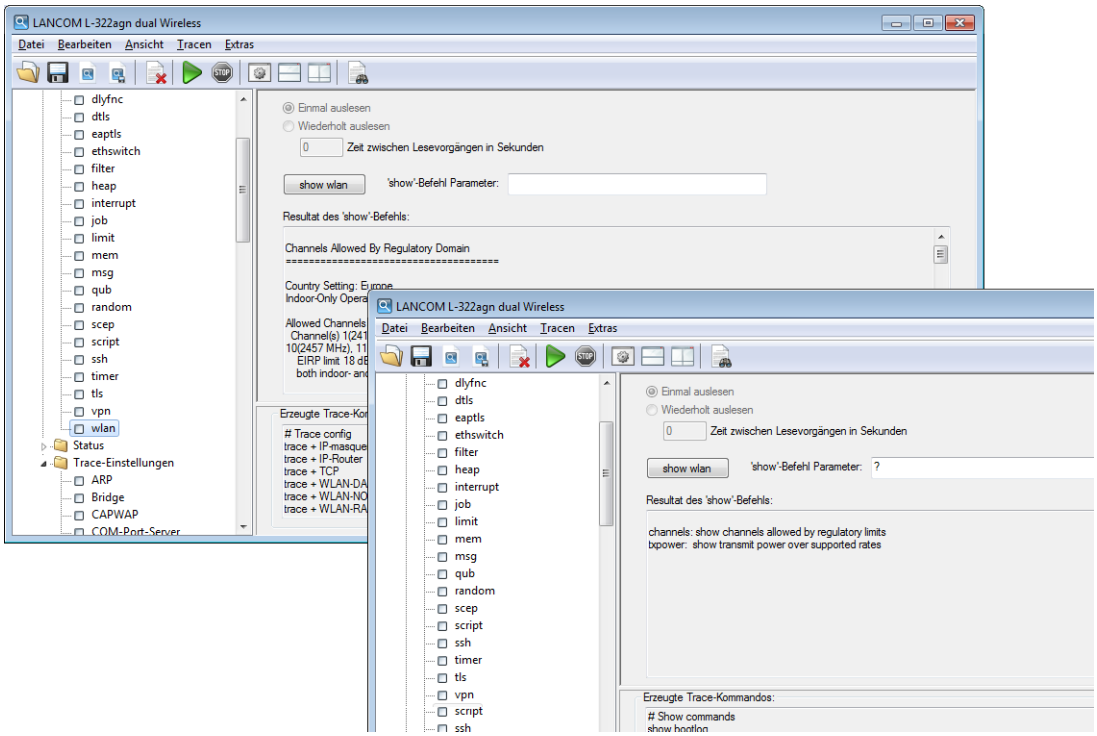
2.2.2 Experten-Konfiguration der Trace-Ausgaben

Über die Einstellungen des Assistenten hinaus können, mit Hilfe der Experten-Konfiguration, die Traces und weitere Anzeigen genauer eingestellt werden. Die Experten-Konfiguration unterteilt sich in drei Bereiche:

Show

Für jeden Gerätetyp können bestimmte Informationen mit einem Show-Kommando aufgerufen werden – üblicherweise werden die Show-Kommandos auf der Kommandozeile (Telnet) angewendet. In der Experten-Konfiguration des Traces kann der Aufruf dieser Show-Kommandos sehr bequem über die grafische Windows-Oberfläche erfolgen. Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Show-Kommandos und dann den Show-Button, um die aktuelle Ausgabe des Show-Kommandos aufzurufen. Je nach gewähltem Eintrag können bzw. müssen noch ergänzende Parameter angegeben werden. Eine Information über diese Parameter erhalten Sie, wenn Sie in das Eingabefeld ein Fragezeichen eingeben und den Show-Button klicken. Um die Ausgabe des Show-Kommandos in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem aktivierten Show-Kommando kann separat eingestellt werden, ob es nur einmal beim Start des Traces ausgeführt wird oder in regelmäßigen Intervallen, die in Sekunden eingestellt werden.

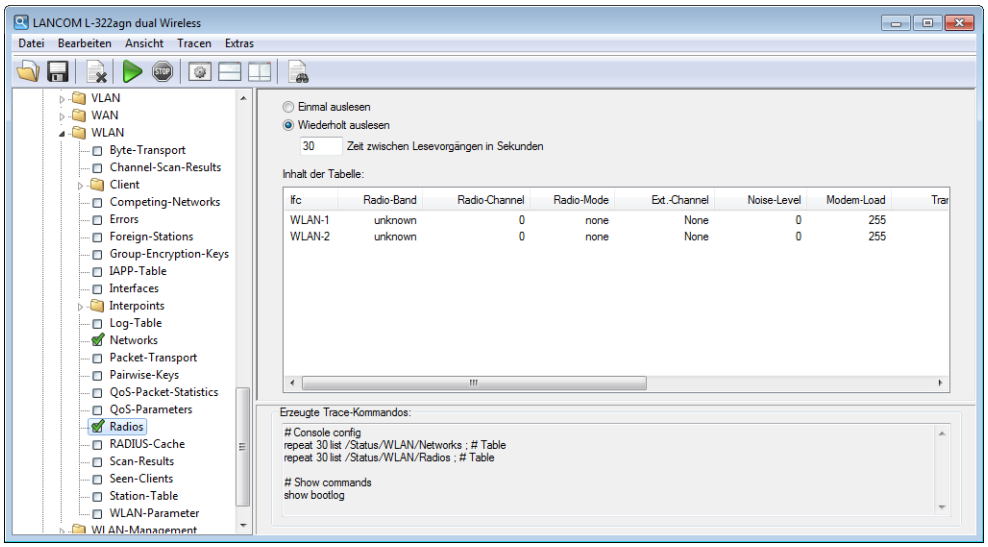
Die Einstellungen der Show-Kommandos werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert.



Status

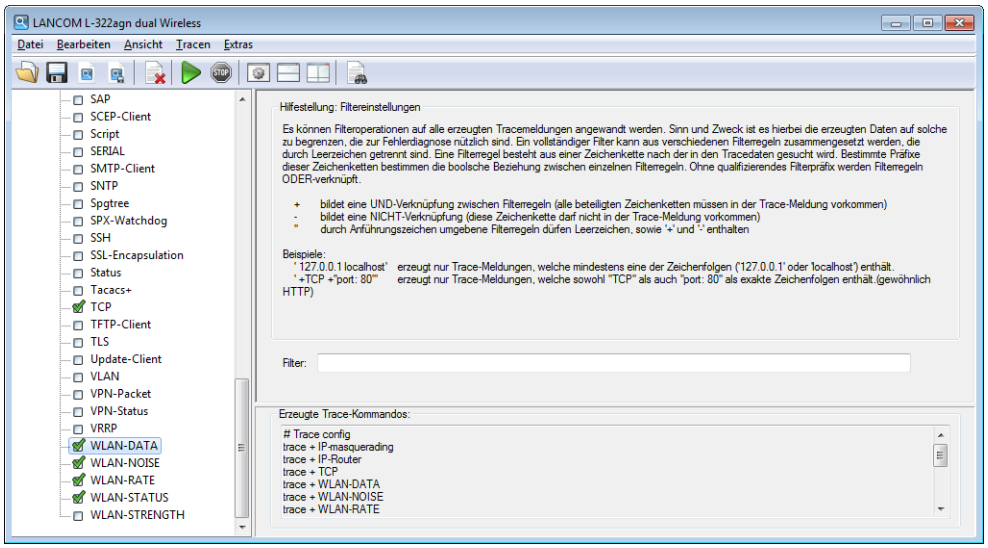
Über die Kommandozeile (Telnet) oder über WEBconfig können umfangreiche Statusinformationen und Statistiken über ein Gerät abgefragt werden. Alle verfügbaren Status-Informationen können auch über den Trace-Dialog eingesehen werden. Tabellen und Einzelwerte werden dabei über spezielle Symbole dargestellt. Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Status-Eintrags, um den aktuellen Inhalt der Tabelle bzw. des Wertes anzuzeigen. Um die Ausgabe des Status-Eintrags in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem aktivierten Status-Eintrag kann separat eingestellt werden, ob er nur einmal beim Start des Traces ausgelesen wird oder in regelmäßigen Intervallen, die in Sekunden eingestellt werden.

Die Einstellungen der Status-Informationen werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert. Die Status-Informationen werden zusammen mit den eigentlichen Trace-Daten gespeichert.



Trace-Einstellungen

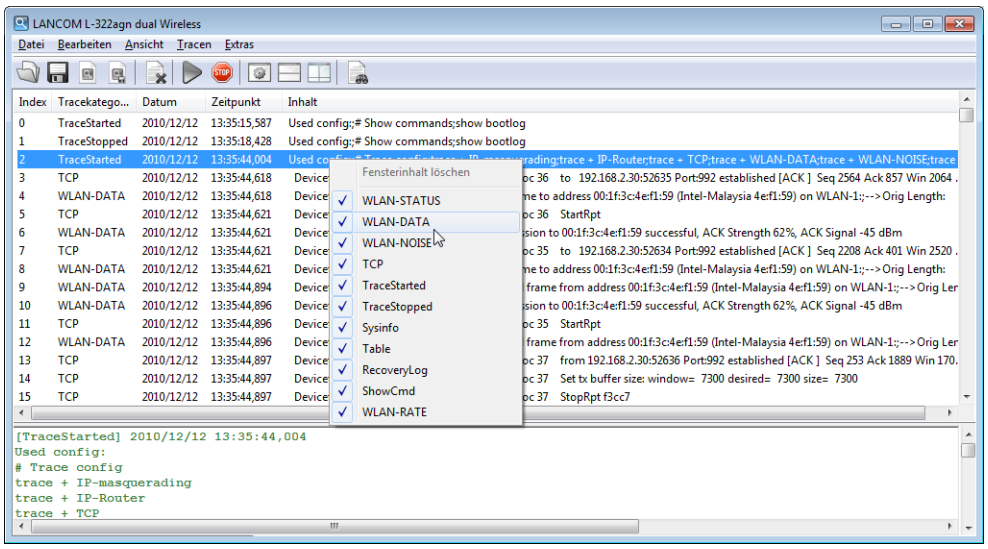
Im Bereich der Trace-Einstellungen können die Traces aktiviert werden, die für das aktuelle Gerät ausgegeben werden sollen. Um die Trace-Kommandos in die Trace-Ergebnisse zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem Trace können Sie einen Filter eingeben. Wenn Sie z. B. nur die IP-Traces einer bestimmten Workstation anzeigen möchten, geben Sie die entsprechende IP-Adresse als Filter des IP-Router-Traces ein.



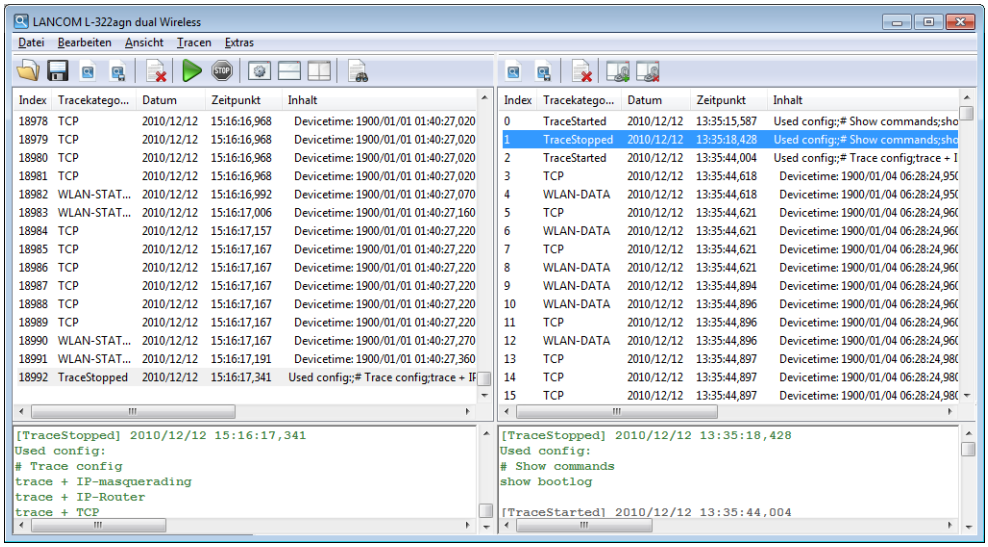
2.2.3 Anzeige der Trace-Ergebnisse

Die komplette Konfiguration des Traces wird im unteren Bereich des Dialogs angezeigt: Alle aktiven Trace-, Status- und Show-Einträge werden mit den jeweiligen Filtern und Parametern dort aufgelistet.

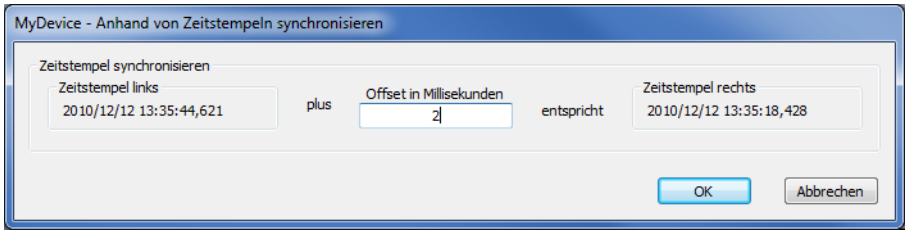
Um die Ausgabe der Trace-Daten zu starten, wechseln Sie mit dem Start-Button in den Anzeige-Modus.



Wenn Sie die Ergebnisse eines Traces mit einem anderen Trace vergleichen wollen, können Sie in der geteilten Trace-Ansicht zwei Traces nebeneinander darstellen.



Starten Sie die Synchronisation der beiden Traces anhand des Zeitstempels mit der Schaltfläche  . Geben Sie im folgenden Fenster einen geeigneten Wert für den Offset in Millisekunden ein und starten Sie die Synchronisation.



In dieser Ansicht werden die laufenden Trace-Ausgaben angezeigt:

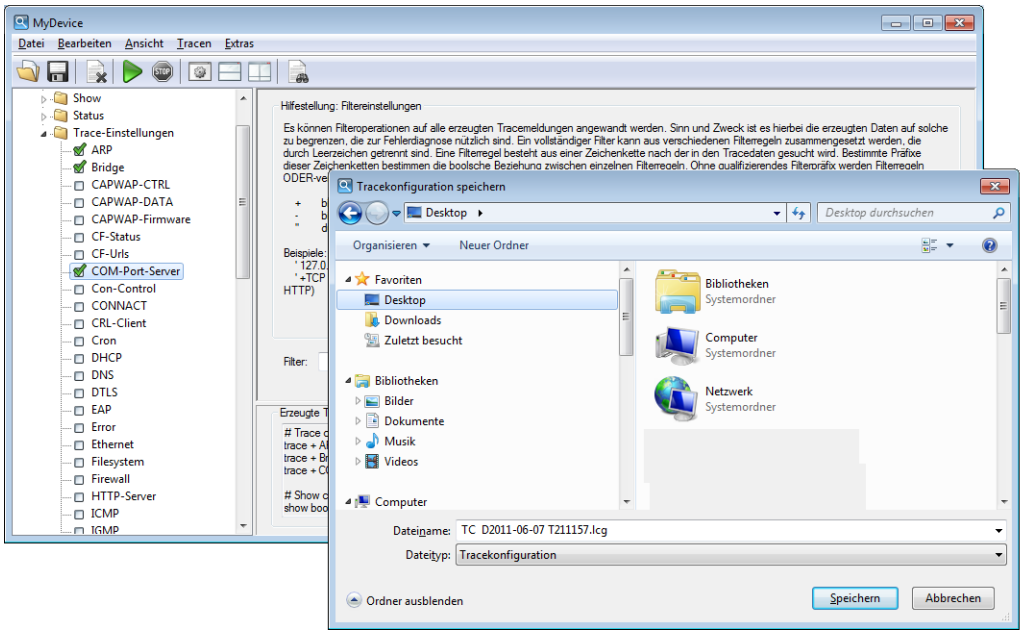
- Der obere Bereich listet die Ergebnisse für die ausgeführten Trace-Kommandos chronologisch in jeweils einer Zeile auf.
- Da die Ergebnisse für ein einzelnes Trace-Kommando sehr umfangreich sein können, stellt der untere Bereich die Ergebnisse für das im oberen Bereich ausgewählte Trace-Kommando ausführlich in meheren Zeilen dar.

Zur leichteren Navigation in langen Trace-Ausgaben können Sie im oberen Bereich auf ein Trace-Ereignis klicken, das entsprechende Ergebnis wird dann in der Liste aktiviert und im unteren Bereich grün hervorgehoben. Mit einem rechten Mausklick auf ein Trace-Ereignis öffnen Sie ein Kontext-Menü, in dem Sie die einzelnen Trace-Ergebnisse ein- und ausblenden können.

Die Trace-Daten werden erfasst, solange die Trace-Ausgabe aktiv ist. Um eine Überlastung des Arbeitsspeichers auf der Workstation mit LANconfig oder LANmonitor zu vermeiden, werden die Trace-Daten automatisch in eine Backup-Datei gespeichert. Die zeitlichen Intervalle und die maximale Größe einer Sicherungsdatei können Sie unter 'Extras / Sonstige Einstellungen / Tracebackup einstellen'.

2.2.4 Sichern und Wiederherstellen der Trace-Konfiguration

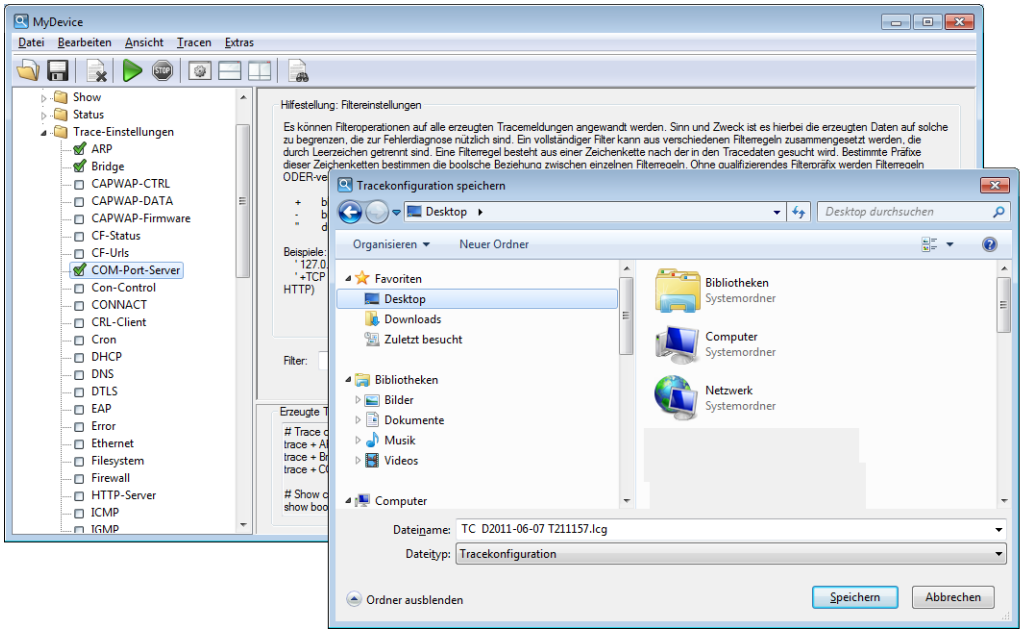
Zur späteren Wiederverwendung oder Weitergabe an einen anderen Benutzer kann die komplette Konfiguration der Trace-Ausgabe über 'Datei > Tracekonfiguration speichern' auf einen Datenträger geschrieben und später mit 'Datei > Tracekonfiguration laden' wieder geöffnet werden.



2.2.5 Sichern und Wiederherstellen der Trace-Daten

Auch die eigentlichen Trace-Daten können zur späteren Bearbeitung oder Weitergabe an einen anderen Benutzer über 'Datei > Tracedaten/Support-Konfigurationsdatei speichern' auf einen Datenträger geschrieben und später mit 'Datei > Tracedaten laden' wieder geöffnet werden.

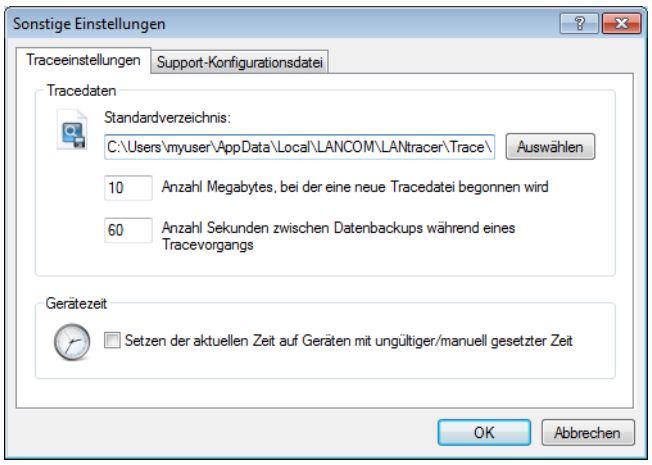
Alternativ können Sie auch die Schaltflächen  zum Laden oder  zum Speichern der Trace-Daten verwenden.



2.2.6 Backup-Einstellungen für die Traces

Beim Starten eines Traces über LANconfig oder LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Die Einstellungen für das Trace-Backup können Sie unter 'Extras / Sonstige Einstellungen / Tracebackup' vornehmen. Stellen Sie dabei die folgenden Parameter ein:

- Verzeichnis für die Trace-Backups
- Maximale Größe einer Trace-Backup-Datei. Wenn diese Größe mit einem aktiven Trace erreicht wird, wird automatisch eine weitere Trace-Backup-Datei angelegt.
- Speicherintervall der Trace-Backup-Datei. Wenn diese Zeit erreicht ist, wird automatisch eine aktualisierte Version der Trace-Backup-Datei gespeichert. In der Trace-Backup-Datei sind also die Informationen zwischen dem letzten Backup und dem aktuellen Zeitpunkt nicht enthalten.
- Zusätzlich kann die aktuelle Zeit der Workstation mit dem LANmonitor als Zeit für den Trace gesetzt werden, z. B. wenn das getracte Gerät selbst nicht über eine gültige Zeitinformation verfügt.



2.2.7 Traces filtern

Die Ausgabe von Traces an der Kommadozeile oder im Trace-Dialog von LCMS ist in vielen Fällen sehr umfangreich, weil der Trace in kurzer zeitlicher Abfolge Informationen aus dem Gerät empfängt. Um die Ausgabe der Traces übersichtlicher zu gestalten, können Sie geeignete Filter anwenden. Die Filter basieren auf einer Suchfunktion, welche die Trace-Ausgaben nach relevanten Informationen untersucht und nur die gewünschten Aspekte darstellt.

Im folgenden Beispiel aktiviert der Administrator einen einfachen IP-Router-Trace auf einem Gerät drei Internetanbindungen und verschickt Pings an verschiedene Ziele. Die ungefilterte Trace-Ausgabe zeigt alle Pakete, die der IP-Router des Gerätes verarbeitet:

```
root@MyDevice:/
> trace # ip-router
IP-Router ON

root@MyDevice:/

>[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cde
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1ccf
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1ccf
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cde
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1cea
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1cea
Route: LAN-1 Tx (INTRANET2):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cd0
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
```

```
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cdf
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cd0
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cdf
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1ceb
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1ceb
Route: LAN-1 Tx (INTRANET2):
```

Die Ausgabe von nur 2 Sekunden reicht schon aus, um eine recht große Menge an Daten zu erzeugen. Um die Ausgabe übersichtlicher zu gestalten, fügen Sie nach dem Trace-Kommando einen Filter an. Die Filter beginnen mit dem @-Zeichen und geben ein Suchkriterium an. In diesem Beispiel reduzieren Sie den Filter auf alle Ausgaben, in denen das Suchkriterium "Internet1" vorkommt, um nur die Pakete dieser Gegenstelle auszugeben.

Die Filter unterscheiden nicht zwischen Groß- und Kleinschreibung.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1

IP-Router ON @ INTERNET1

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfb
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfb
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfc
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfc
Route: LAN-1 Tx (INTRANET1):
```

Wieder beträgt der Zeitrahmen des Traces zwei Sekunden, die Menge an Daten wurde aber schon deutlich reduziert. Lediglich die Daten zur Gegenstelle „INTERNET1“ werden angezeigt. Es können aber auch noch weitere Filterkriterien angegeben werden indem einfach ein Leerzeichen zwischen dem ersten und zweiten Kriterium gesetzt werden. Zusätzlich zum Leerzeichen können sowohl „+“ als auch „-“ als Operatoren verwendet werden. Hierbei gilt, bei einem „+“ müssen beide Kriterien erfüllt sein, bei einem „-“ darf das Kriterium nicht erfüllt sein und bei einem Leerzeichen muss eines der verknüpften Kriterien erfüllt sein. Die Möglichkeit Strings, die Operatoren enthalten auch als Filter zu nutzen wird durch Anführungszeichen umgesetzt.

Wenn Sie mehrere Suchbegriffe verwenden möchten, trennen Sie die einzelnen Begriffe durch die folgenden Operatoren:

- Leerzeichen: Ein Leerzeichen vor einem Suchbegriff stellt eine logische ODER-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie eine der so markierten Zeichenketten enthält.
- +: Ein Pluszeichen vor einem Suchbegriff stellt eine logische UND-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie alle der so markierten Zeichenketten enthält.
- -: Ein Minuszeichen vor einem Suchbegriff stellt eine logische NICHT-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie keine der so markierten Zeichenketten enthält.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 -"echo request"

IP-Router ON @ INTERNET1 -"echo request"

[IP-Router] 2010/12/20 17:12:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0b
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:12:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0c
Route: LAN-1 Tx (INTRANET1):
```

Jetzt zeigt der Trace nur noch die Einträge an, welche die Gegenstelle 'INTERNET1' enthalten, die aber **nicht** die Zeichenkette 'echo request' enthalten. So reduzieren Sie die Anzeige auf die Antworten eines Pings, die von der entsprechenden Gegenstelle stammen.

Sie können zeitgleich mehrere Traces verwenden und nach unterschiedlichen Kriterien filtern. Im folgenden Beispiel läuft neben dem IP-Router Trace auch ein Ethernet Trace, um sich das zum Ping zugehörige Paket auf dem Ethernet anzuschauen.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 +"echo reply"
IP-Router ON @ INTERNET1 +"echo reply"

root@MyDevice:/
> trace # eth @ ICMP +“echo reply”
Ethernet ON @ icmp +"echo reply"

[IP-Router] 2010/12/21 14:17:21,000
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0002, seq: 0x2654
Route: LAN-1 Tx (INTRANET1):

[Ethernet] 2010/12/21 14:17:21,000
Sent 98 byte Ethernet packet via LAN-1:
HW Switch Port : ETH-1
-->IEEE 802.3 Header
Dest : 00:a0:57:12:a9:21 (LANCOM 12:a9:21)
Source : 00:a0:57:12:f7:81 (LANCOM 12:f7:81)
Type : IPv4
-->IPv4 Header
```

```
Version : 4
Header Length : 20
Type of service : (0x00) Precedence 0
Total length : 84
ID : 18080
Fragment : Offset 0
TTL : 59
Protocol : ICMP
Checksum : 24817 (OK)
Src Address : 11.11.11.1
Dest Address : 192.168.1.100
-->ICMP Header
Msg : echo reply
Checksum : 18796 (OK)
Body : 00 00 00 02 00 00 26 54 ......
 7e c9 6d 8c 00 00 00 00 ~.m.....
 00 01 02 03 04 05 06 07 ........
 08 09 0a 0b 0c 0d 0e 0f ........
 10 11 12 13 14 15 16 17 ........
 18 19 1a 1b 1c 1d 1e 1f ........
 20 21 22 23 24 25 26 27 !"#$%
```

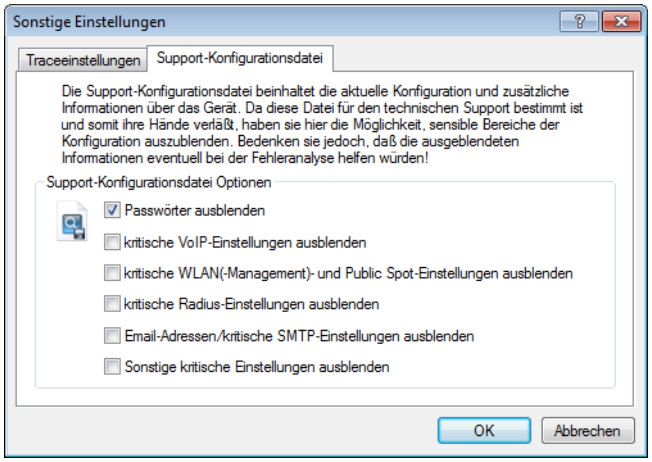
2.2.8 Support-Datei speichern

Mit einer Support-Datei können alle für den Support relevanten Informationen komfortabel in eine Datei geschrieben werden:

- Tracedaten wie in den aktuellen Einstellungen konfiguriert (wie mit der Funktion “Tracedaten speichern”)
- aktuelle Gerätekonfiguration
- Bootlog
- Sysinfo

Beim Speichern der Gerätekonfiguration können dabei sicherheitsrelevante Informationen, die für den Support nicht von Bedeutung sind, ausgeblendet werden. Im Trace-Fenster unter 'Extras / Sonstige Einstellungen / Supportfile' können Sie auswählen, welche Informationen nicht in der Support-Datei gespeichert werden sollen.

Die so erstellte Support-Datei enthält alle Informationen im Klartext. Sie können die Datei daher in einem Editor öffnen und auf ggf. noch vorhandene sensible Einträge prüfen.



2.3 LANCOM Software Update für LCMS

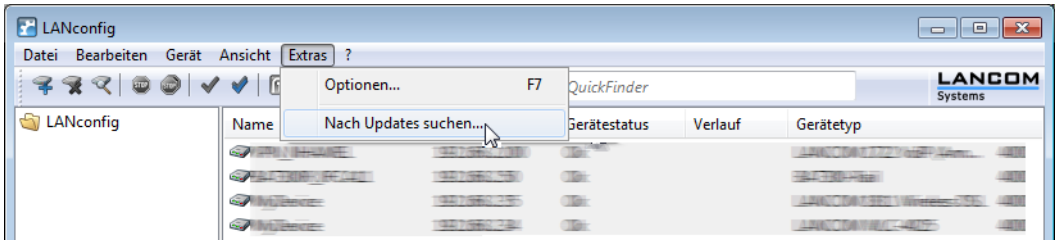
Das Software Update für LCMS bietet Ihnen neue Versionen von LCMS und der Firmware zu Ihren Geräten automatisch zum Download an.

Neue Versionen für LCMS (LANconfig und LANmonitor sowie WLANmonitor) laden Sie direkt aus dem frei zugänglichen Download-Bereich des LANCOM Web-Servers. Gerätespezifische Software wie neue Firmware-Versionen erfordern einen Account im Kunden-Portal myLANCOM.

2.3.1 Software Update manuell starten

Um das Software Update für LANconfig manuell zu starten gehen Sie vor wie in den folgenden Schritten beschrieben:

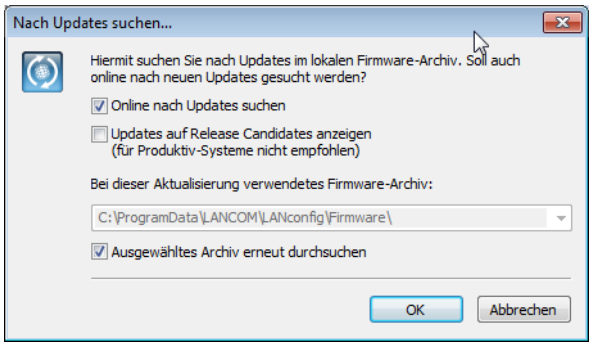
1. Starten Sie LANconfig.
2. Wählen Sie im Menü Extras den Eintrag 'Nach Updates suchen...'.



LANconfig sucht im lokalen Firmware-Archiv nach verfügbaren Updates. Optional können Sie die Suche um die folgenden Punkte erweitern:

- Suchen Sie online nach weiteren Updates im Download-Bereich des LANCOM Web-Servers.
- Beziehen Sie Release Candidates in die Suche ein. Wenn Sie diese Option einschalten, wird das Software Update nicht nur die für den Einsatz in Produktivumgebungen freigegebenen Software-Versionen zum Download anbieten, sondern auch die verfügbaren Release Candidates.

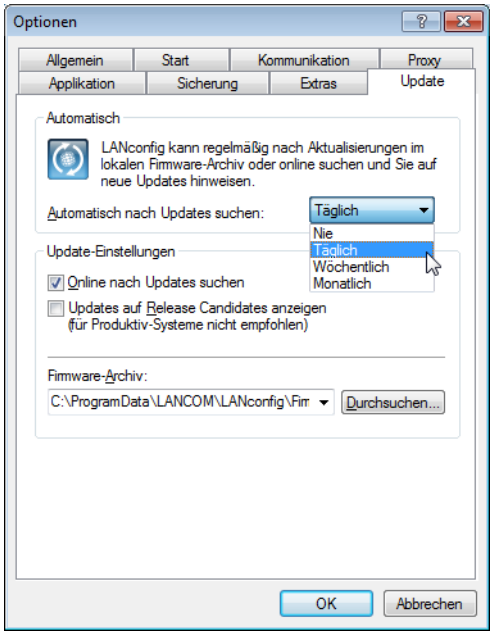
Release Candidates enthalten die neuen Features der kommenden Software-Version und sind ausführlich getestet. Bis zur endgültigen Freigabe der Version sind – u. a. aufgrund der Rückmeldungen der Anwender – noch weitere Optimierungen der Software möglich.



2.3.2 Einstellungen für die automatische Suche nach Updates

Um das Software Update für LANconfig bei jedem Start der Applikation automatisch zu starten gehen Sie vor wie in den folgenden Schritten beschrieben:

1. Starten Sie LANconfig.
2. Wählen Sie im Menü Extras den Eintrag 'Optionen'.
3. Wechseln Sie auf die Registerkarte 'Update'.



Konfigurieren Sie die folgenden Punkte für das automatische Update:

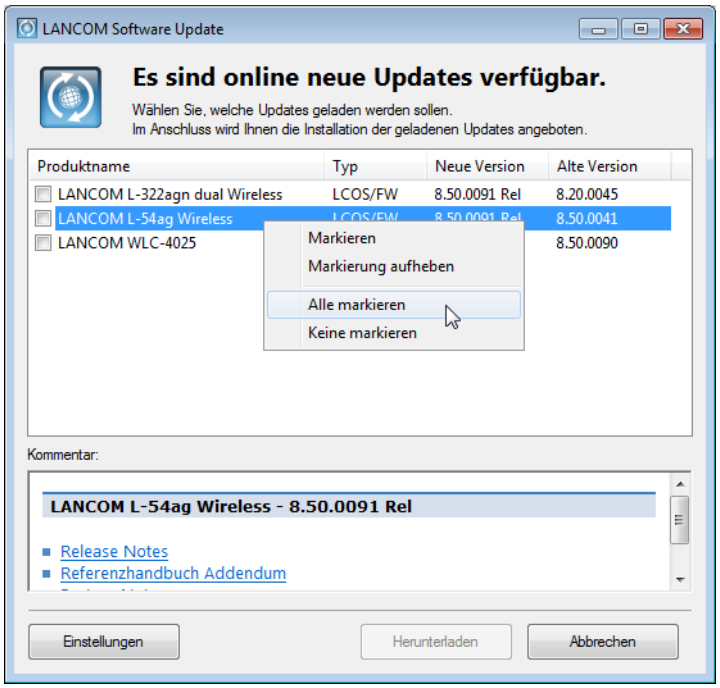
- Wählen Sie das zeitliche Intervall für die automatische Suche nach Updates (täglich, wöchentlich oder monatlich). Alternativ deaktivieren Sie die automatische Suche mit der Einstellung 'Nie'.
- Suchen Sie online nach weiteren Updates im Download-Bereich des LANCOM Web-Servers.
- Release Candidates enthalten die neuen Features der kommenden Software-Version und sind ausführlich getestet. Bis zur endgültigen Freigabe der Version sind – u. a. aufgrund der Rückmeldungen der Anwender – noch weitere Optimierungen der Software möglich.

  Beziehen Sie Release Candidates in die Suche ein. Wenn Sie diese Option einschalten, wird das Software Update nicht nur die für den Einsatz in Produktivumgebungen freigegebenen Software-Versionen zum Download anbieten, sondern auch die verfügbaren Release Candidates.
- Wählen Sie für das Firmware-Archiv einen geeigneten Speicherort. Das Firmware-Archiv hat die folgenden Funktionen:
  - LANconfig sucht bei der automatischen Suche nach Updates an diesem Speicherort nach neuen Versionen von LCMS und der Firmware.
  - LANCOM Software Update speichert die Updates vom Download-Bereich des LANCOM Web-Servers an diesem Speicherort.

2.3.3 Auswahl und Installation der verfügbaren Updates

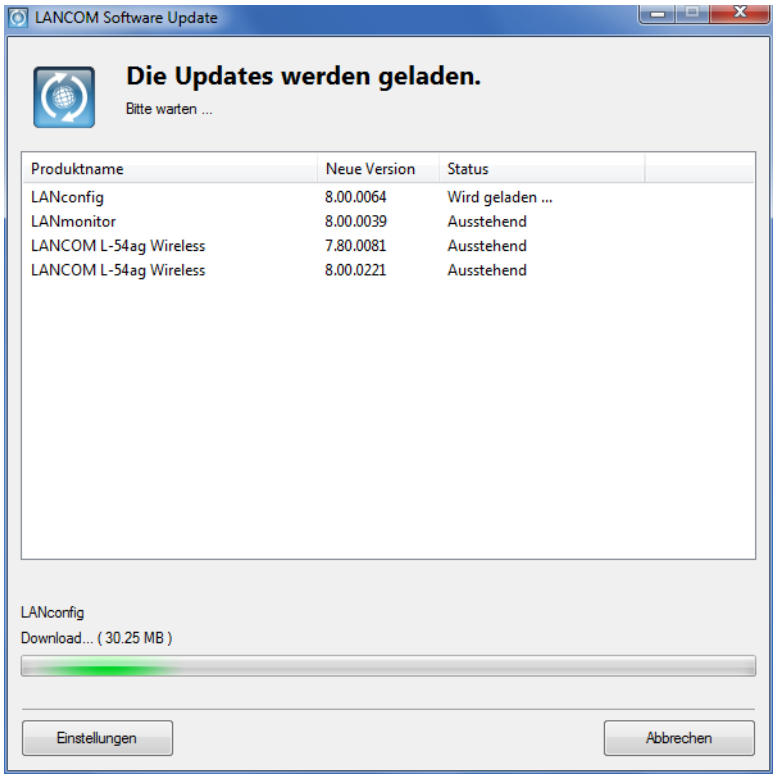
Nach einer erfolgreichen Verbindung zum Update-Server zeigt LANconfig die verfügbaren Updates an.

Wählen Sie die gewünschten Versionen aus und klicken Sie 'Herunterladen'. Klicken Sie alternativ mit der rechten Maustaste auf einen der Einträge und wählen Sie im Kontextmenü 'Alle markieren' oder 'Keine markieren'.

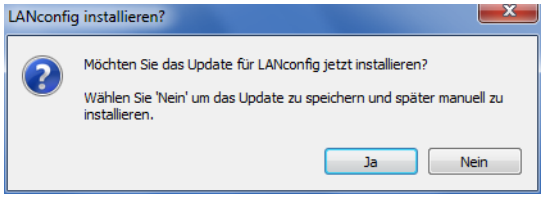


Bei der ersten Auswahl einer Firmware für den Download fordert das LANCOM Software Update Sie zur Eingabe Ihrer Zugangsdaten zu myLANCOM auf.

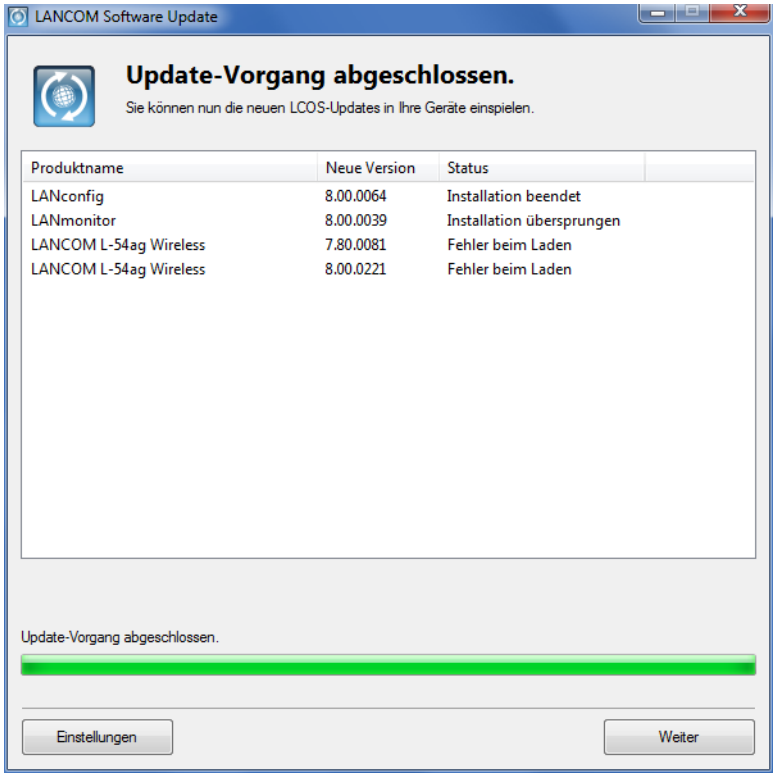
LANCOM Software Update lädt die gewählte Software nun nacheinander herunter und speichert die Dateien im Firmware-Archiv.



Nach dem erfolgreichen Download bietet LANCOM Software Update die Installation der geladenen Software an (nur LANconfig und LANmonitor):



Nach der Installation zeigt LANCOM Software Update die Ergebnisse des Updates-Vorgangs an:



2.3.4 Software Update über MyLANCOM

Für einige Funktionen benötigt das LANCOM Software Update einen Zugang zum Kunden-Portal myLANCOM.

Um die Zugangsdaten für myLANCOM einzutragen gehen Sie vor wie in den folgenden Schritten beschrieben:

1. Starten Sie LANconfig.
2. Wählen Sie im Menü Extras den Eintrag 'Online nach Updates suchen...'.
3. Klicken Sie im Dialog mit den Ergebnissen der Software Updates die Schaltfläche 'Einstellungen'.
4. Geben Sie im folgenden Dialog den Benutzernamen und das Passwort für den Zugang zu myLANCOM ein.

5 Aktivieren Sie auf Wunsch die Option 'Falls vorhanden, auf Release Candidates updaten'. Wenn Sie diese Option einschalten, wird das Software Update nicht nur die für den Einsatz in Produktivumgebungen freigegebenen Software-Versionen zum Download anbieten, sondern auch die verfügbaren Release Candidates.

2.4 Eingangsspannungsüberwachung für Geräte mit Weitbereichsnetzteil

Das in einige Modelle integrierte Weitbereichsnetzteil für zweipolige Industriestecker ermöglicht eine flexible Stromversorgung mit Spannungen von 10–28 Volt.

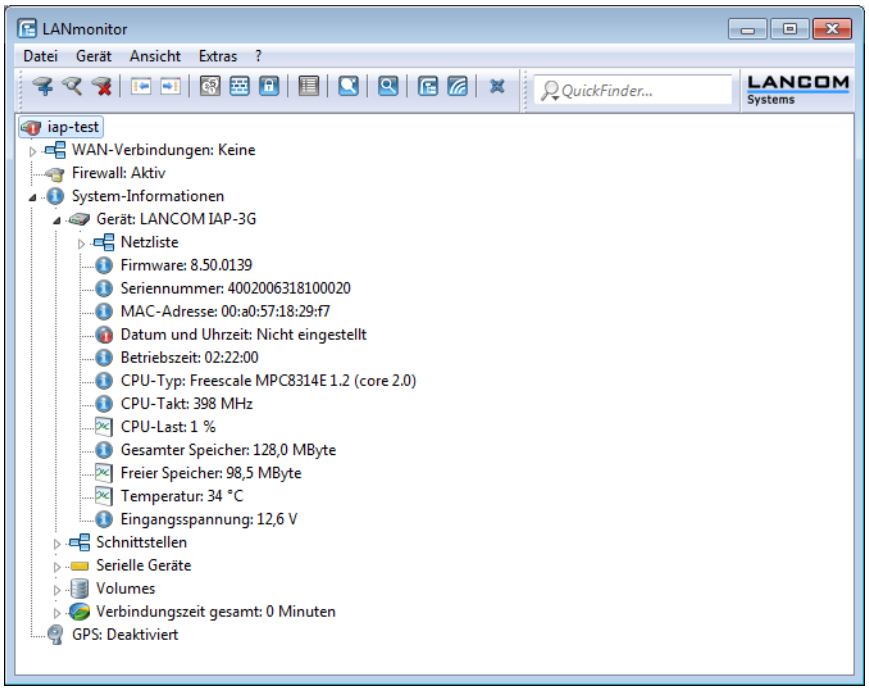
Um einen Ausfall (z. B. aufgrund sich entleerender Akkus) oder eine Beschädigung der Geräte zu vermeiden, überwachen diese Modelle regelmäßig die anliegende Spannung und melden das Über- und Unterschreiten des erlaubten Spannungsbereiches.

Die angezeigte Spannung stellt die aktuelle Eingangsspannung des integrierten Weitbereichsnetzteils dar. Für die Eingangsspannung gilt ein Minimalwert von 10 Volt und ein Maximalwert von 28 Volt. Wenn die aktuelle Eingangsspannung den erlaubten Bereich über- oder unterschreitet, meldet das Gerät die Abweichung per SNMP-Trap und als SYSLOG-Nachricht. Außerdem protokolliert der LANmonitor diese Zustände in der Geräteaktivitätsliste. Stellen Sie in diesem Fall sicher, dass die zulässige Eingangsspannung umgehend wieder hergestellt wird.

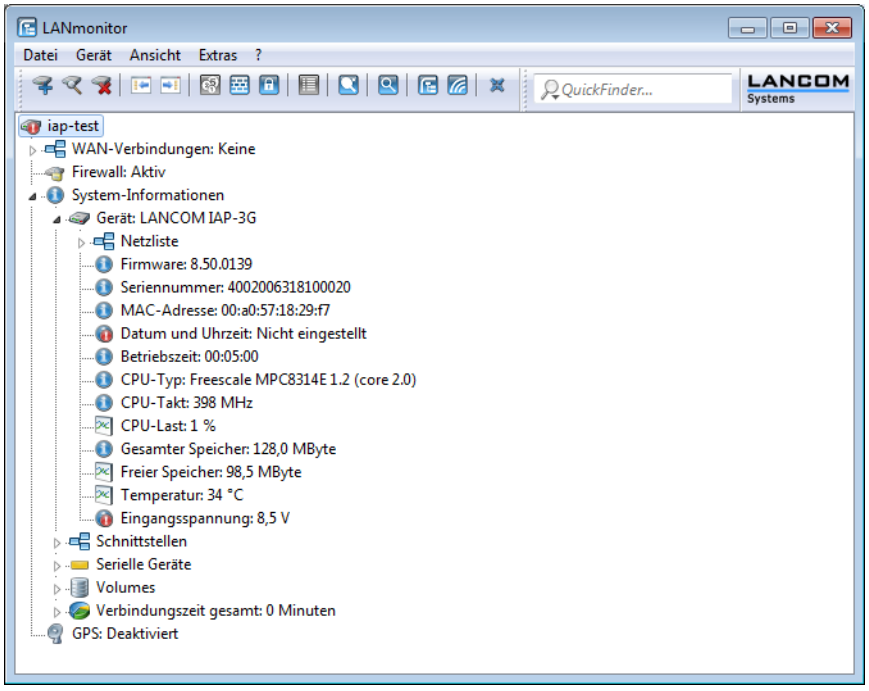
Konfigurieren Sie für das Gerät die erforderlichen SYSLOG-Server oder SNMP-Manager, um die Meldungen an die entsprechenden Monitoring-Systeme zu übertragen.

2.4.1 Anzeige im LANmonitor

Der LANmonitor zeigt die aktuelle Eingangsspannung im Bereich der System-Informationen an:

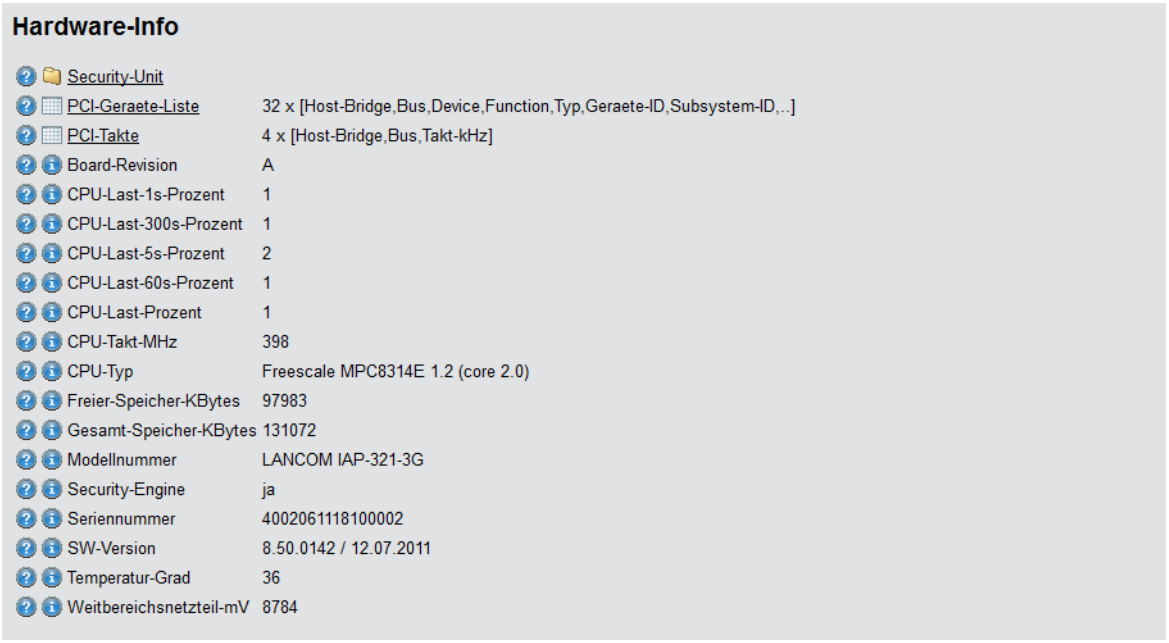


Im Fall einer Über- oder Unterschreitung des erlaubten Spannungsbereiches zeigt der LANmonitor ein entsprechendes Warnsymbol für die Eingangsspannung an:



2.4.2 Anzeige in Webconfig

Webconfig zeigt die aktuelle Eingangsspannung im Bereich der Hardware-Info an (Status > Hardware-Info > Weitbereichsnetzteil mV):



2.4.3 SNMP-Traps

Geräte mit Weitbereichsnetzteil melden das Über- und Unterschreiten des zulässigen Eingangsspannungsbereiches mit den folgenden SNMP-Traps:

- TRP_VOLTMON_OVERVOLT (4500): Dieser Trap zeigt an, dass die aktuelle Eingangsspannung den zulässigen Bereich überschreitet.
- TRP_VOLTMON_NO_OVERVOLT (4501): Dieser Trap zeigt an, dass die aktuelle Eingangsspannung nach einer Überschreitung der maximalen Spannung wieder in den zulässigen Bereich zurückgekehrt ist.
- TRP_VOLTMON_UNDERVOLT (4502): Dieser Trap zeigt an, dass die aktuelle Eingangsspannung den zulässigen Bereich unterschreitet.
- TRP_VOLTMON_NO_UNDERVOLT (4503): Dieser Trap zeigt an, dass die aktuelle Eingangsspannung nach einer Unterschreitung der minimalen Spannung wieder in den zulässigen Bereich zurückgekehrt ist.

Konfigurieren Sie für das Gerät die erforderlichen SNMP-Manager, um die Meldungen an die entsprechenden Monitoring-Systeme zu übertragen.

2.4.4 SYSLOG-Nachrichten

Geräte mit Weitbereichsnetzteil melden das Über- und Unterschreiten des zulässigen Eingangsspannungsbereiches mit den folgenden SYSLOG-Nachrichten:

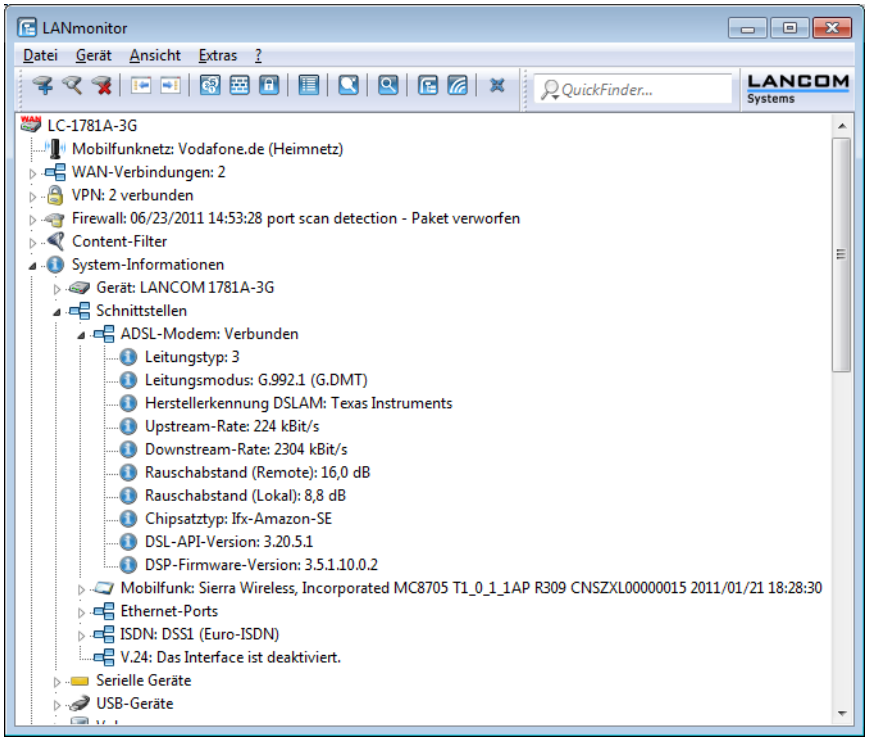
- Spannung über dem zulässigen Bereich: <aktuelle Eingangsspannung>: Diese SYSLOG-Nachricht zeigt an, dass die aktuelle Eingangsspannung den zulässigen Bereich überschreitet.
- Spannung wieder im zulässigen Bereich: <aktuelle Eingangsspannung>: Diese SYSLOG-Nachricht zeigt an, dass die aktuelle Eingangsspannung nach einer Über- oder Unterschreitung der zulässigen Spannung wieder in den zulässigen Bereich zurückgekehrt ist.

- Spannung unter dem zulässigen Bereich: <aktuelle Eingangsspannung>: Diese SYSLOG-Nachricht zeigt an, dass die aktuelle Eingangsspannung den zulässigen Bereich unterschreitet.

Konfigurieren Sie für das Gerät die erforderlichen SYSLOG-Server, um die Meldungen an die entsprechenden Monitoring-Systeme zu übertragen.

2.5 Aktuelles Protokoll für das ADSL-Interface anzeigen

Der LANmonitor zeigt für Geräte mit integriertem ADSL-Modem den aktuell verwendeten ADSL-Standard in den System-Informationen an.



3 LAN

3.1 Bandbreitenbeschränkung der LAN-Schnittstellen

3.1.1 Einleitung

Bei einem Gerät mit integriertem WLAN-Modul können Sie ein Bandbreitenlimit für einzelne LAN-Schnittstellen definieren. Die Tabelle der LAN-Schnittstellen bietet zur Konfiguration der Bandbreitenbeschränkung die entsprechenden Parameter.

3.1.2 Ergänzungen im Menüsystem

LAN-Schnittstellen

Dieses Menü enthält die Einstellungen für die LAN-Schnittstellen.

SNMP-ID: 2.23.21

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

Tx-Limit

Geben Sie hier das Bandbreitenlimit (kbit/s) in Senderichtung an. Der Wert 0 entspricht keinem Limit.

SNMP-ID: 2.23.21.8

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

Mögliche Werte:

- Maximal 10 numerische Zeichen

Default: 0

Diese Einstellung ist nur bei Geräten verfügbar, die über ein WLAN-Modul verfügen.

Rx-Limit

Geben Sie hier das Bandbreitenlimit (kbit/s) in Empfangsrichtung an. Der Wert 0 entspricht keinem Limit.

SNMP-ID: 2.23.21.9

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

Mögliche Werte:

- Maximal 10 numerische Zeichen

Default: 0

Diese Einstellung ist nur bei Geräten verfügbar, die über ein WLAN-Modul verfügen.

4 WLAN

4.1 WLAN Layer-3 Tunneling

4.1.1 Einleitung

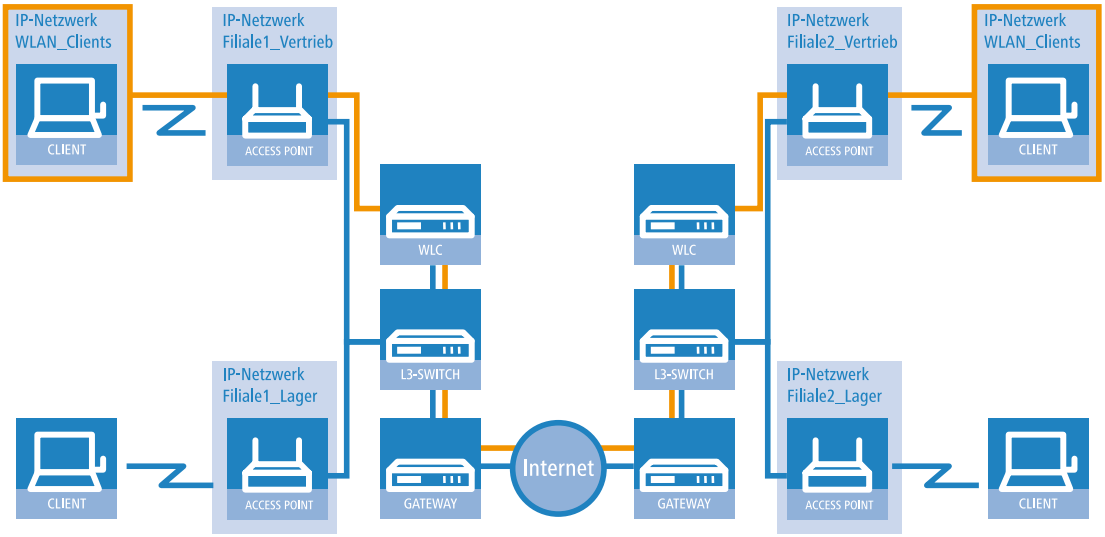
Der CAPWAP-Standard für das zentrale WLAN-Management bietet zwei verschiedene Übertragungskanäle an:

- Der obligatorische Kontrollkanal überträgt Verwaltungsdaten zwischen dem verwalteten Access Point und dem WLAN-Controller.
- Der optionale Datenkanal überträgt die Nutzdaten aus den jeweiligen WLAN-Netzwerken (SSID) zwischen dem verwalteten Access Point und dem WLAN-Controller.

Die optionale Nutzung des Datenkanals zwischen dem verwalteten Access Point und dem WLAN-Controller entscheidet über den Weg der Nutzdaten:

- Wenn Sie den Datenkanal deaktivieren, leitet der Access Point die Nutzdaten direkt in das LAN weiter. In diesem Fall steuern Sie die Zuordnung von WLAN-Clients zu bestimmten LAN-Segmenten z. B. über die Zuweisung von VLAN-IDs. Der Vorteil dieser Anwendung liegt vor allem in der geringen Belastung des Controllers und des gesamten Netzwerks, weil der Access Point ausschließlich die Verwaltungsdaten über den CAPWAP-Tunnel überträgt, während er die Nutzdaten auf dem kürzesten Weg überträgt.
- Wenn Sie den Datenkanal aktivieren, leitet der Access Point auch die Nutzdaten an den zentralen WLAN-Controller weiter. Dieser Ansatz hat folgende Vorteile:
  - Die Access Points können Netzwerke anbieten, die nur auf dem Controller verfügbar sind, z. B. einen zentralen Internetzugang für einen Public Spot.
  - Die von den Access Points angebotenen WLANs (SSIDs) sind auch ohne die Nutzung von VLAN voneinander separiert verfügbar. Der Verzicht auf VLAN reduziert den Aufwand für die Konfiguration der anderen Netzwerkkomponenten wie Switches etc.
  - Die an den Access Points in verschiedenen IP-Netzwerken angemeldeten WLAN-Clients können ohne Unterbrechung der IP-Verbindung zu einem anderen Access Point roamen, weil die Verbindung fortlaufen vom zentralen Controller verwaltet wird und nicht vom Access Point (Layer-3-Roaming).

Mit der Nutzung des Datenkanals entstehen auf der Basis der vorhandenen, physikalischen Netzwerkstruktur zusätzliche logische Netzwerke, die so genannten Overlay-Netzwerke.



Overlay-Netzwerk über mehrere IP-Netzwerke hinweg

Über den Datenkanal können Sie so sogar über mehrere WLAN-Controller hinweg logische Overlay-Netzwerke aufspannen.

Mehrere WLC innerhalb einer Broadcast-Domäne können das gleiche Overlay-Netzwerk unterstützen. Deaktivieren Sie den WLC-Datenkanal zwischen diesen Controllern. Der mehrfache Empfang der Broadcast-Nachrichten führt ansonsten zu Schleifen. Da Router die Broadcast-Nachrichten verwerfen, haben Sie für Controller in getrennten Netzen die Möglichkeit, den CAPWAP-Datenkanal zu aktivieren.

Die Access Points nutzen virtuelle WLC-Schnittstellen (WLC-Tunnel), um die Datenkanäle der jeweiligen SSIDs zwischen dem Access Point und dem WLAN-Controller zu verwalten. Jeder WLAN-Controller bietet je nach Modell 16 bis 32 WLC-Tunnel an, die Sie bei der Konfiguration der logischen WLANs nutzen können.

Die Geräte bieten die virtuellen WLC-Schnittstellen in allen Dialogen zur Auswahl von logischen Schnittstellen an (LAN oder WLAN), z. B. in den Port-Tabellen der LAN- und VLAN-Einstellungen oder bei der Definition von IP-Netzwerken.

4.1.2 Ergänzungen im Menüsystem

Multicast-Netzwerke

Diese Tabelle enthält die Einstellungen für die Übertragung von CAPWAP-Multicast-Paketen über die jeweiligen Bridge-Schnittstellen.

Wenn ein WLAN-Controller ein Broadcast- oder Multicast-Paket für ein Netzwerk einer SSID empfängt, so muss er dieses Paket an alle Access Points weiterleiten, welche die betreffende SSID anbieten. Der WLAN-Controller hat zwei Möglichkeiten, alle betroffenen Access Points zu erreichen:

- Der WLAN-Controller kopiert das Paket und sendet es als Unicast an die jeweiligen Access Points. Die Vervielfältigung der Pakete steigert die CPU-Last auf dem Controller und die benötigte Bandbreite, was sich besonders im Fall von WAN-Verbindungen negativ auf die Performance auswirkt.
- Der WLAN-Controller sendet das Paket als Multicast. In diesem Falle reicht in den meisten Fällen ein einziges Paket. Allerdings erreicht der Controller mit diesen Multicast-Paketen nur die Access Points in der eigenen Broadcast-Domäne. Access Points, die über eine geroutete WAN-Strecke angebunden sind, können diese Multicast-Pakete des Controllers in der Regel nicht empfangen.

Die Weiterleitung der Multicast-Pakete ist abhängig von den verwendeten Routern auf der WAN-Strecke.

Der WLAN-Controller versendet regelmäßig Keep-Alive-Multicast-Pakete an die Multicast-Gruppe. Wenn ein Access Point diese Pakete beantwortet, kann der Controller diesen Access Point über Multicast-Pakete erreichen. Für alle anderen Access Points kopiert der Controller die bei ihm eingehenden Multicast-Pakete und versendet sie als Unicast an die entsprechenden Access Points.

Wenn die Übertragung von CAPWAP-Multicast-Paketen aktiviert ist und für die Bridge-Schnittstelle eine gültige Multicast-IP-Adresse mit Port definiert ist, sendet das Gerät die eingehenden Broadcast- und Multicast-Pakete als Multicast weiter an diese Adresse.

Bei der Aktivierung von Multicast schalten die Geräte auch implizit das IGMP Snooping ein, welches die Informationen über die Multicast-Struktur aktuell hält.

In Anwendungen mit mehreren WLAN-Controllern führen Multicast-Pakete möglicherweise zu Schleifen. Um Schleifen durch Multicasts bei Verwendung der Bridge zu vermeiden nutzt der WLAN-Controller die folgenden Maßnahmen:

- Der WLAN-Controller unterstützt im WLC-Datentunnel keine Multicast-Pakete und überträgt die Pakete als Unicast.
- Der WLAN-Controller leitet keine Pakete weiter, die eine CAPWAP-Multicast-Adresse als Empfänger tragen.
- Der WLAN-Controller aktiviert automatisch IGMP-Snooping auf allen verwalteten Access Points, wenn CAPWAP selbst Multicast verwendet.

Bridge-Schnittstelle

Wählen Sie hier eine Bridge-Schnittstelle für die Multicast-Einstellungen aus.

SNMP-ID: 2.37.1.14.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Auswahl aus einer der definierten Bridge-Schnittstellen

Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von CAPWAP-Multicast-Paketen für diese Bridge-Schnittstelle.

SNMP-ID: 2.37.1.14.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- ja
- nein

Default: nein

Multicast-Adresse

Wählen Sie hier eine IP-Adresse, an welche das Gerät für die gewählte Bridge-Schnittstelle die CAPWAP-Multicast-Pakete übermittelt.

SNMP-ID: 2.37.1.14.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Maximal 15 Zeichen zur Definition einer gültigen IP-Adresse

Default: 233.252.124.1 bis 233.252.124.32 (IP-Adressen aus dem nicht zugewiesenen Bereich)

Multicast-Port

Wählen Sie hier einen Port für die Übertragung von CAPWAP-Multicast-Paketen über die gewählte Bridge-Schnittstelle.

SNMP-ID: 2.37.1.14.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Maximal 5 Ziffern zur Bezeichnung einer gültigen Port-Nummer

Default: 20000 bis 20031

Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.37.1.14.5

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

Default: 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

WLC-Cluster

Dieses Menü enthält die Einstellungen für die Datenverbindungen und Statusverbindungen zwischen mehreren WLAN-Controllern.

SNMP-ID: 2.37.34

Pfad Telnet: /Setup/WLAN-Management

WLC-Daten-Tunnel-aktiviert

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von Datentunneln zwischen mehreren WLAN-Controllern.

SNMP-ID: 2.37.34.2

Pfad Telnet: /Setup/WLAN-Management

Mögliche Werte:

- ja
- nein

Default: nein

WLC-Discovery

In dieser Tabelle können Sie für jedes IP-Netzwerk separat die automatische Suche nach weiteren WLCs aktivieren oder deaktivieren.

SNMP-ID: 2.37.34.4

Pfad Telnet: /Setup/WLAN-Management/WLC-Cluster

Netzwerk

Wählen Sie hier eines der im Gerät definierten IP-Netzwerke aus, für welches Sie die automatische Suche nach weiteren WLAN-Controllern einstellen möchten.

SNMP-ID: 2.37.34.4.1

Pfad Telnet: /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery

Mögliche Werte:

- Auswahl aus der Liste der definierten IP-Netzwerke, maximal 16 Zeichen.
- nein

Default: INTRANET: nein, DMZ: nein

Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie die automatische Suche nach anderen WLAN-Controllern in dem ausgewählten IP-Netzwerk.

SNMP-ID: 2.37.34.4.2

Pfad Telnet: /Setup/WLAN-Management/WLC-Cluster/WLC-Discovery

Mögliche Werte:

- ja
- nein

Default: INTRANET: ja, DMZ: nein

Die automatische Suche nach anderen WLAN-Controllern ist eine Möglichkeit für den Verbindungsaufbau zwischen zwei WLCs. Wenn Sie diese Option deaktivieren, kann der WLAN-Controller über dieses Netzwerk keine Verbindung zu einem anderen WLC automatisch aufbauen. Alternativ können Sie die gewünschten Gegenstellen in der statischen WLC-Liste definieren.

Statische WLC Liste

In dieser Tabelle können Sie weitere WLAN-Controller als Gegenstellen definieren, zu denen eine Verbindung aufgebaut werden kann. Der Controller baut zunächst einen Kontroll-Tunnel zu dieser Gegenstelle auf. Wenn Sie die Option für den Datentunnel aktiviert haben, baut der Controller anschließend automatisch einen Daten-Tunnel zu dieser Gegenstelle auf.

SNMP-ID: 2.37.34.3

Pfad Telnet: /Setup/WLAN-Management/WLC-Cluster

IP-Adresse

Definieren Sie hier die IP-Adresse eines weiteren WLAN-Controllers, zu dem der konfigurierte Controller einen Daten-Tunnel aufbauen kann.

SNMP-ID: 2.37.34.3.1

Pfad Telnet: /Setup/WLAN-Management/WLC-Cluster/Statische WLC Liste

Die beiden WLAN-Controller können nur dann eine Verbindung aufbauen, wenn die Geräte die folgenden Voraussetzungen erfüllen:

- Sie haben die jeweilige Gegenstelle in beiden Geräten statisch oder über die automatische Suche definiert.
- Die beiden Controller verfügen über ein Zertifikat der gleichen CA.

Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.37.34.3.2

Pfad Telnet: /Setup/WLAN-Management/WLC-Cluster/Statische WLC Liste

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

Default: 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

Netzwerkprofile

Hier definieren Sie die logischen WLAN-Netzwerke, die auf den angemeldeten Access-Points (APs) aktiviert und betrieben werden können.

SNMP-ID: 2.37.1.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

VLAN-Id

Stellen Sie hier die VLAN-ID für dieses logische WLAN-Netzwerk ein. Der Access Point überträgt die Daten aus diesem WLAN-Netzwerk (SSID) mit der hier eingestellten VLAN-ID, wenn der VLAN-Modus auf 'tagged' eingestellt ist.

SNMP-ID: 2.37.1.1.34

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 2 bis 4094

Default: 2

Inter-Stations-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Stellen Sie für jedes logische WLAN separat ein, ob die Clients in dieser SSID untereinander Daten austauschen können.

SNMP-ID: 2.37.1.1.33

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Ja
- Nein

Default: Ja

Verbinde-SSID-mit

Stellen Sie hier ein, an welche logische Schnittstelle der Access Point die Nutzdaten aus diesem WLAN-Netzwerk (SSID) überträgt.

SNMP-ID: 2.37.1.1.32

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- LAN: Der Access Point leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an die eigene lokale LAN-Schnittstelle weiter. Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen direkt auf dem Access Point, z. B. durch einen separaten Internet-Zugang.
- WLC-Tunnel-1 bis WLC-Tunnel-x (modellabhängig): Der Access Point leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an eine der virtuellen Schnittstellen für den WLAN-Controller weiter (WLC-Tunnel). Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen zentral auf dem WLAN-Controller, z. B. durch einen gemeinsam genutzten Internet-Zugang.

Default: LAN

Die Weiterleitung der Nutzdaten aus mehreren SSIDs an den WLAN-Controller steigert die CPU-Last und die benötigte Bandbreite der zentralen Geräte. Berücksichtigen Sie die erforderlichen Leistungswerte beim zentralen WLAN-Management mit Layer-3-Tunneling.

Sie können für jeden Access Point bis zu 7 SSIDs mit einem WLC-Tunnel verbinden. Der WLAN-Controller verbindet auf dem jeweiligen Access Point den WLC-Tunnel und damit die verbundene SSID mit einer freien Bridge-Gruppe. Da eine der verfügbaren 8 Bridge-Gruppen für andere Zwecke reserviert ist, verbleiben 7 Bridge-Gruppen für die Zuordnung der WC-Tunnel.

VLAN-Modus

Wählen Sie hier die VLAN-Modus für dieses WLAN-Netzwerks (SSID) aus.

SNMP-ID: 2.37.1.1.30

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- tagged: Der Access Point markiert die Pakete dieser SSID mit der unter *2.37.1.1.34 VLAN-Id* konfigurierten ID.
- untagged: Der Access Point leitet die Pakete dieser SSID ohne zusätzliche VLAN-ID weiter.

Default: untagged

Der Access Point verwendet die VLAN-Einstellungen für das logische WLAN nur dann, wenn Sie das VLAN-Modul des Access Points in den physikalischen WLAN-Parametern aktivieren. Mit der Einstellung 'untagged' für ein spezielles WLAN können Sie auch bei aktiviertem VLAN ein WLAN ohne VLAN betreiben.

Radioprofile

Hier definieren Sie physikalische WLAN-Parameter, die auf allen logischen WLAN-Netzen eines gemanagten Access-Points gemeinsam gelten.

SNMP-ID: 2.37.1.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

VLAN-Modul-der-verwalteten-APs-aktivieren

Aktivieren oder deaktivieren Sie hier das VLAN-Modul der verwalteten Access Points. Ist das VLAN aus, dann werden alle VLAN-Einstellungen in den logischen Netzen ignoriert.

SNMP-ID: 2.37.1.2.17

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- ja
- nein

Default: nein

Mgmt-VLAN-ID

VLAN-ID für das Management-Netzwerk. Mit der Management-VLAN-ID wird das Management-Netzwerk getaggt, auf dem der WLAN-Controller mit den Access Points kommuniziert. VLAN wird nur benutzt, wenn das VLAN-Modul des APs aktiviert ist. Das Mangement-Netzwerk kann trotz aktiviertem VLAN auch ungetaggt betrieben werden, indem die entsprechende Einstellung für den Managment-VLAN-Modus gewählt wird. Hierzu wird intern die VLAN-ID '1' reserviert.

SNMP-ID: 2.37.1.2.19

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- 2 bis 4094

Default: 2

Mgmt-VLAN-Modus

VLAN-Modus für das Management-Netzwerk. VLAN wird nur benutzt, wenn das VLAN-Modul des Access Points aktiviert ist. Das Management-Netzwerk kann trotz aktiviertem VLAN auch ungetaggt betrieben werden.

SNMP-ID: 2.37.1.2.18

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- untagged: Die Management-Pakete des Access Points werden nicht mit einer VLAN-ID markiert.
- tagged: Die Management-Pakete des Access Points werden mit der als Management-VLAN-ID in diesem Radioprofil konfigurierten VLAN-ID markiert.

Default: untagged

DSCP-für-Kontrollpakete

Wählen Sie hier die passende Einstellung für die Priorisierung der Kontrollpakete über DiffServ (Differentiated Services) aus.

SNMP-ID: 2.37.1.12

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

Mögliche Werte:

- Best-Effort

- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited-Forwarding

Default: Best-Effort

DSCP-für-Datenpakete

Wählen Sie hier die passende Einstellung für die Priorisierung der Datenpakete über DiffServ (Differentiated Services) aus.

SNMP-ID: 2.37.1.13

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

Mögliche Werte:

- Best-Effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited-Forwarding

Default: Best-Effort

4.1.3 Tutorials

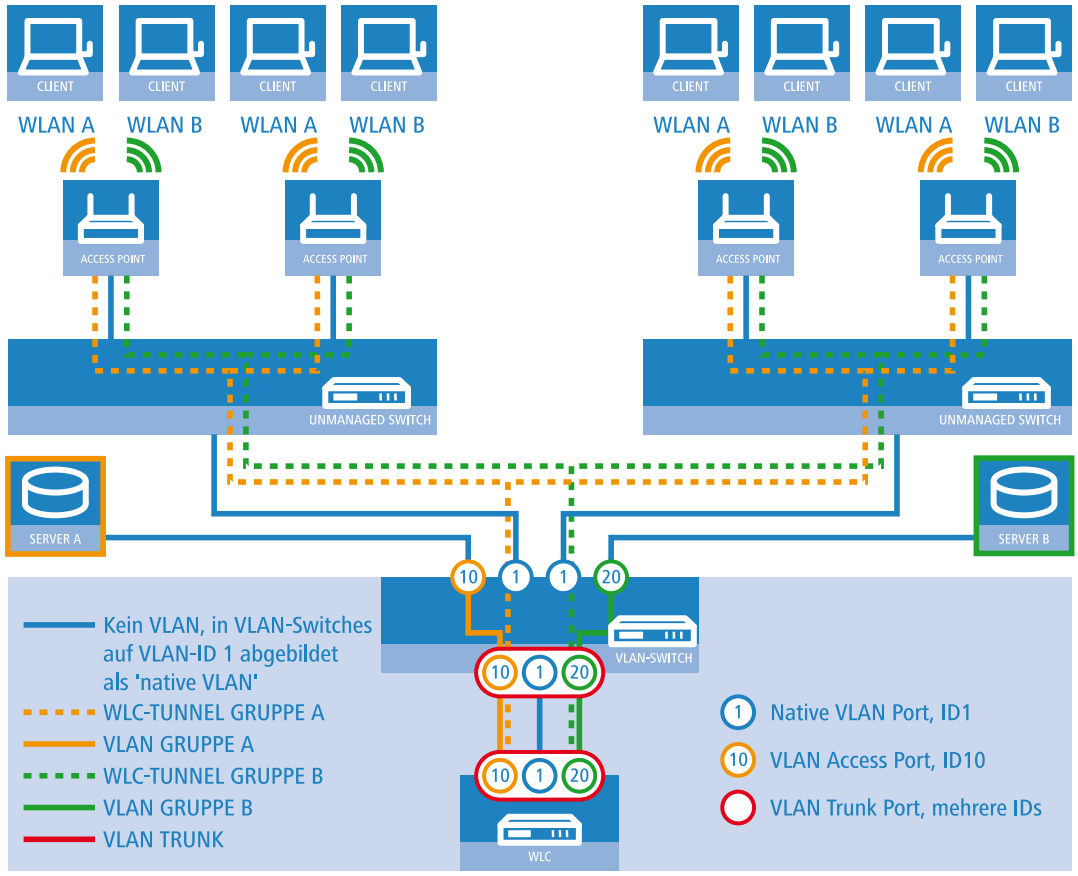
In den folgenden Abschnitten finden Sie konkrete Szenarien mit Schritt-für-Schritt Anleitungen für eine Reihe von Standard-Szenarien beim Einsatz von WLAN Controllern.

"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLAN-Controller können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die Access Points die Nutzdaten der angeschlossenen WLAN-Clients direkt zum Controller, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den Controller und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.



Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

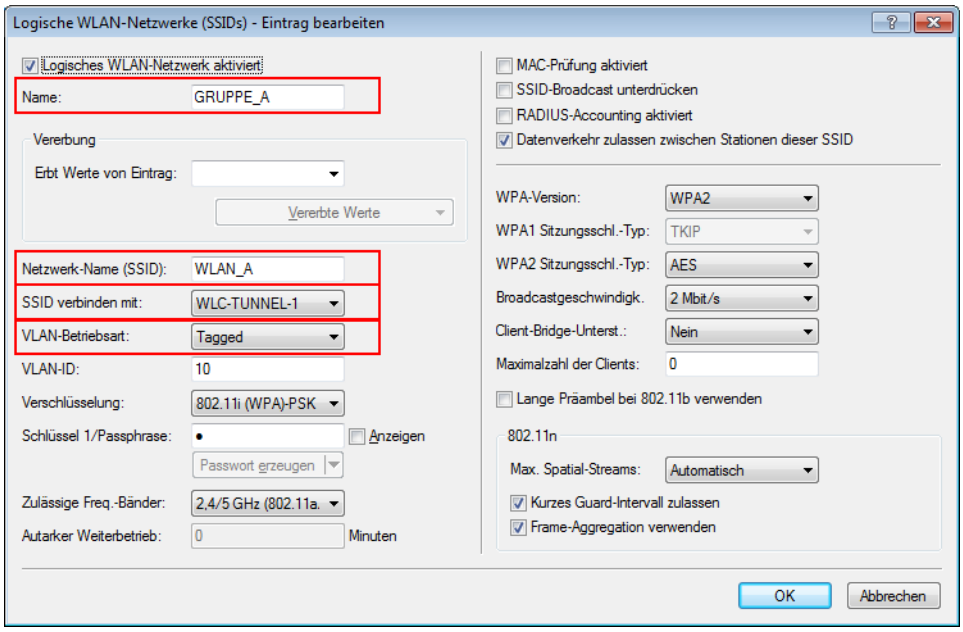
- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere Access Points, angeschlossen an den jeweiligen Switch.
- Jeder Access Point bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLAN-Controller verwaltet alle Access Points in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLAN-Controller.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten Access Point und unabhängig vom Segment, in dem er sich gerade befindet.

Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLAN-Controllers. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

Konfiguration der WLAN-Einstellungen

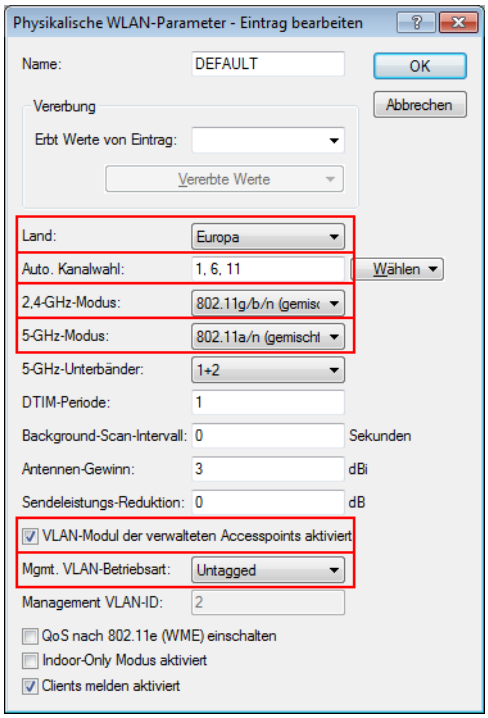
1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter Konfiguration/WLAN-Controller/Profile/Logische WLAN-Netzwerke (SSIDs).



Logische WLAN-Netze für Overlay-Netze

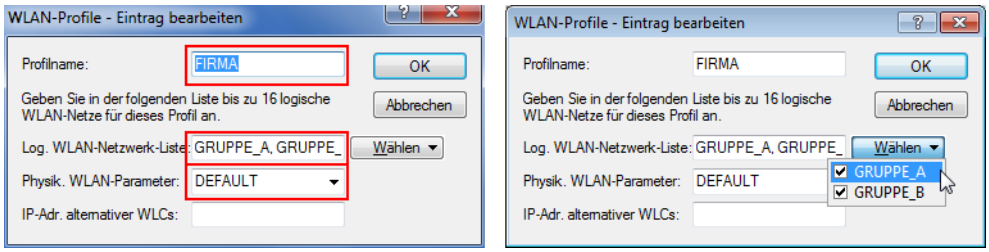
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre Access Points, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den Access Points einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den Access Points auf

'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter Konfiguration/WLAN-Controller/Profile/Physikalische WLAN-Parameter.



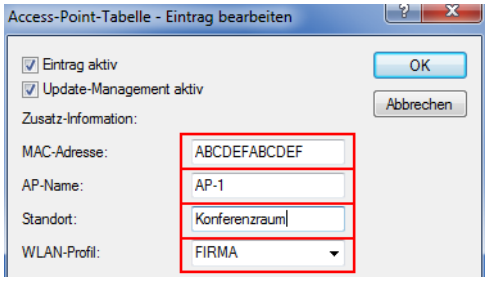
Physikalische WLAN-Parameter für Overlay-Netze

3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter Konfiguration/WLAN-Controller/Profile/Physikalische WLAN-Profile.



WLAN-Profile für Overlay-Netze

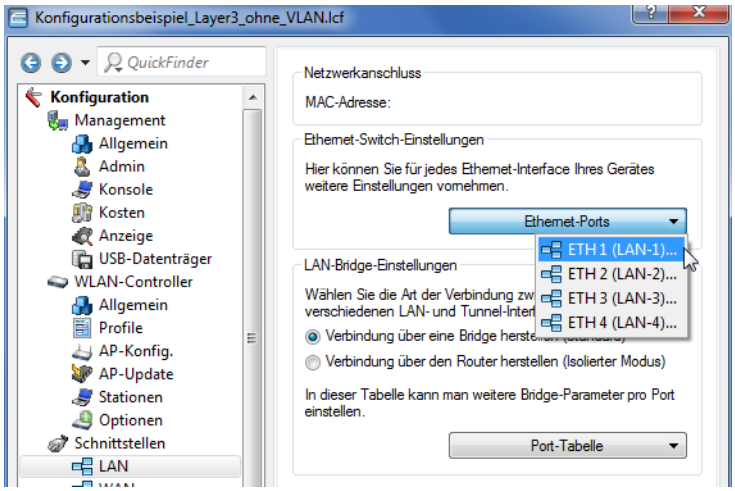
4. Erstellen Sie für jeden verwalteten Access Point einen Eintrag in der Access-Point-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem Access Point das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter Konfiguration/WLAN-Controller/AP-Konfig/Access-Point-Tabelle.



Access-Point-Tabelle für Overlay-Netze

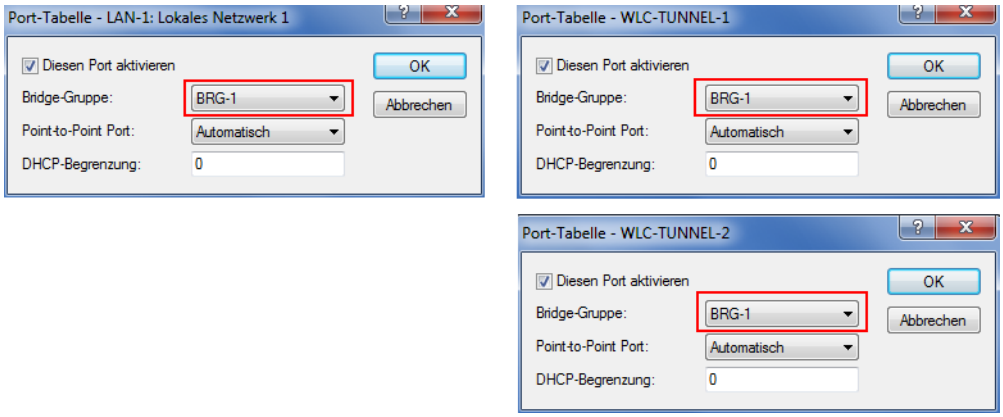
Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter Konfiguration/Schnittstellen/LAN/Ethernet-Ports.



Ethernet-Einstellungen für Overlay-Netze

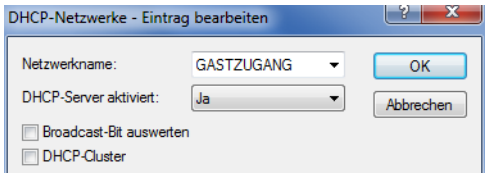
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter Konfiguration/Schnittstellen/LAN/Port-Tabelle.



Port-Einstellungen für Overlay-Netze

Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Der WLAN-Controller kann optional als DHCP-Server für die Access Points fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter Konfiguration/TCP/DHCP/DHCP-Netzwerke.

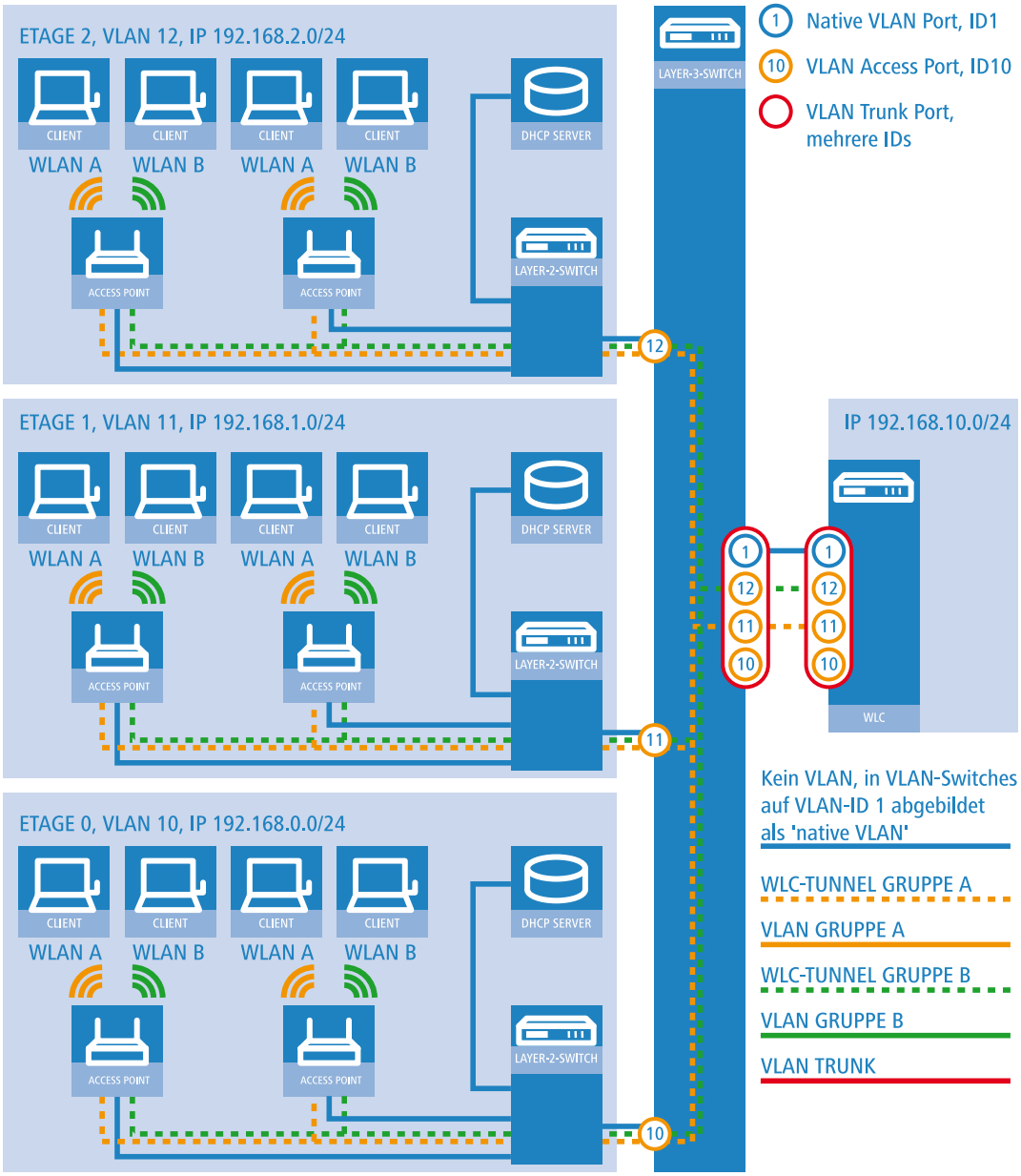


DHCP-Netzwerk für Overlay-Netze

"Layer-3-Roaming"

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum Controller ermöglicht das Roaming auch über die Grenzen von Broadcast-Domänen hinweg. In diesem Anwendungsbeispiel verhindert ein Layer-3-Switch zwischen den Etagen die Weiterleitung der Broadcasts und trennt so die Broadcast-Domänen.

In diesem Beispiel haben zwei Benutzergruppen A und B jeweils Zugang zu einem eigenen WLAN (SSID). Die Access Points in mehreren Etagen des Gebäudes bieten die beiden SSIDs 'GRUPPE_A' und 'GRUPPE_B' an.



Anwendungsbeispiel Layer-3-Roaming

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus 3 Segmenten in separaten Etagen eines Gebäudes.
- Ein zentraler Layer-3-Switch verbindet die Segmente und teilt das Netzwerk in 3 Broadcast-Domänen auf.
- Jedes Segment nutzt einen eigenen IP-Adressbereich und ein eigenes VLAN.
- In jedem Segment arbeitet ein lokaler DHCP-Server, der den Access Points die folgenden Informationen übermittelt:
  - IP-Adresse des Gateways
  - IP-Adresse des DNS-Servers
  - Domänen-Suffix

Die Bereitstellung dieser Informationen ermöglicht es den Access Points, Kontakt mit dem WLC-Controller in einer anderen Broadcast-Domäne aufzunehmen.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll beim Wechsel der Etage nahtlos Zugang zu "seinem" WLAN behalten – unabhängig vom verwendeten Access Point und unabhängig vom Segment, in dem er sich gerade befindet. Da die Segmente in diesem Beispiel unterschiedliche IP-Adresskreise nutzen, gelingt das nur durch die Verwaltung der Access Points auf Layer 3 direkt über den zentralen WLAN-Controller über die Grenzen der VLANs hinweg.

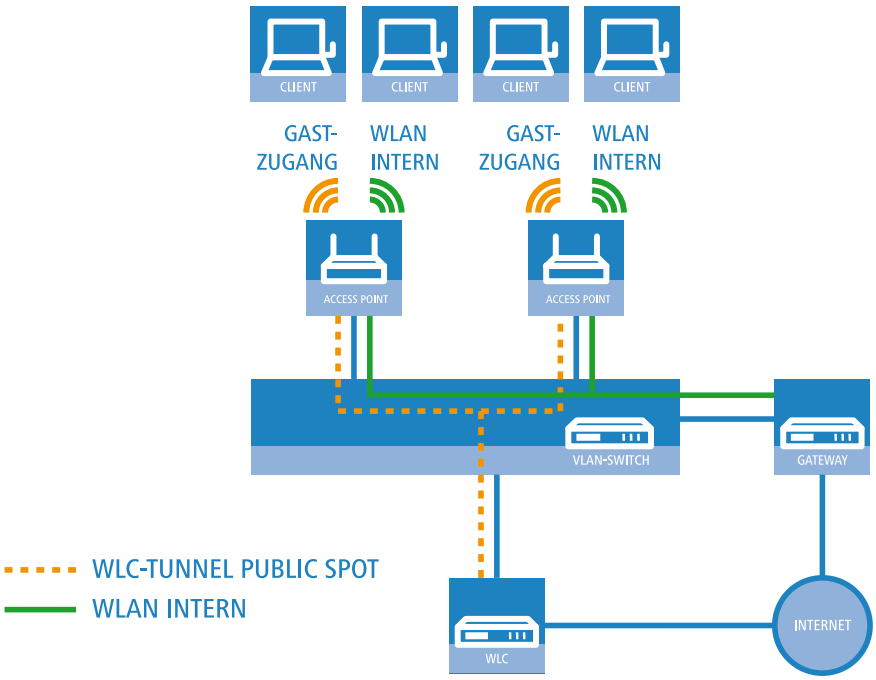
Die Konfiguration entspricht dem Beispiel *"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN* auf Seite 45.

WLAN-Controller mit Public Spot

Dieses Szenario basiert auf dem ersten Szenrio (Overlay Netzwerk) und erweitert es um spezifische Einstellungen für eine Benutzer-Authentifizierung.

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum Controller ermöglicht eine besonders einfache Konfiguration von Public Spots z. B. für Gäste parallel zu einem intern genutzten WLAN.

In diesem Beispiel haben die Mitarbeiter einer Firma Zugang zu einem eigenen WLAN (SSID), die Gäste erhalten über einen Public Spot ebenfalls Zugang zum Internet. Die Access Points in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.

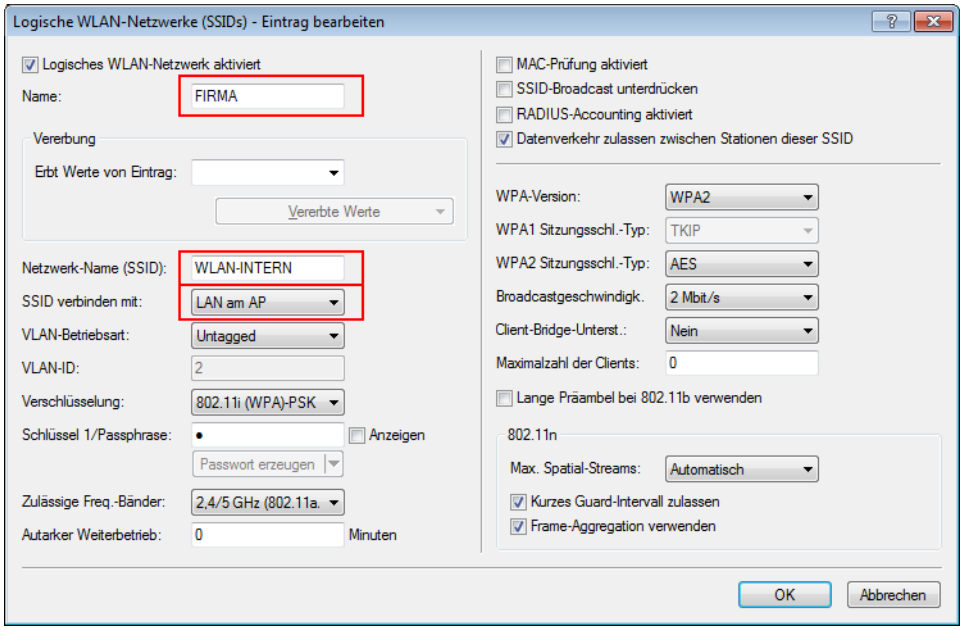


Anwendungsbeispiel WLAN-Controller mit Public Spot

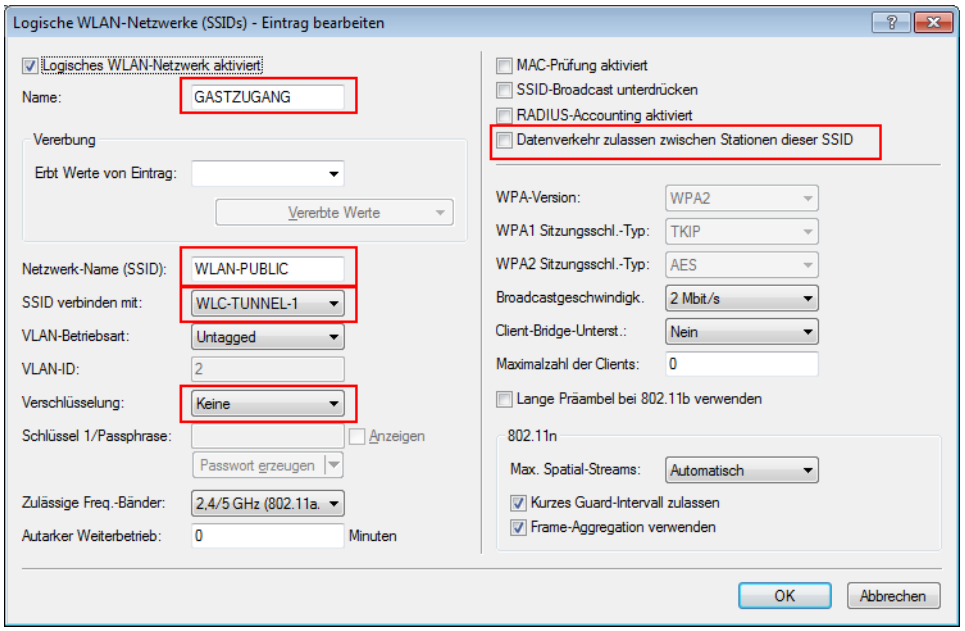
Das Ziel der Konfiguration: Ein WLAN-Client, der sich an der internen SSID anmeldet, soll Zugang zu allen internen Ressourcen und zum Internet über das zentrale Gateway erhalten. Die Access Points koppelt die Nutzdaten der internen Clients lokal aus und leiten sie direkt in das LAN weiter. Die WLAN-Clients der Gäste melden sich am Public Spot an. Die Access Points leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLAN-Controller, der über eine separate WAN-Schnittstelle Zugang zum Internet ermöglicht.

1. Erstellen Sie für das interne WLAN und das Gäste-WLAN jeweils einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie die SSID für die interne Nutzung mit dem

'LAN am AP', die SSID für die Gäste mit z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästenetzwerk die Verschlüsselung, damit sich die WLAN-Clients der Gäste beim Public Spot anmelden können. Unterbinden Sie für diese SSID außerdem den Datenverkehr der Stationen untereinander (Interstation-Traffic). In LANconfig finden Sie diese Einstellung unter Konfiguration/WLAN-Controller/Profile/Logische WLAN-Netzwerke (SSIDs).



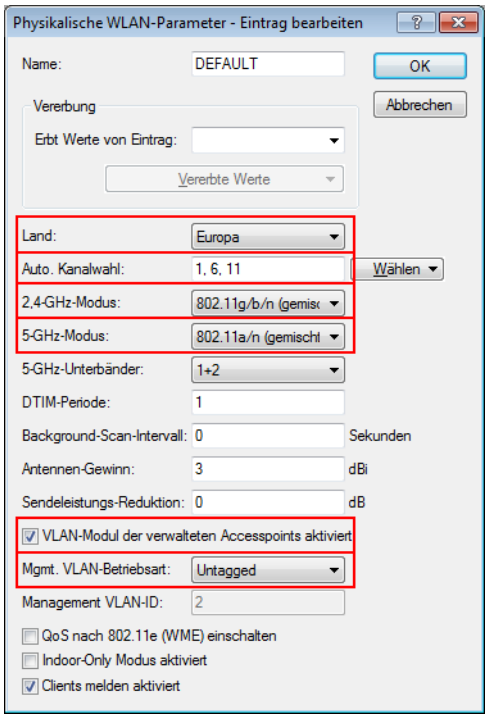
Logische WLAN-Netze für interne Nutzung



Logische WLAN-Netze für den Gastzugang

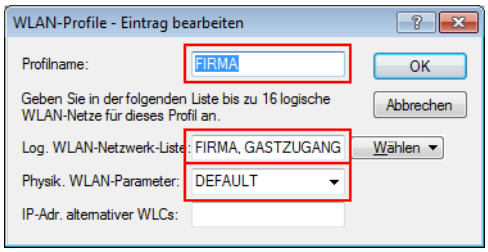
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre Access Points, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten

Modus. In LANconfig finden Sie diese Einstellung unter Konfiguration/WLAN-Controller/Profile/Physikalische WLAN-Parameter.



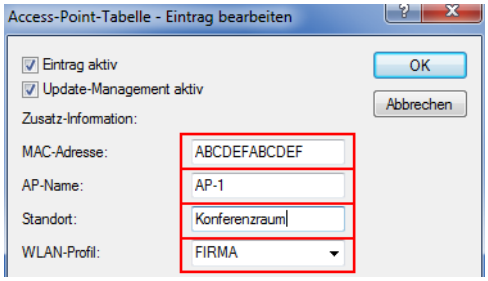
Physikalische WLAN-Parameter für Public-Spot-APs

3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellung unter Konfiguration/WLAN-Controller/Profile/Physikalische WLAN-Profile.



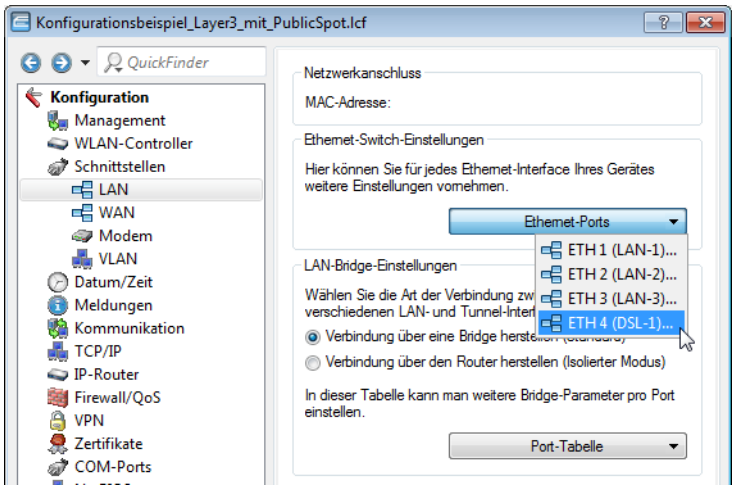
WLAN-Profile für Public-Spot-APs

4. Erstellen Sie für jeden verwalteten Access Point einen Eintrag in der Access-Point-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem Access Point das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellung unter Konfiguration/WLAN-Controller/AP-Konfig/Access-Point-Tabelle.



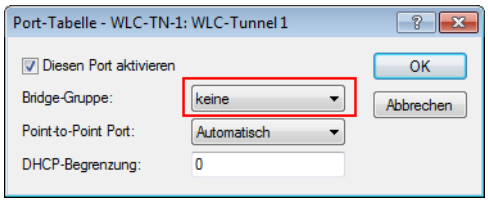
Access-Point-Tabelle für Public-Spot-APs

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie den 4. Ethernet-Port auf die logische LAN-Schnittstelle 'DSL-1' ein. Der WLAN-Controller verwendet diese LAN-Schnittstelle später für den Internetzugang des Gästenetzes. In LANconfig finden Sie diese Einstellung unter Konfiguration/Schnittstellen/LAN/Ethernet-Ports.



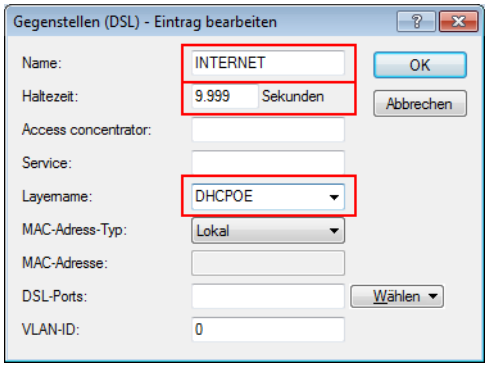
Ethernet-Einstellungen für Public-Spot-APs

6. Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public-Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter Konfiguration/Schnittstellen/LAN/Port-Tabelle.



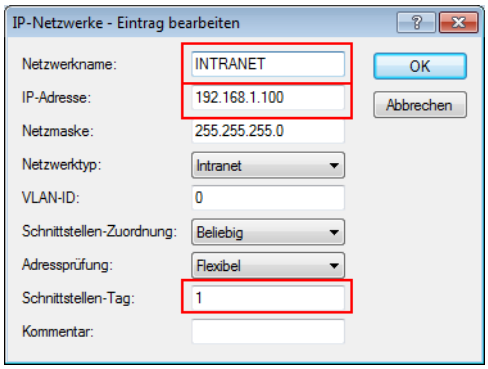
Port-Einstellungen für Public-Spot-APs

7. Erstellen Sie für den Internetzugang der Gäste einen Eintrag in der Liste der DSL-Gegenstellen mit der Haltezeit '9999' und dem vordefinierten Layer 'DHCPOE'. Dieses Beispiel setzt voraus, dass ein Router mit aktiviertem DHCP-Server den Internetzugang bereitstellt. In LANconfig finden Sie diese Einstellung unter Konfiguration/Kommunikation/Gegenstellen/Gegenstellen (DSL).

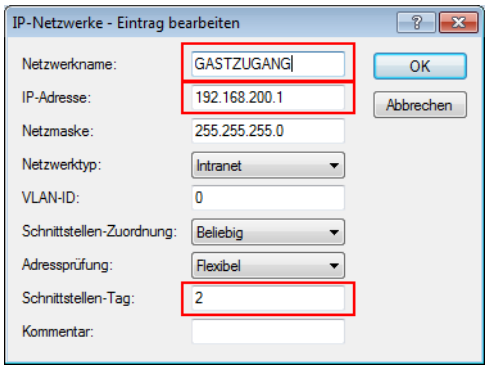


Gegenstelle für Internet-Zugang

8. Erstellen Sie für die interne Nutzung das IP-Netzwerk 'INTRANET' z. B. mit der IP-Adresse '192.168.1.100' und mit dem Schnittstellen-Tag '1', für die Gäste das IP-Netzwerk 'GASTZUGANG' z. B. mit der IP-Adresse '192.168.200.1' und mit dem Schnittstellen-Tag '2'. Der virtuelle Router im WLAN-Controller nutzt die Schnittstellen-Tags, um die Routen für die beiden Netzwerke zu trennen. In LANconfig finden Sie diese Einstellung unter Konfiguration/TCP/IP/Allgemein/IP-Netzwerke.

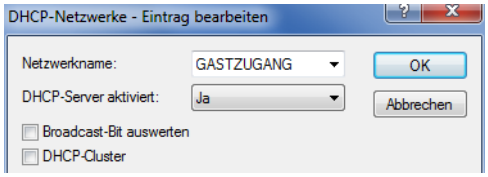


IP-Netzwerk für interne Nutzung



IP-Netzwerk für Gastzugang

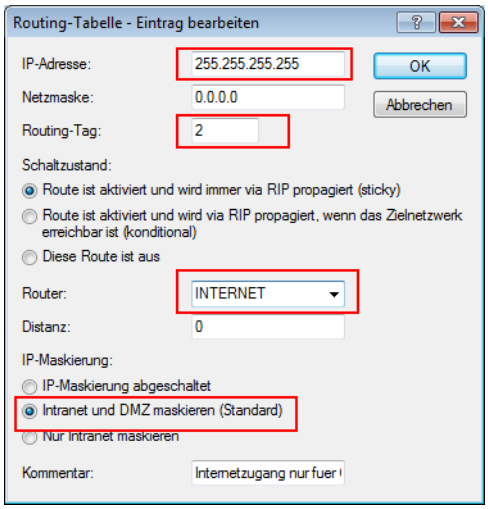
9. Der WLAN-Controller kann als DHCP-Server für die Access Points und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG. In LANconfig finden Sie diese Einstellung unter Konfiguration/TCP/DHCP/DHCP-Netzwerke.



DHCP-Netzwerk für Gastzugang

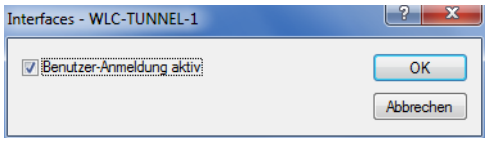
10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästenetzwerk auf den Internet-Zugang des WLAN-Controllers leitet. Wählen Sie dazu das Routing-Tag '2' und den Router 'Internet'.

Aktivieren Sie außerdem die Option 'Intranet und DMZ maskieren (Standard)'. In LANconfig finden Sie diese Einstellung unter Konfiguration/IP-Router/Routing/Routing-Tabelle.



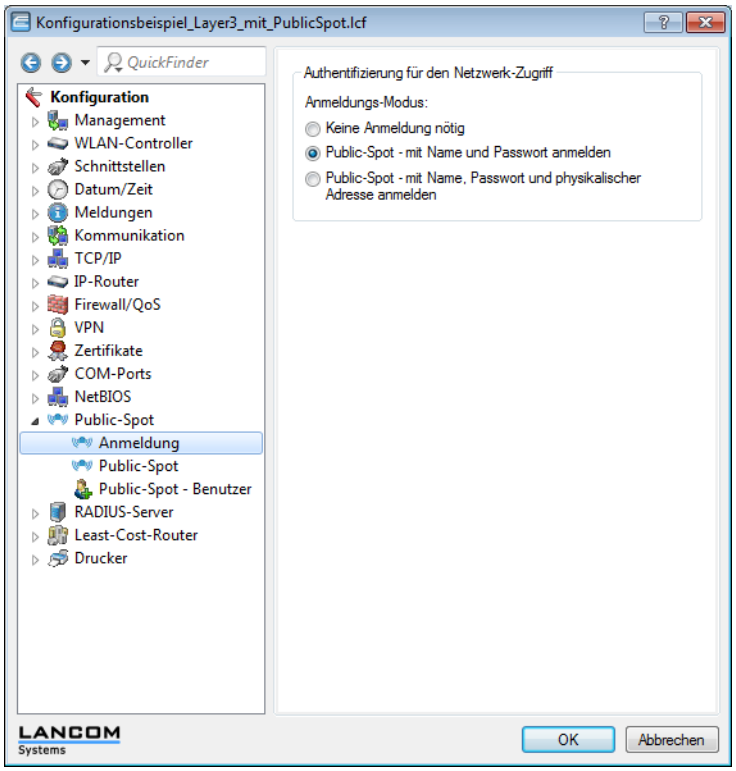
Routing-Eintrag für Internet-Zugang

11. Aktivieren Sie die Public-Spot-Anmeldung für die logische LAN-Schnittstelle 'WLC-Tunnel 1'. In LANconfig finden Sie diese Einstellung unter Konfiguration/Public-Spot/Public-Spot.



Aktivierung der Benutzer-Anmeldung für den WLC-Tunnel

12. Aktivieren Sie im letzten Schritt die Anmeldung über den Public-Spot für den WLAN-Controller. In LANconfig finden Sie diese Einstellung unter Konfiguration/Public-Spot/Anmeldung.



Aktivierung der Anmeldung über den Public-Spot

Neben der Konfiguration des WLAN-Controllers konfigurieren Sie den Public Spot nach Ihren Wünschen entweder für die interne Benutzerliste oder für die Verwendung eines RADIUS-Servers.

4.2 Alarm-Grenzwerte für WLAN Geräte

Typische Situationen, welche sich im WLAN-Umfeld meist für Probleme verantwortlich zeigen, sind ein Absinken der Signalstärke unter einen gewissen Grenzwert, der Prozentsatz der Anzahl an verlorenen Paketen einen gewissen Grenzwert überschreitet oder Pakete müssen sehr oft erneut versendet werden, was die effektiv zur Verfügung stehende Bandbreite stark reduziert.

Um diese Situationen zu erkennen und darauf zu reagieren bietet LANCOM nun auf WLAN Geräten diverse Konfigurationsmöglichkeiten für Grenzwerte, die beim Über- beziehungsweise Unterschreiten einen Alarm auslösen.

Eine Verbindung wird nicht absolut als schlecht bewertet, die Bewertung hängt immer von den Parametern ab, die angegeben werden. Hierbei ist insbesondere zu beachten, dass das zu hohe oder zu niedrige Grenzwerte eine Verbindung auch falsch bewerten können und unnötige Alarme in einer sehr großen Anzahl erzeugen können. Ein gewisses Mass an Paketverlusten und eine schwankende Signalstärke sind auch bei stabilen WLAN-Verbindungen zu erwarten.

Es können Grenzwerte für die einzelnen SSIDs und die Punkt-zu-Punkt-Verbindungen eines Access Points festgelegt werden. Diese werden zur Bewertung der Verbindung jedes Clients zu der entsprechenden SSID und bei der Verbindung zu einem entsprechenden P2P-Partner genutzt.

4.2.1 Ergänzungen im Menüsystem

Netzwerk-Alarm-Grenzen

In dieser Tabelle finden Sie die Einstellungen der Netzwerk-Alarm-Grenzen für die logischen WLAN-Netzwerke des Gerätes (SSIDs).

SNMP-ID: 2.23.20.13

Pfad Telnet: /Setup/Schnittstellen/WLAN

Ifc

Wählen Sie hier das logische WLAN_Netzwerk (SSID), für welches Sie die Netzwerk-Alarm-Grenzen bearbeiten möchten.

SNMP-ID: 2.23.20.13.1

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren SSIDs, z. B. WLAN-1, WLAN-1-2 etc.

Phy-Signal

Der negative Grenzwert für den Signalpegel der entsprechenden SSID. Wird dieser Grenzwert unterschritten, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.13.2

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- 3 numerische Zeichen

Default: 0

Total-Wiederholungen

Der Grenzwert für die Gesamtanzahl an Sendewiederholungen für die entsprechende SSID. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.13.3

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

Tx-Fehler

Die Gesamtanzahl der verlorenen Pakete für die entsprechende SSID. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.13.4

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

4.3 Auto-Konfiguration von WLAN-P2P-Strecken über serielle Verbindungen

Bei der Konfiguration von P2P-Strecken im WLAN-Bereich erkennen sich die Gegenstellen üblicherweise anhand eines definierten Merkmals des jeweiligen P2P-Partners: entweder der Stations-Name oder die MAC-Adresse des P2P-Partners wird in die Konfiguration der Access Points eingetragen.

Bei wechselnden P2P-Partnern können Sie dieses Merkmal jedoch nicht fest in die Konfiguration eintragen. Wenn Sie z. B. zwischen zwei Waggons eines Zuges eine P2P-Verbindung aufbauen möchten, um im ganzen Zug IP-Dienste anzubieten, können die jeweiligen P2P-Gegenstellen bei jeder Zusammenstellung des Zuges wechseln.

In diesen Fällen können die Access Points die jeweiligen MAC-Adressen über die serielle Schnittstelle austauschen. Dazu verbinden Sie die Geräte über zwei Adern der seriellen Schnittstelle untereinander. Stellen Sie dann die Erkennung der P2P-Gegenstelle auf den Wert 'Serial-Autoconfig'. Konfigurieren Sie die P2P-Verbindungen wie bei einer festen Installation der Access Points.

Im Default-Zustand sind die WLAN-Module deaktiviert. Wenn die Geräte eingeschaltet werden, tauschen sie die MAC-Adressen aus, erst dann werden die WLAN-Module aktiviert und die P2P-Verbindung wird automatisch aufgebaut.

4.3.1 Ergänzungen im Menüsystem

Serielle-Konfig

Dieses Menü enthält die Konfiguration für die Autokonfiguration von WLAN-Strecken über eine serielle Verbindung.

SNMP-ID: 2.52.4

Pfad Telnet: /Setup/COM-Ports

Bit-Rate

Stellen Sie hier die Bitrate ein, mit der die Geräte bei der automatischen Konfiguration von WLAN-Strecken über serielle Verbindungen kommunizieren.

SNMP-ID: 2.52.4.1

Pfad Telnet: /Setup/COM-Ports

Mögliche Werte:

- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200

Default: 9600

Die identische Einstellung der Bit-Rate bei allen Geräten, die über serielle Verbindungen kommunizieren, ist eine zwingende Voraussetzung für die automatische Konfiguration der WLAN-Strecken.

4.4 Interpoint-Alarm-Grenzen

4.4.1 Ergänzungen im Menüsystem

Interpoint-Alarm-Grenzen

In dieser Tabelle finden Sie die Einstellungen der Interpoint-Alarm-Grenzen für P2P-Verbindungen des Gerätes (SSIDs).

SNMP-ID: 2.23.20.14

Pfad Telnet: /Setup/Schnittstellen/WLAN

Ifc

Wählen Sie hier die P2P-Verbindung, für welche Sie die Interpoint-Alarm-Grenzen bearbeiten möchten.

SNMP-ID: 2.23.20.14.1

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren P2P-Verbindungen, z. B. P2P-1-1, P2P-1-2 etc.

Phy-Signal

Der negative Grenzwert für den Signalpegel der entsprechenden P2P-Verbindung. Wird dieser Grenzwert unterschritten, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.14.2

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- 3 numerische Zeichen

Default: 0

Total-Wiederholungen

Der Grenzwert für die Gesamtanzahl an Sendewiederholungen für die entsprechende P2P-Verbindung. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.14.3

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

Tx-Fehler

Die Gesamtanzahl der verlorenen Pakete für die entsprechende P2P-Verbindung. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.14.4

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

4.5 Übernahme der User-Priorität von IEEE 802.11e in VLAN-Tags

IEEE 802.11e ist ein Standard zur Erweiterung der WLAN-Standards um Quality-of-Service-Funktionen (QoS). Wenn ein Access Point diesen Standard nutzt, kann das Gerät den angebundenen WLAN-Clients eine bestimmte Priorität zuweisen (User-Priorität). Mit der Priorisierung der WLAN-Datenpakete kann der Access Point u. a. die Daten von Voice-over-IP-Clients bevorzugt übertragen. Auf der LAN-Seite sind die Access Points in vielen Fällen mit einem Switch verbunden, verschiedene LAN-Segmente sind oft durch VLANs getrennt. Das kabelgebundene LAN nutzt andere Mechanismen zur Priorisierung der Datenpakete.

Das folgende Anwendungsbeispiel verdeutlicht die Situation:

- Ein WLAN-Client (z. B. VoIP-Telefon) ist an einen Access Point angebunden, QoS ist auf dem WLAN aktiviert, die Daten zwischen Telefon und Access Point sind nicht VLAN-getaggt.
- Der Access Point ist auf der Ethernet-Seite mit einem VLAN-fähigen Switch verbunden, die Daten zwischen AP und Switch sind VLAN-getaggt.

Der Access Point als Schnittstelle zwischen kabelgebundenem LAN und drahtlosem WLAN setzt die unterschiedlichen Priorisierungsinformationen entsprechend um:

- Bei der Übertragung von Daten vom Access Point zum WLAN-Client (Senderichtung aus Sicht des Access Points) ermittelt das Gerät die Priorität eines empfangenen Paketes entweder aus dem VLAN-Tag oder aus dem ToS/DSCP-Feld des IP-Headers. Mit dieser Priorität sendet der Access Point die Pakete an den Client.
- Bei der Übertragung von Daten vom WLAN-Client zum Access Point (Empfangsrichtung aus Sicht des Access Points) enthält das Datenpaket jedoch kein VLAN-Tag. In dieser Richtung untersucht der Access Point außerdem nicht den IP-Header. Stattdessen entnimmt der Access Point die User-Priorität aus dem WLAN-Paket und setzt diese entsprechend in das VLAN-Tag der ausgehenden Datenpakete in Richtung Switch ein.

4.6 Automatische Authentifizierung am Public Spot mit der MAC-Adresse

Ein Public Spot gewährt in der Regel einem Benutzer im WLAN nach erfolgreicher Authentifizierung Zugang zu bestimmten Diensten. Zur Authentifizierung zeigt der Public Spot dem Benutzer nach dem Öffnen des Browsers üblicherweise eine Webseite. Der Benutzer gibt in dieser Anmeldeseite seine Benutzerdaten ein, der Public Spot leitet den Benutzer dann auf die erlaubten Webseiten weiter.

In manchen Anwendungsfällen ist die Authentifizierung über eine Webseite nicht erwünscht oder nicht möglich, wie die folgenden Beispiele zeigen:

- Der WLAN-Client verfügt nicht über einen Browser und kann daher die Anmeldeseite nicht öffnen.
- Der manuelle Aufruf der Anmeldeseite ist z. B. für einen Performance-Test zu langwierig.

Die automatische Authentifizierung am Public Spot mit der MAC-Adresse erlaubt die Nutzung des Public Spot ohne den vorherigen Aufruf der Anmeldeseite. Dazu trägt der Administrator alle MAC-Adressen der entsprechenden WLAN-Clients in die Tabelle der erlaubten MAC-Adressen ein.

4.6.1 Ablauf der MAC-Adress-Prüfung

Wenn der Access Point die Anfrage eines WLAN-Clients empfängt, vollzieht der Public Spot bei der automatischen Authentifizierung mit der MAC-Adresse folgende Schritte:

- Wenn der Public Spot die MAC-Adresse des empfangenen Paketes schon authentifiziert hat, leitet das Gerät die zugehörigen Pakete weiter.
- Wenn die MAC-Adresse in der Liste der erlaubten WLAN-Clients enthalten ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Pakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert und eine positive, noch gültige Authentifizierung für die MAC-Adresse im Public Spot-Cache gespeichert ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Pakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert, jedoch keine gültige Authentifizierung für die MAC-Adresse im Cache des Public Spot gespeichert ist, leitet der Public Spot die Authentifizierung der MAC-Adresse bei dem entsprechenden RADIUS-Server ein. Nach einer positiven Antwort startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Pakete weiter.
- Sind alle zuvor beschriebenen Prüfungen erfolglos, leitet der Public Spot den Benutzer an die Anmeldeseite weiter.

4.6.2 Authentifizierung der MAC-Adresse über RADIUS

Wenn die MAC-Adresse eines anfragenden WLAN-Clients nicht in der Liste der erlaubten Adressen enthalten ist, kann der Public Spot die Adresse alternativ über einen RADIUS-Server authentifizieren.

Zur Aktivierung dieser RADIUS-Authentifizierung wählt der Administrator einen der im Gerät definierten RADIUS-Server aus der Anbieter-Liste aus.

Zusätzlich definiert der Administrator eine Lebensdauer für die abgelehnten MAC-Adressen. Mit dieser Lebensdauer verhindert der Public Spot das Fluten des RADIUS-Servers mit wiederholten Anfragen nach MAC-Adressen, die weder über die MAC-Adress-Tabelle noch über den RADIUS-Server ohne Anmeldung authentifiziert werden können.

Wenn eine MAC-Adresse bei einer Anfrage zur Authentifizierung über den RADIUS-Server abgelehnt wird, speichert der Public Spot diese Ablehnung für die definierte Lebensdauer. Weitere Anfragen für die gleiche MAC-Adresse beantwortet der Public Spot innerhalb der Lebensdauer direkt ohne Weiterleitung an den RADIUS-Server.

4.6.3 Ergänzungen im Menüsystem

MAC-Adress-Tabelle

In dieser Tabelle finden Sie die erlaubten WLAN-Clients für die automatische Authentifizierung am Public Spot mit Hilfe der MAC-Adresse.

SNMP-ID: 2.24.23

Pfad Telnet: /Setup/Public-Spot

MAC-Adresse

MAC-Adresse des WLAN-Clients, der die automatische Authentifizierung nutzen kann.

SNMP-ID: 2.24.23.1

Pfad Telnet: /Setup/Public-Spot/MAC-Adress-Tabelle

Mögliche Werte:

- Gültige MAC-Adresse, 12 Zeichen

Default: leer

Benutzer

Benutzername des WLAN-Clients, der die automatische Authentifizierung nutzen kann. Der Public Spot verwendet diesen Namen für das optionale Accounting der Sitzung über einen RADIUS-Server.

SNMP-ID: 2.24.23.2

Pfad Telnet: /Setup/Public-Spot/MAC-Adress-Tabelle

Mögliche Werte:

- Innerhalb dieser Tabelle eindeutiger Name, maximal 32 alphanumerische Zeichen

Default: leer

Provider

Der Public Spot verwendet diesen Provider für das optionale Accounting der Sitzung über einen RADIUS-Server.

SNMP-ID: 2.24.23.3

Pfad Telnet: /Setup/Public-Spot/MAC-Adress-Tabelle

Mögliche Werte:

- Auswahl aus den in der Anbieter-Liste definierten RADIUS-Server.

Default: leer

4.6.4 MAC-Address-Prüfungs-Anbieter

Der Public Spot verwendet diesen Provider für die Authentifizierung der MAC-Adresse über einen RADIUS-Server.

SNMP-ID: 2.24.24

Pfad Telnet: /Setup/Public-Spot

Mögliche Werte:

- Auswahl aus den in der Anbieter-Liste definierten RADIUS-Server.

Default: leer

Besondere Werte: Wenn kein Provider ausgewählt ist, findet keine Authentifizierung der MAC-Adresse über einen RADIUS-Server statt. In diesem Fall werden nur die in der MAC-Adress-Tabelle aufgeführten WLAN-Clients ohne Anmeldung am Public Spot authentifiziert.

4.6.5 MAC-Address-Prüfungs-Cache-Zeit

Wenn eine MAC-Adresse bei einer Anfrage zur Authentifizierung über den RADIUS-Server abgelehnt wird, speichert der Public Spot diese Ablehnung für die definierte Lebensdauer. Weitere Anfragen für die gleiche MAC-Adresse beantwortet der Public Spot während der Lebensdauer direkt ohne Weiterleitung an den RADIUS-Server.

SNMP-ID: 2.24.25

Pfad Telnet: /Setup/Public-Spot

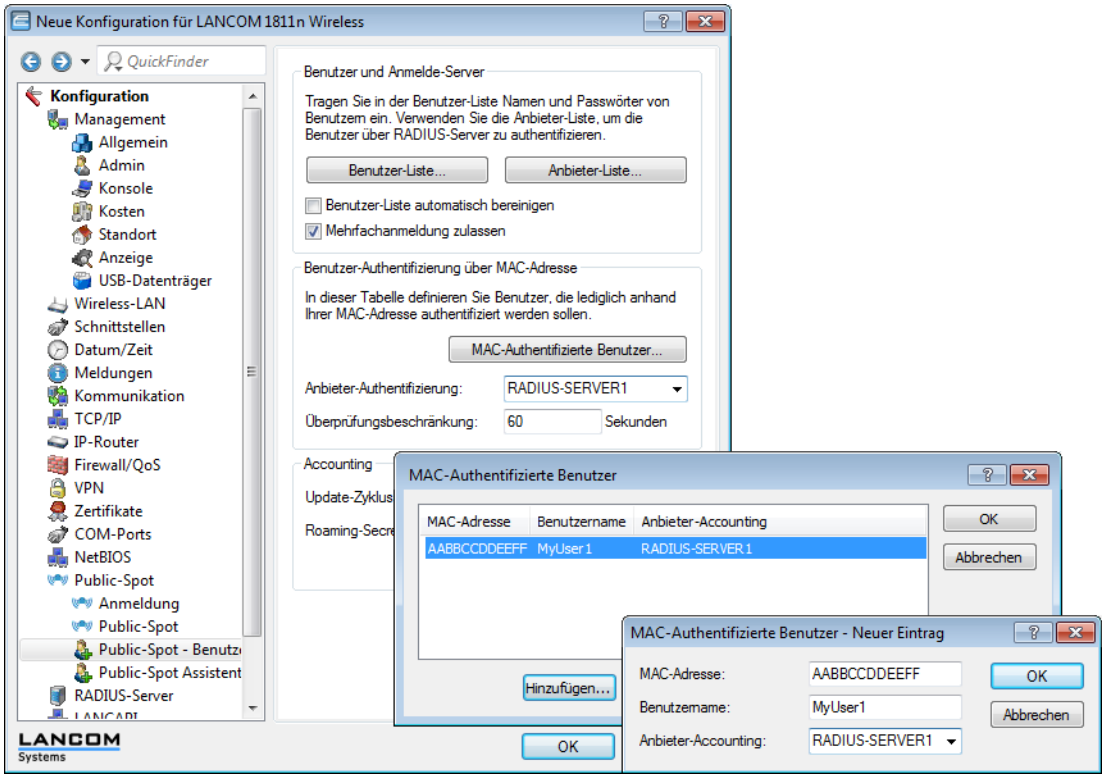
Mögliche Werte:

- Lebensdauer in Sekunden, maximal 10 Ziffern

Default: leer

4.6.6 Konfiguration in LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Parameter für die Authentifizierung der WLAN-Clients über die MAC-Adresse im Konfigurationsbereich Public-Spot > Public-Spot-Benutzer.



5 UTM

5.1 Erweiterungen und Änderungen im Content-Filter

5.1.1 Content-Filter für HTTPS-Seiten

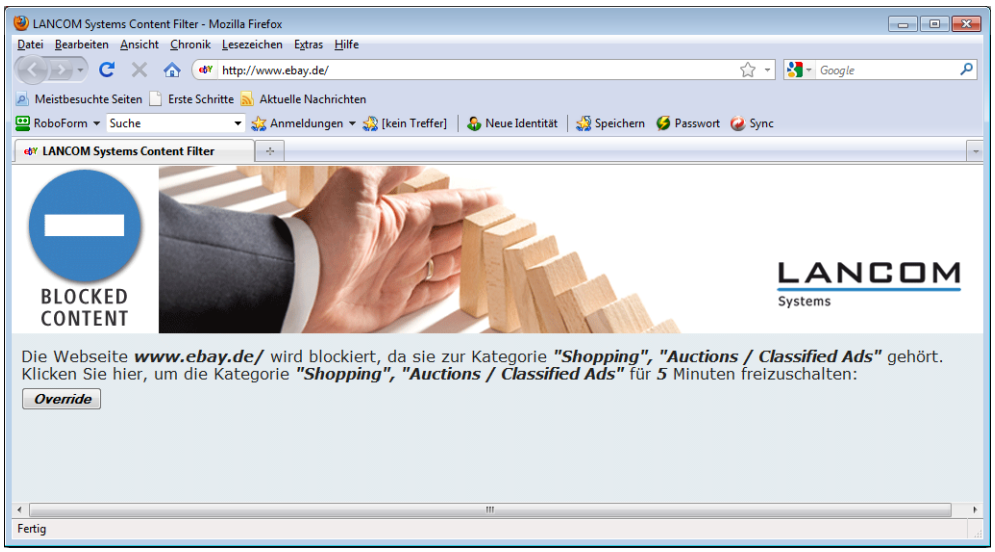
In der ersten Version unterstützte der Content-Filter lediglich HTTP-Seiten, ab LCOS 8.50 auch HTTPS-Seiten.

Die standardmäßig für den Content-Filter verwendete Firewall-Regel 'CONTENT-FILTER' nutzt bei einer Aktivierung der Content Filter Option auf einem Gerät mit LCOS 8.50 oder neuer das Ziel 'WEB', welches ausgehende Verbindungen über HTTP und HTTPS (Ports 80 und 443) erfasst.

Wenn Sie die Content Filter Option auf einem Gerät mit einer LCOS-Version vor 8.50 aktiviert haben, verwendet diese Firewall-Regel nur die HTTP (Port 80) als Ziel. Stellen Sie in diesem Fall das Ziel der Firewall-Regel auf 'WEB' ein, um auch ausgehende HTTPS-Verbindungen mit dem Content-Filter zu prüfen.

5.1.2 One-Click-Override

Die Override-Funktion ermöglicht eine Webseite zu öffnen, obwohl sie zu einer verbotenen Kategorie gehört. Wenn diese Funktion aktiviert ist, zeigt der Content-Filter dem Benutzer eine Information über den Grund der Blockierung und bietet gleichzeitig die Möglichkeit, die betroffene Kategorie für die eingestellte Dauer freizuschalten.



Der Content-Filter zeigt im Falle des Override den entsprechenden Text aus der Tabelle der Block-Texte und direkt darunter den Text aus der Tabelle der Override-Texte mit der Schaltfläche 'Override'. Wenn der Benutzer diese Schaltfläche klickt, leitet der Content-Filter den Benutzer nach Möglichkeit zu der angeforderten Seite weiter. Wenn die Weiterleitung auf die gewünschte Seite nicht gelingt, zeigt der Content-Filter eine Fehlerseite.

In den LCOS-Versionen vor 8.50 wurden Block-Texte, Override-Texte und Fehler-Texte sowie die zugehörigen Attribute teilweise anders verwendet als in den LCOS-Versionen 8.50 und neuer.

Prüfen Sie bei einem Update auf LCOS 8.50 die Texte in den in den Texttabellen auf eventuell erforderliche Anpassungen.

HTTP-Requests übertragen die Argumente zu einem angeforderten URL je nach Anwendung unterschiedlich. In den meisten Fällen sendet der Browser ein GET-Anfrage, bei der die Argumente in dem URL enthalten sind (z. B. ein Suchbegriff). Der Content-Filter kann die Weiterleitung bei einem Override für GET-Anfragen wie gewünscht ausführen, da alle benötigten Informationen in dem URL enthalten sind. In manchen Fällen sendet der Browser jedoch POST-Anfragen, um z. B. bei Datei-Uploads die zu übertragenden Daten im Header der Anfrage zu übermitteln. In diesem Fall sind nicht alle benötigten Informationen für die Weiterleitung beim Override in dem URL enthalten. Der Content-Filter kann Post-Anfragen im Falles eines Override nur dann erfolgreich weiterleiten, wenn der Benutzer in seinem Browser Javascript aktiviert hat. Die auf der HTML-Rendering-Bibliothek 'WebKit' basierenden Browser unterstützen den Override von Post-Anfragen mit Javascript nicht.

Der Content-Filter zeigt den Benutzern ohne aktiviertes Javascript oder mit WebKit-Browsern nach dem Klick auf die Schaltfläche 'Override' eine Fehlerseite. Diese Benutzer klicken dann die Schaltfläche zum erneuten Laden der Webseite für die erfolgreiche Weiterleitung.

Die nachfolgenden Abschnitte zeigen die geänderten Einträge des Menüsystems für den Content-Filter.

URL bei Fehler

Hier können Sie einen alternativen URL eintragen. Im Falle eines Fehlers wird dann statt der Standard-Webseite der hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen Tags wie im Override-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- gültige URL-Adresse

Default: leer

Loopback bei Fehler

Hier können Sie optional eine Absenderadresse für den Fehler-URL konfigurieren, der statt der ansonsten automatisch für die Ziel-Adresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Englische Bezeichnung: Loopback-To-Use-On-Override

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

Default: leer

Die hier eingestellte Absenderadresse wird für jede Gegenstelle unmaskiert verwendet.

Text

Geben Sie hier den Text ein, der als Blocktext für diese Sprache verwendet werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Blocktext

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

leer

Besondere Werte:

Sie können für den Blocktext auch spezielle Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für den verbotenen URL
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-CATEGORIES/> für die Liste der Kategorien aufgrund der die Webseite verboten wurde
- <CF-PROFILE/> für den Profilnamen
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-OVERRIDEURL/> für den URL zum Freischalten des Overrides (dieser kann in ein einfaches <a>-Tag oder einen Button eingebaut werden)
- <CF-LINK/> fügt einen Link zum Freischalten des Overrides ein
- <CF-BUTTON/> für einen Button zum Freischalten des Overrides

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute sind:

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- FORBIDDEN: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- CATEGORY: wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- ERR: wenn ein Fehler aufgetreten ist.

Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Tag nur sinnvoll, wenn Sie einen alternativen Block-URL konfiguriert haben.

- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Blocktext nur maximal 254 Zeichen lang sein darf.

Beispiel:

- <CF-URL/> wird wegen der Kategorien <CF-CA/> verboten.
Ihr Contentfilterprofil ist <CF-PR/>.
<CF-IF OVERRIDEOK>
<CF-BU/></CF-IF>

Die hier beschriebenen Tags können auch in externen HTML-Seiten (alternativer Block-URL) verwendet werden.

Text

Geben Sie hier den Text ein, der als Fehlertext für diese Sprache verwendet werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Fehlertext

Mögliche Werte:

254 alphanumerische Zeichen

Default:

leer

Besondere Werte:

Sie können für den Fehlertext auch HTML-Tags verwenden.

Für die einzusetzenden Werte können Sie folgende Empty-Element-Tags verwenden:

- <CF-URL/> für den verbotenen URL
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des blockierten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-PROFILE/> für den Profilnamen
- <CF-ERROR/> für die Fehlermeldung

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute sind:

- CHECKERROR: der Fehler ist beim Prüfen des URL aufgetreten
- OVERRIDEERROR: der Fehler ist beim Freischalten eines Override aufgetreten

Beispiel:

<CF-URL/> wird verboten, weil ein Fehler aufgetreten ist:
<CF-ERROR/>

<CF-URL>: blockierter URL <CF-HOST> oder <CF-DOMAIN>: Hostteil des blockierten URL <CF-PROFILE>: Contentfilterprofil des Benutzers <CF-DURATION>: Overridedauer in Minuten <CF-ERROR>: Fehlermeldung <CF-IF> bis </CF-IF>: bedingte Auswertung mit logischem ODER der folgenden Parameter: CHECKERROR: der Fehler ist beim Prüfen des URL aufgetreten (wie früher) OVERRIDEERROR: der Fehler ist beim Freischalten eines Overrides aufgetreten

Text

Geben Sie hier den Text ein, der als Overridetext für diese Sprache verwendet werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Overridetext

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

leer

Besondere Werte:

Sie können für den Blocktext auch HTML-Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für den ursprünglich verbotenen URL, der jetzt aber freigeschaltet ist
- <CF-CATEGORIES/> für die Liste der Kategorien, die durch diesen Override freigeschaltet sind (außer bei Domain-Override).
- <CF-BUTTON/> zeigt einen Override-Button, der auf den ursprünglich aufgerufenen URL weiterleitet.
- <CF-LINK/> zeigt einen Override-Link an, der auf den ursprünglich aufgerufenen URL weiterleitet.

- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-ERROR/> erzeugt eine Fehlermeldung, falls der Override fehlschlägt.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute können sein:

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- FORBIDDEN: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- CATEGORY: wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- DOMAIN: wenn der Override-Typ "Domain" ist und der Override erfolgreich war
- BOTH: wenn der Override-Typ "Kategorie und Domain" ist und der Override erfolgreich war
- ERROR: falls der Override fehlgeschlagen ist
- OK: falls entweder CATEGORY oder DOMAIN oder BOTH zutreffend sind

Werden in einem Tag mehrere Attribute angegeben, dann sollte der Bereich eingeblendet werden, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Text nur maximal 254 Zeichen lang sein darf.

Beispiel:

<CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> in der Domain <CF-DO/></CF-IF><CF-IF DO>Die Domain <CF-DO/> ist</CF-IF><CF-IF OK> für <CF-DU/> Minuten freigeschaltet.
<CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:
<CF-ERR/></CF-IF>

6 Projekt-Management

6.1 Benutzerdefinierter Rollout-Assistent

6.1.1 Einleitung

In größeren Projekten zur Vernetzung richten die Administratoren oft zahlreiche Geräte vom gleichen oder ähnlichen Typ an unterschiedlichen Standorten ein. Um die persönliche Anwesenheit an den jeweiligen Standorten zu reduzieren oder ganz zu vermeiden, bereiten die Administratoren die Geräte oft in der Zentrale für den Rollout vor. Am Einsatzort führt ein Mitarbeiter oder ein Kunde dann einen speziellen Assistenten aus, der die standortbezogenen Teile der Konfiguration ergänzt und das Gerät in den gewünschten Betriebszustand bringt.

Mit einer speziellen Beschreibungssprache gibt LCOS den Administratoren die Möglichkeit, auch sehr komplexe Assistenten zu definieren. Die benutzerdefinierten Assistenten unterstützen folgende Funktionen:

- Definition von beliebigen internen Variablen
- Bedingte Verzweigungen
- Bedingte Sprunganweisungen zu beliebigen URL
- Bedingte Anzeige von Hinweisen
- Ausführen von allen (nicht interaktiven) Aktionen, die in der LCOS-Kommandozeile zur Verfügung stehen
- Auslesen von aktuellen Werten aus der Konfiguration der Geräte
- Schreiben von neuen Werten in die Konfiguration der Geräte
- Statusprüfungen wie z. B. Prüfen der Uhrzeit im Gerät
- Verbindungsprüfungen wie z. B. die erfolgreiche VPN-Verbindung zu einer bestimmten Gegenstelle

Der Administrator erstellt nach den Regeln der Beschreibungssprache einen neuen Assistenten in Form einer Text-Datei, die er anschließend in das Gerät lädt. Der Anwender am Einsatzort kann den benutzerdefinierten Assistenten dann unter WEBconfig über den gewählten Namen ausführen.

Sie können bestimmte Administrators-Accounts gezielt auf die Ausführung des Rollout-Assistenten beschränken und so auch ungeübten Anwendern die Konfiguration bestimmter Funktionen ermöglichen, ohne einen kompletten Konfigurationszugriff zu erlauben.

Zum Zeitpunkt der Freigabe von LCOS 8.50 können die Nutzer der folgenden Geräte die Beschreibungssprache für benutzerdefinierte Assistenten verwenden:

- LANCOM 1681V
- LANCOM 1711+ VPN
- LANCOM 1721+ VPN
- LANCOM 1821n Wireless
- LANCOM 1811n Wireless
- LANCOM 1751 UMTS

6.1.2 Struktur des benutzerdefinierten Assistenten

Die Beschreibung eines benutzerdefinierten Assistenten besteht aus den folgenden Abschnitten:

- String-Tabellen mit den benötigten Texten in Deutsch und Englisch.
- Eine Definition des Assistenten.

- Beliebig viele Sektionen zur Beschreibung der einzelnen HTML-Seiten, die der Assistent anzeigen kann.
- Ein Initialisierungs-Bereich, der die Aktionen beim Starten des Assistenten definiert.
- Ein abschließender Bereich, der die Aktionen beim Beenden des Assistenten definiert.

Beachten Sie für die Beschreibung des Assistenten die folgenden Konventionen:

- Die Elemente der Beschreibung folgen genau der oben genannten Struktur.
- Die Textdatei mit der Beschreibung ist nach ISO 8859-1 kodiert.
- Kommentare beginnen mit einem Semikolon und dienen nur der Lesbarkeit der Beschreibung.
- Interne Variablen beginnen mit dem Schlüsselwort `wizard.` (inklusive des Punktes) und speichern Informationen für die interne Vearbeitung des Assistenten.
- Konfigurationsvariablen beginnen mit dem Schlüsselwort `config.` (inklusive des Punktes) und lesen Informationen aus der aktuellen Gerätekonfiguration aus oder schreiben Werte in die aktuelle Konfiguration hinein. Geben Sie die Konfigurationsvariablen in einer der folgenden Schreibweisen an:
  - Dedizierte Parameter der Konfiguration referenzieren Sie über `config.1.<SNMP-ID>`, also z. B. `config.1.2.1` für den Zugriff auf den Namen des Gerätes (im Menü zu finden unter /setup/name)

    Die SNMP-ID zu einem Parameter der Konfiguration ermitteln Sie z. B. mit dem Befehl `ls -a` an der Kommandozeile in dem entsprechenden Untermenü.
  - Die Werte in einer Tabelle referenzieren Sie über:

    ```
    config.1.<SNMP-ID>.<Zeile>.ID:<Spalte>
    ```

    Beispiel für den Wert in der ersten Zeile und der Spalte mit der ID '2' in der Routing-Tabelle '1.2.8.2':

    ```
    config.1.2.8.2.1.ID:2
    ```

  - Wenn Ihnen die ID der Spalte nicht bekannt ist, referenzieren Sie die Werte in einer Tabelle alternativ über:

    ```
    config.1.<SNMP-ID>.<Zeile>.<Spalte>
    ```

    Beispiel für den Wert in der ersten Zeile und der zweiten Spalte:

    ```
    config.1.2.8.2.1.2
    ```

  - Wenn Ihnen die benötigte Zeile der Tabelle nicht bekannt ist, referenzieren Sie die Werte in einer Tabelle über einen bekannten Wert in der ersten Spalte mit:

    ```
    config.<SNMP-ID>."<Bekannter-Wert>".ID:<Spalte>
    ```

    Beispiel für den Wert der Spalte mit der ID '2' von genau der Zeile, die in der ersten Spalte den Wert der Default-Route enthält:

    ```
    config.1.2.8.2."255.255.255.0".ID:2
    ```

    Enthält die Tabelle mehrere Zeilen mit dem gleichen Wert in der ersten Spalte, referenziert die Konfigurationsvariable die erste dieser Zeilen.
  - Wenn die benötigte Zeile der Tabelle erst bei der Ausführung des Assistenten durch eine Benutzereingabe definiert wird, referenzieren Sie die Wert in der Tabelle über die Verwendung einer Variablen mit:

    ```
    config.<SNMP-ID>.\"<Interne-Variable>\".ID:<Spalte>
    ```

    Beispiel für die Zeile, deren Wert in der ersten Spalte mit dem aktuellen Wert der internen Variablen wizard.target_network übereinstimmt:

    ```
    config.1.2.8.2."\wizard.target_network"\.ID:2
    ```

- Geräte-Variablen für Geräteeigenschaften beginnen mit dem Schlüsselwort `device.` (inklusive des Punktes) und lesen bestimmte Geräteeigenschaften aus dem Gerät aus. Weitere Informationen über die Geräte-Variablen finden Sie im Abschnitt *Geräteeigenschaften als Variable nutzen*.

6.1.3 String-Tabellen

Die Beschreibung des benutzerdefinierten Assistenten basiert auf der Definition der zur Anzeige benötigten Texte in deutscher und englischer Sprache.

Die Zeile `stringtable "English"` leitet die englischen Texte ein, die Zeile `stringtable "Deutsch"` die deutschen Texte. Jede String-Definition besteht aus dem Schlüsselwort `string`, gefolgt vom Namen des Strings und dem in doppelte Hochkommata gesetzen Wert.

Das folgende Beispiel zeigt die String-Tabellen mit nur einem Eintrag:

```
; -String tables start-----------------------------------------------
   stringtable "English"
   string title_test, "Test wizard"
   stringtable "Deutsch"
   string title_test, "Test-Assistent"
; -String tables end-------------------------------------------------
```

Der Interpreter für die Beschreibung des benutzerdefinierten Assistenten im LCOS erwartet alle Texte zwingend mit einer deutschen und einer englischen Definition. LCOS führt den Assistenten nicht aus, wenn zu einem Eintrag in der englischen String-Tabelle kein gleichnamiger Eintrag in der deutschen String-Tabelle gefunden wird (oder umgekehrt).

6.1.4 Definition des Assistenten

Die Definition legt den Namen des Assistenten fest. Nach dem Schlüsselwort `wizard` folgt der interne Name in doppelten Hochkommata, gefolgt von der Referenz auf einen Eintrag der String-Tabelle (*String-Tabellen*). Der Assistent zeigt den mit diesem String definierten externen Namen bei der Ausführung in der HTML-Seite an:

```
; -Assistenenten-Definition Start----------------------------
   wizard "Mein_Test-Assistent", title_test
; -Assistenenten-Definition Ende-----------------------------
```

6.1.5 Sektionen

Die Sektionen stellen die eigentlichen HTML-Seiten dar, die während der Ausführung des Assistenten im Browser des Anwenders angezeigt werden.

Jede Sektion beginnt mit dem Schlüsselwort `section` und endet mit dem Beginn der nächsten Sektion. Die letzte Sektion endet mit dem Beginn des Bereiches 'on-init', die Sektionen enden also ohne ein explizites Schlüsselwort für das Ende.

Die Sektionen beinhalten die folgenden Elemente in beliebieger Reihenfolge und Menge:

- Bedingungen
- Optional eigene Bezeichnung für die Sektion, beginnend mit dem Schlüsselwort `label`, gefolgt von einer Zeichenkette aus Groß- und Kleinbuchstaben und dem Unterstrich '_':

  ```
  Label Mein_RolloutAssistent
  ```

  Die Beschreibung des Assistenten kann die eigene Bezeichnung (Label) als Sprungziel nutzen.

- Statischer Text, beginnend mit dem Schlüsselwort `static_text`, gefolgt von einer Referenz auf einen Eintrag der String-Tabelle (*String-Tabellen*):

  ```
  static_text str.conf_general
  ```

- Felder für verschiedene Datentypen wie Text oder IP-Adresse, Kontrollkästchen, Optionsfelder, Auswahllisten etc.

Hinweise zu den verfügbaren Feldern finden Sie im Abschnitt *"Felder"*.

- Aktionen, die der Assistent je nach Schlüsselwort zu Beginn des Blocks in unterschiedlichen Situationen ausführt:
  - on_show: Der Assistent führt die Aktionen in diesem Block aus, bevor eine Sektion (HTML-Seite) angezeigt wird.
  - on_skip: Der Assistent führt die Aktionen in diesem Block aus, wenn eine Sektion (HTML-Seite) aufgrund der darin enthaltenen Bedingungen nicht angezeigt wird.
  - on_next: Der Assistent führt die Aktionen in diesem Block aus, wenn der Benutzer die Schaltfläche 'Weiter' in der Sektion (HTML-Seite) klickt.
  - on_back: Der Assistent führt die Aktionen in diesem Block aus, wenn der Benutzer die Schaltfläche 'Zurück' in der Sektion (HTML-Seite) klickt.

Hinweise zum Aufbau der Blöcke mit den Aktionen und den darin verfügbaren Elementen finden Sie im Abschnitt *Aktionen*.

6.1.6 Bedingungen

Man kann für ein Element beliebig viele Bedingungen angeben, Bedingungen in verschiedenen Zeilen sind UND-verknüpft, die in einer Zeile ODER-verknüpft.

Die Beschreibung des Assistenten kann alle Elemente einer Sektion mit Bedingungen versehen. Die Bedingungen beziehen sich dabei immer auf das vorhergehende Element und bestehen aus der Angabe einer Klasse und einem oder mehreren Bedingungsmustern. Ein Muster wiederum besteht aus zwei Operanden und einem Operator.

Wenn eine Bedingung mehrere Bedingungsmuster in einer Zeile enthält, wertet der Assistent diesen Ausdruck als ODER-Verknüpfung.

Wenn die Beschreibung mehrere Bedingungen in separaten Zeilen zu einem übergeordneten Element enthält, wertet der Assistent diesen Ausdruck als UND-Verknüpfung.

Die Beschreibung kann die folgenden Klassen enthalten:

- `only-if`: Das vorhergehende Element wird nur ausgeführt oder angezeigt, wenn mindestens eines der folgenden Bedingungsmuster erfüllt ist.
- `skip-if`: Das vorhergehende Element wird nicht ausgeführt oder angezeigt, wenn alle der folgenden Bedingungsmuster erfüllt sind.

Das Bedingungsmuster kann folgende Operanden enthalten:

- Statische Texte
- Interne Variablen des Assistenten
- Variablen zur Referenzierung von Werten aus der aktuellen Konfiguration des Gerätes (Konfigurations-Variablen)
- Das Zeichen '*' als Platzhalter (Wildcard)

Das Bedingungsmuster kann folgende Operatoren enthalten:

- `equal`: Prüft, ob die beiden Operanden gleich sind.
- `exists`: Prüft, ob die angegebene Konfigurations-Variable gesetzt ist, also der Wert des Parameters in der Konfiguration nicht leer ist.
- `empty`: Prüft, ob der erste Operand leer ist. Der zweite Operand wird als Platzhalter (Wildcard) '*' angegeben.
- `contains`: Prüft, ob der erste Operand den zweiten Operanden enthält.
- `!`: Verneint die Bedingung.

Beispiele:

Die folgende Bedingung zeigt die Sektion nur dann an, wenn die interne Variable 'wizard.test_select' gleich '0' ist.

```
section
only_if wizard.test_select, "0", equal
```

Die folgende Bedingung setzt die interne Variable 'wizard.intranet_name' auf den Wert 'INTRANET', wenn diese Variable bisher leer ist.

```
set wizard.intranet_name, "INTRANET"
only_if wizard.intranet_name, *, empty
```

Die folgende Bedingung setzt die interne Variable 'wizard.target_1' auf den Wert 'ZIEL_1', wenn die interne Variable 'wizard.select_target' entweder den Wert '1' oder den Wert '5' hat.

```
set wizard.target_1,"ZIEL_1"
only_if wizard.select_target,"1",equal,wizard.select_target,"5",equal
```

6.1.7 Felder und Attribute

Der Assistent verwendet Felder, um dem Benutzer Informationen anzuzeigen und um dem Benutzer die Möglichkeit zur Eingabe von Informationen zu geben. Jedes Feld entspricht einer internen Variablen.

Der Assistent definiert ein Feld durch die Angabe des entsprechenden Schlüsselwortes, gefolgt von einer internen Variablen in der gleichen Zeile. In weiteren Zeilen folgen optional die Attribute für das Feld.

Ein Beispiel für eine Felddefinition im Assistenten:

```
selection_buttons select_inet
 description   str.inet_Selection
 button_text   str.inet_PPPoE, str.inet_IPoE
```

Dieses Feld erzeugt eine Gruppe von Optionsschaltflächen, von denen der Benutzer nur eine aktivieren kann. Der Assistent setzt den in der String-Tabelle definierten Text `str.inet_Selection` als Beschreibung neben das Feld. Für die Optionsschaltflächen selbst zeigt der Assistent die Texte `str.inet_PPPoE` und `str.inet_IPoE` an. Nach der Auswahl einer Option durch den Benutzer schreibt der Assistent den gewählten Wert in die interne Variable `wizard.select_inet`.

Folgende Felder können Sie im Assistenten verwenden:

`check_local_ip`: Dieses Feld prüft, ob der Assistent zuvor die IP-Adresse des Gerätes verändert hat und leitet den Benutzer auf die entsprechende HTML-Seite weiter. Mögliche Attribute:

- `destination`: Ziel für die Weiterleitung als FQDN oder IPv4-Adresse.
- `timeout`: Wartezeit vor der Weiterleitung.

`check_time`: Dieses Feld prüft, ob das Gerät über eine gültige Zeitinformation verfügt. Mögliche Attribute:

- `success_jump`: Label der Seite, die der Assistent bei erfolgreicher Prüfung öffnet.
- `fail_jump`: Label der Seite, die der Assistent bei nicht erfolgreicher Prüfung öffnet.
- `limit`: Maximale Anzahl der Prüfungen, bevor der Assistent die Prüfung als erfolglos ansieht. Setzen Sie das Limit auf den Wert '0', um die Prüfungen ohne Limit fortzusetzen.
- `timeout`: Wartezeit zwischen zwei Prüfungen.

`entryfield_hex`: Dieses Feld dient zur Eingabe von hexadezimalen Werten, z. B. MAC-Adressen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_ipaddress`: Dieses Feld dient zur Eingabe von IPv4-Adressen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `never_zero`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches nicht den Wert '0' enthalten darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_numbers`: Dieses Feld dient zur Eingabe von Telefonnummern. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_numeric`: Dieses Feld dient zur Eingabe von Zahlen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `ange_min`: Minimaler Wert, den der Benutzer in dieses Feld eintragen kann
- `ange_max`: Maximaler Wert, den der Benutzer in dieses Feld eintragen kann
- `signed_value`: Ermöglicht die Angabe eines numerischen Wertes mit Vorzeichen
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld anzeigt.

`entryfield_text`: Dieses Feld dient zur Eingabe von Texten. Mit dem Attribut `hidden` dient das Feld zur Eingabe von Passwörtern. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `hidden`: Kennzeichnet ein Feld, in welches der Benutzer Kennwörter einträgt.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `convert_to_upper`: Wandelt die Eingabe des Benutzers in Großbuchstaben um
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `min_len`: Minimale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld anzeigt.

`entryfield_textwithlist`: Dieses Feld dient zur Eingabe von Texten. Außerdem kann der Benutzer aus einer Reihe von vordefinierten Werten auswählen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `default_value`: Standardwert
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `item_value`: Liste mit vordefinierten Werten, die der Benutzer für dieses Feld auswählen kann

`onoff_switch`: Dieses Feld erzeugt ein einfaches Kontrollkästchen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `value_list`: Liste der beiden Werte, welche das Kontrollkästchen annehmen kann
- `default_selection`: Standardwert

`page_switch`: Dieses Feld erzeugt einen Link, über den der Benutzer zu einer von mehreren anderen HTML-Seiten des Assistenten wechseln kann. Mögliche Attribute:

- `page_description`: Komma separierte Liste mit Texte-Strings oder Referenzen auf Strings zur Beschreibung der möglichen Link-Ziele.

- `page_label`: Komma separierte Liste mit Seiten-Labels der möglichen Link-Ziele.
- `description`: Beschreibung des Feldes in der HTML-Darstellung

`ping_barrier`: Dieses Feld verzögert die weitere Ausführung des Assistenten, bis ein Ping zu dem verwendeten Ziel erfolgreich beantwortet wurde. Mögliche Attribute:

- `destination`: Zieladresse für den Ping.
- `loopback`: Loopback-Adresse, die der Ping anstelle der standardmäßigen Antwortadresse verwendet
- `success_jump`: Label der Seite, die der Assistent bei erfolgreichem Ping öffnet.
- `fail_jump`: Label der Seite, die der Assistent bei nicht erfolgreichem Ping öffnet.
- `limit`: Maximale Anzahl der Pings, bevor der Assistent die Prüfung als erfolglos ansieht. Setzen Sie das Limit auf den Wert '0', um die Pings ohne Limit fortzusetzen.
- `timeout`: Wartezeit zwischen zwei Pings.

`popup`: Dieses Feld öffnet die angegebene Zieladresse in einem Popup-Fenster. Mögliche Attribute:

- keine

Die Zieladresse kann Variablen enthalten (siehe *Variablen* auf Seite 77).

`eadonly_text`: Dieses Feld erzeugt ein Feld ohne Eingabemöglichkeit. Der Assistent kann diese Felder nutzen, um Text anzuzeigen. Mit dem Attribut `hidden` kann der Assistent interne Variablen definieren. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld
- `hidden`: Kennzeichnet ein verstecktes Feld.

`selection_buttons`: Dieses Feld erzeugt eine Gruppe von Optionsschaltflächen, von denen der Benutzer nur eine aktivieren kann. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `button_text`: Komma separierte Liste mit Texte-Strings oder Referenzen auf Strings zur Beschreibung der einzelnen Optionsschaltflächen.
- `button_value`: Komma separierte Liste mit Texte-Strings mit den Werten der einzelnen Optionsschaltflächen.

`selection_list`: Dieses Feld erzeugt eine Auswahlliste (Drop-Down-Liste), aus welcher der Benutzer einen Wert auswählen kann. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `item_text`: Komma separierte Liste mit Texte-Strings oder Referenzen auf Strings zur Beschreibung der einzelnen Listeneinträge.
- `item_value`: Komma separierte Liste mit Texte-Strings mit den Werten der einzelnen Listeneinträge.
- `default_selection`: Standardwert

`static_text`: Dieses Feld erzeugt einen statischen Text auf der HTML-Seite, der als Referenz auf einen Text-String dem Feldnamen folgt. Mögliche Attribute:

- keine

6.1.8 Variablen

In einigen Attributen der Felder können Sie Variablen verwenden, um den Wert des Attributs durch eine anderen Zeichenkette zu ersetzen oder mit einer zusätzlichen Zeichenkette zu ergänzen.

Um eine interne Variable in den Werte eines Attributs einzusetzen, verwenden Sie die Syntax `$(VariablenName)`. Um den Benutzernamen aus der internen Variablen `wizard.username` in einen URL einzusetzen, fügen Sie z. B. das folgende Attribut ein:

```
http://host/directory?param=$(username)
```

Um eine vordefinierte Variable in den Wert eines Attributs einzusetzen, verwenden Sie die Syntax `%VariablenName`. Die folgenden vordefinierten Variablen können Sie in den Attributen verwenden:

- `%` fügt ein Prozentzeichen ein.
- `f` fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- fügt die Hardware-Release des Gerätes ein.
- `v` fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- `m` fügt die MAC-Adresse des Gerätes ein.
- `s` fügt die Seriennummer des Gerätes ein.
- `n` fügt den Namen des Gerätes ein.
- `l` fügt den Standort des Gerätes ein.
- `d` fügt den Typ des Gerätes ein.

6.1.9 Aktionen

Der Assistent verwendet die Aktionen, um Werte in der Konfiguration der Geräte zu verändern.

Für jede Aktion können Sie eine oder mehrere Bedingungen definieren, bei deren Eintreffen der Assistent die Aktion ausführt.

set

Syntax:

- `set $target, $sourcelist`
- `set $target, $number, add`
- `set $target, $number, sub`

Diese Aktion ersetzt den Inhalt der Ziel-Variable durch die angegebene Quelle. Die Quelle enthält in Form einer Komma separierten Liste entweder Variablen oder Text-Strings.

Wenn es sich bei der Ziel-Variablen um einen einzelnen Konfigurationsparameter handelt, geben Sie als Quelle nur einen Wert an, weitere Werte werden ansonsten ignoriert.

Wenn es sich bei der Ziel-Variablen um eine Tabelle handelt, geben Sie in der Quelle zuerst den Wert aus der Zeile an, die der Assistent ändern soll. Der Assistent durchsucht die erste Indexspalte nach diesem Wert und ändert die erste Zeile, in der er diesen Wert findet. Findet der Assistent keine passende Zeile mit diesem Wert, fügt er eine neue Zeile in die Tabelle ein.

Wenn es sich bei der Ziel-Variablen um einen numerischen Wert handelt, können Sie mit Hilfe der `add`- oder `sub`-Aktion den als `$number` definierten Betrag addieren oder subtrahieren.

Beispiele

Die folgende Aktion setzt die Default-Route auf die gewünschten Werte:

```
set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0",
 "on", "Yes", ""
```

Die folgende Aktion erhöht den Wert der ARP-Aging-Minuten um '5':

```
set config.1.2.7.11, "5", add
```

Die folgende Aktion reduziert den Wert der ARP-Aging-Minuten um '5':

```
set config.1.2.7.11, "5", sub
```

del

Diese Aktion löscht den Inhalt der Ziel-Variable. Wenn es sich bei dieser Variablen um eine Tabelle handelt, geben Sie den Wert in aus der ersten Indexspalte aus der zu löschenden Zeile an.

Beispiel

Die folgende Aktion löscht die Default-Route aus der Routing-Tabelle:

```
del config.1.2.8.2, "255.255.255.0"
```

cat

Diese Aktion hängt den Inhalt der Quell-Variablen an die Ziel-Variable an.

Beispiel

Die folgende Aktion fügt den Inhalt der Variablen `wizard.user` und die Variable `wizard.name` an:

```
cat wizard.name, wizard.user
```

cut

Diese Aktion löscht eine bestimmte Anzahl von Zeichen aus der Ziel-Variablen. Geben Sie die Position der zu löschenden Stelle von links gesehen sowie optional die Anzahl der zu löschenden Zeichen als Parameter an.

Beispiele

Die folgende Aktion löscht in der Variablen `wizard.name` alle Zeichen nach dem 2. Zeichen.

```
cut wizard.name, 2
```

Die folgende Aktion löscht in der Variablen `wizard.name` genau 4 Zeichen nach dem 2. Zeichen.

```
cut wizard.name, 2, 4
```

trigger_config_change

Änderungen der Konfiguration durch den Wizard sind je nach Teil der Firmware nicht sofort wirksam, da einige Module interne Strukturen für die Konfiguration verwenden.

Die Aktion `trigger_config_change` löst eine Aktualisierung dieser internen Strukturen aus. Setzen Sie diese Aktion in einer Sektion ein, wenn Sie beim Wechsel einer Seite im Rollout-Assistenten sichergehen möchten, dass die Konfiguration aktualisiert wurde.

Beim Beenden führt der Assistent diese Aktion automatisch aus.

exec

Der danachfolgende String wird als Befehl auf der Konsole ausgeführt. Dabei ist auch die Nutzung von Variablen im String möglich, z. B. um ein LoadScript zu starten.

6.1.10 Trace für Rollout-Assistenten

Die HTML-Seiten des Assistenten zeigen nur das jeweilige Ergebnis einer internen Verarbeitung an. Während der Entwicklung eines Assistenten kann der Trace zum Assistenten dem Administrator zusätzliche Informationen z. B. über die Auswertung der einzelnen Bedingungen liefern, die er für die weitere Optimierung nutzt.

Starten Sie den Trace in der Kommandozeile mit dem Befehl `trace + Rollout-Wizard`.

6.1.11 Benutzerdefiniertes HTML-Template nutzen

Zur Anpassung des Assistenten an die Gestaltungsrichtlinien Ihres Unternehmens laden Sie optional ein benutzerdefiniertes HTML-Template in das Gerät. In dem Template legen Sie z. B. den grundlegenden Aufbau der HTML-Seiten und die Gestaltung von Farben, Schriften etc. über CSS-Regeln fest.

Der Assistent verwendet zwei feste Tags im HTML-Template, um die Inhalte des Assistenten in die jeweiligen HTML-Seiten einzufügen:

- `<WIZARD_LOGO>`: An dieser Stelle setzt der Assistent das Logo ein, welches Sie unter 'WEBconfig/Dateimanagement/Zertifikat oder Datei hochladen' im Format GIF, JPEG oder PNG in das Gerät eingespielt haben.
- `<WIZARD_CONTENT>`: An dieser Stelle setzt der Assistent den Inhalt der Sektionen in Form einer zweispaltigen Tabelle mit den zugehörigen Schaltflächen ein.

Ein sehr einfaches Beispiel für ein HTML-Template sieht folgendermaßen aus:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">   <html>
     <head>       <title>Titel des Assistenten</title>
       <meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">     </head>
     <body>
       <div>
         <WIZARD_LOGO>
       </div>
         <WIZARD_CONTENT>
       </body>
   </html>
```

Der Assistent verwendet einige vordefinierte CSS-Klassen, die Sie durch die Angabe von entsprechenden Werte in Ihrem HTML-Template einfach anpassen können, u.a.:

- `class="header"`: Die CSS-Klasse für den Kopfbereich mit dem Logo.
- `class="wizardName"`: Die CSS-Klasse Absatz mit dem Namen des Assistenten im Kopfbereich.
- `class="headerLogo"`: Die CSS-Klasse für den Bereich des Logos im Kopfbereich.
- `class="wizardTable"`: Die CSS-Klasse für Tabelle mit den angezeigten Feldern.
- `class="footer"`: Die CSS-Klasse für den Fußbereich mit den Schaltflächen.

Geräteeigenschaften als Variable nutzen

In manchen Situationen soll ein Assistent Entscheidungen aufgrund der Geräteeigenschaften treffen. So soll der Assistent z. B. bestimmte Werte nur dann in die Konfiguration schreiben, wenn das jeweilige Gerät über eine bestimmte Art von WAN-Schnittstelle verfügt. Als Basis für diese Entscheidungen kann der Assistent mit bestimmten Variablen auf die Geräteeigenschaften zugreifen. Diese Variablen beginnen mit dem Schlüsselwort `device.` (inklusive des Punktes), gefolgt von dem Bezeichner der jeweiligen Eigenschaft. Der Assistent kann folgende Variablen für den lesenden Zugriff auf Geräteeigenschaften nutzen:

`device.flags.dhcp_addr`: Diese Variable gibt an, ob ein DHCP-Server dem Gerät eine IP-Adresse zugewiesen hat (in diesem Fall hat die Variable den Wert '128') oder nicht ('0').

`device.hasADSL`: Diese Variable gibt an, ob das Gerät über eine ADSL-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasISDN`: Diese Variable gibt an, ob das Gerät über eine ISDN-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasUMTS`: Diese Variable gibt an, ob das Gerät über eine UMTS-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasDSL`: Diese Variable gibt an, ob das Gerät über eine DSL-Schnittstelle verfügt ('1') oder nicht ('0').

`device.FirmwareVersion`: Diese Variable gibt die aktuelle Firmware-Version des Gerätes an.

`device.HardwareRelease`: Diese Variable gibt die Hardware-Release des Gerätes an.

`device.LoaderVersion`: Diese Variable gibt die aktuelle Loader-Version des Gerätes an.

`device.MacAddress`: Diese Variable gibt die MAC-Adresse des Gerätes in hexadezimaler Schreibweise ohne Trennzeichen an.

`device.SerialNumber`: Diese Variable gibt die Seriennummer des Gerätes an.

`device.Location`: Diese Variable gibt den Standort des Gerätes an, wie er unter `/setup/snmp` eingetragen ist.

`device.DeviceString`: Diese Variable gibt den Typ des Gerätes an.

`device.Name`: Diese Variable gibt den Namen des Gerätes an, wie er unter `/setup` eingetragen ist.

6.1.12 Dateien für den Assistenten hochladen

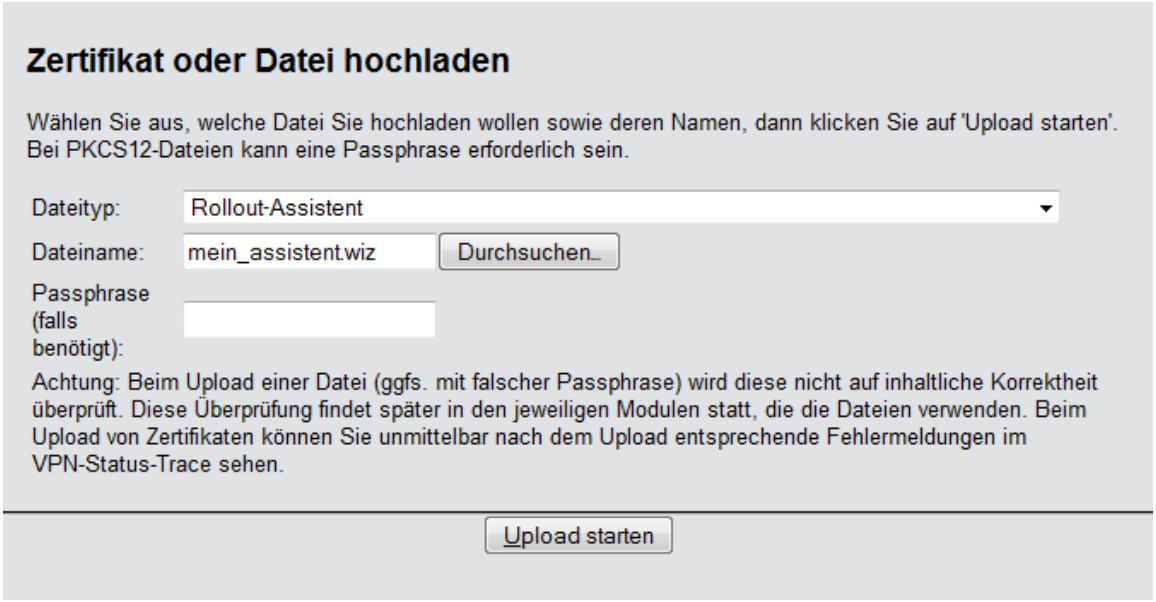
Um den Assistenen verfügbar zu machen, laden Sie die folgenden Dateien in das Gerät:

`Rollout-Assistent`: Die Beschreibung des Assistenten (erforderlich). Diese ISO-8859-1-kodierte Text-Datei ist für den Betrieb des Assistenten notwendig und in der Größe nicht beschränkt.

`Template-fuer-Rollout-Assistent(*.html,*.htm)`: Ein HTML-Template für den Assistenten (optional). Mit diesem Template steuern Sie die Darstellung der Sektionen in den HTML-Seiten des Assistenten im Browser des Anwenders. In diesem Template können Sie u.a. eigene CSS-Informationen zur Definition des Layouts verwenden. Wenn Sie kein eigenes HTML-Template in das Gerät laden, verwendet der Assistent ein vordefiniertes Template. Das Template darf eine Größe von 64kB nicht übersteigen.

`Logo-fuer-Rollout-Assistent(*.gif,*.png.*.jpeg)`: Das Logo Ihrer Unternehmens (optional). Der Assistent setzt diese Bilddatei an der Stelle des Markers `<WIZARD_LOGO>` im HTML-Template ein.Wenn Sie kein eigenes Logo in das Gerät laden, verwendet der Assistent ein vordefiniertes Logo.

Starten Sie den Upload dieser Dateien über 'WEBconfig/Dateimanagement/Zertifikat oder Datei hochladen'.



6.1.13 Dateien des Assistenten aus dem Gerät entfernen

Um die Dateien des Assistenen aus dem Gerät zu entfernen verwenden Sie den Befehl `emove`. Mit dem entsprechenden Parameter definieren Sie, welche Dateien gelöscht werden:

```
ollout <action> [file]
```

Mögliche Aktionen:

- `-r`
- `-remove`

Mögliche Dateien:

- `alle`: Löscht den Assistenten, das Template und das Logo
- `wizard`: Löscht den Assistenten
- `template`: Löscht das Template
- `logo`: Löscht das Logo

6.1.14 Der Rollout-Assistent im LCOS-Menüsystem

Mit den folgenden Parametern steuern Sie das Verhalten des Rollout-Assistenten im LCOS-Menüsystem.

In-Betrieb

Schaltet den Rollout-Assistenten ein oder aus. Nach dem Einschalten wird der Assistent auf der Startseite von WEBconfig angeboten.

SNMP-ID: 2.21.20.1

Pfad Telnet: /Setup/HTTP/Rollout-Wizard

Mögliche Werte:

- Ein
- Aus

Default: Aus

Titel

Name für den Rollout-Assistenten, wie er auf der Startseite von WEBconfig angezeigt wird.

SNMP-ID: 2.21.20.2

Pfad Telnet: /Setup/HTTP/Rollout-Wizard

Mögliche Werte:

- max. 50 Zeichen

Default: ollout

Benutze-Zusatzpruefungen

Diese Option aktiviert einige Konsistenz-Tests, die interne Aspekte des Assistenten püfen.

Die Ausführung der Zusatzprüfungen ist sehr zeitaufwändig. Aktivieren Sie diese Option nur während der Entwicklung des Assistenten und deaktivieren Sie diese Option für den normalen Betrieb.

SNMP-ID: 2.21.20.8

Pfad Telnet: /Setup/HTTP/Rollout-Wizard

Mögliche Werte:

- Ein
- Aus

Default: Aus

6.1.15 Rollout-Assistenten starten

Um den Assistenen verfügbar zu machen, laden Sie die folgenden Dateien in das Gerät:

Starten Sie den Upload dieser Dateien über 'WEBconfig/Dateimanagement/Zertifikat oder Datei hochladen'.

6.1.16 Beispiel für einen Rollout-Assistenten

Dieser Abschnitt stellt ein Beispiel für einen Rollout-Assistenten vor. Der Assistent ermöglicht die Einrichtung eines Internet-Zugangs.

Im ersten Abschnitt definiert der Assistent die Texte, die das Gerät auf den verschiedenen HTML-Seiten anzeigt.

```
stringtable "Deutsch"
 string title_MyCompany,   "MyCompany Rollout"
 string txt_Welcome,      "Willkommen beim MyCompany Rollout Assistenten"

 string dev_serial_number, "Seriennummer"
 string dev_type,          "Gerätetyp"
 ;---Seite: Auswahl der Internetverbindung
 string inet_Selection,    "Typ der Internetverbindung"
 string inet_PPPoE,        "PPPoE"
 string inet_IPoE,         "IPoE"
 ;---Seite: IPoE
 string inet_ipoe,        "Bitte geben Sie die Details für die Verbindung
 ein."
 string con_ipaddress,     "IP-Adresse"
 string con_subnet,        "Netzmaske"
 string con_gateway,       "Gateway"
 string con_dns,           "DNS"
 ;---Seite: PPPoE
 string inet_pppoe,        "Bitte geben sie Benutzername und Kennwort
ein."
 string con_username,      "Benutzername"
 string con_password,      "Passwort"
 ;---Seite: Ende
 string ende,              "Die Konfiguration wird nun abgeschlossen."
```

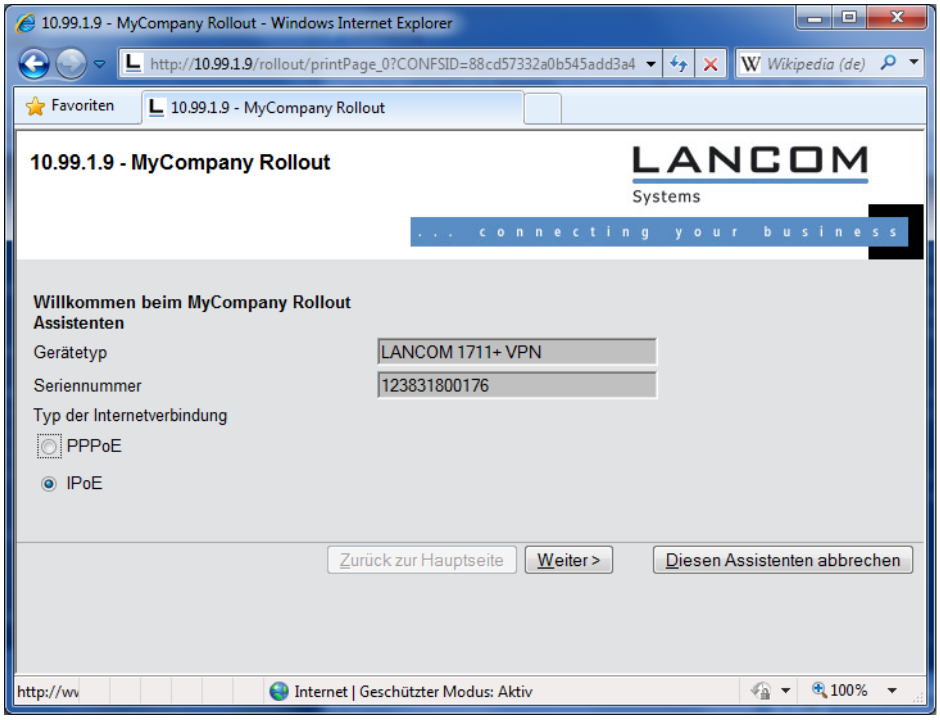
Die erste Zeile des nächsten Abschnitts leitet den Assistenten mit dem Namen 'MyCompany Rollout' ein. Das Gerät zeigt den Text-String `str.title_MyCompany` als Titel in den HTML-Seiten an.

Danach definiert der Assistent die Sektionen, also die benötigten HTML-Seiten.

Die Sektion 'Start' zeigt zunächst einen statischen Text zur Begrüßung an. Darunter zeigt der Assistent in zwei Read-Only-Feldern den Gerätetyp und die Seriennummer an. Der Assistent liest diese beiden Werte beim Öffnen der Seite über den Bereich `on_show` aus dem Gerät aus. In einer Optionsliste bietet der Assistent dem Benutzer die Auswahl für einen Internetzugang über 'PPPoE' oder 'IPoE' an. Da keine Werte für die Optionsfelder definiert sind, setzt der Assistent die Variable `select_inet` je nach Auswahl des Benutzers für PPPoE auf '0' und für IPoE auf '1'.

```
wizard "MyCompany Rollout", str.title_MyCompany

section ;---Start---
 static_text    str.txt_Welcome

 readonly_text device_string
  description   str.dev_type
 readonly_text device_serial_number
  description   str.dev_serial_number

 selection_buttons select_inet
  description   str.inet_Selection
```

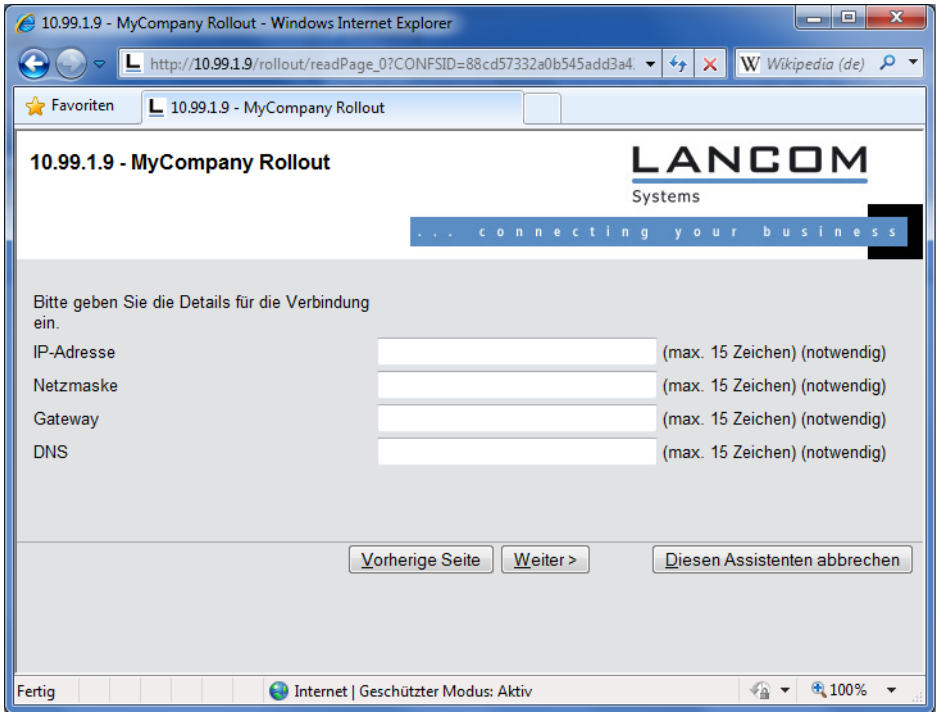
```
 button_text   str.inet_PPPoE, str.inet_IPoE

on_show
 set wizard.device_string, device.DeviceString
 set wizard.device_serial_number, device.SerialNumber

on_next
```



Der Assistent zeigt die Sektion IPoE nur dann an, wenn die Variable select_inet den Wert '1' hat.

Auf dieser Seite fragt der Assistent vom Benutzer die Werte für die IP-Adresse, die Netzmaske, das Gateway und den DNS-Server ab. Alle Felder sind für die Ausführung des Assistenten notwendig.

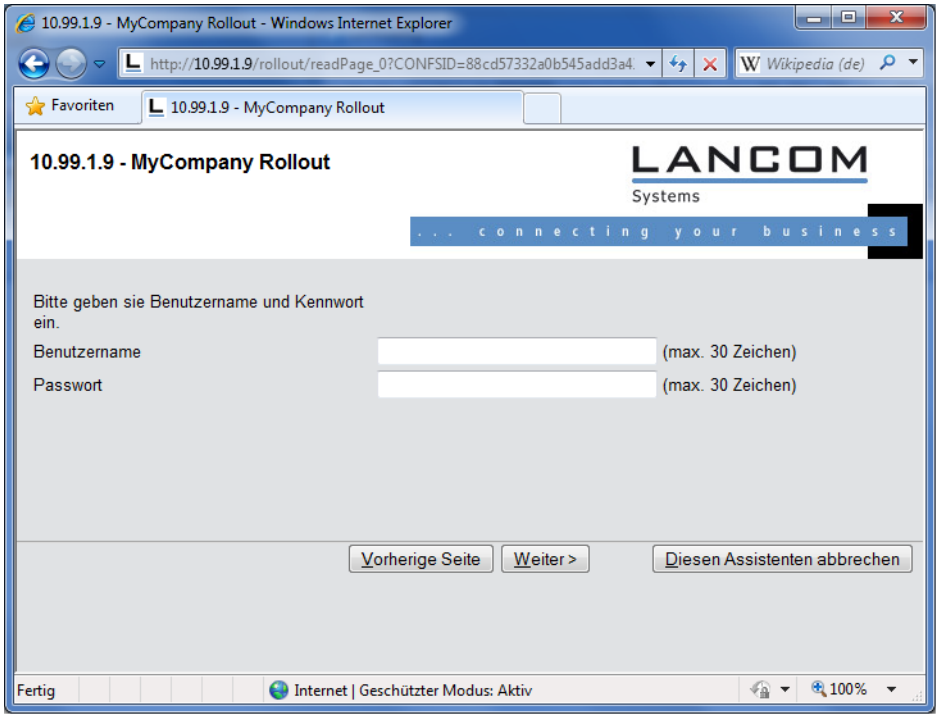
```
section ;---IPoE---
 only_if wizard.select_inet, "1", equal

 static_text   str.inet_ipoe

 entryfield_ipaddress inet_ipaddress
  description  str.con_ipaddress
  never_empty  1
 entryfield_ipaddress inet_subnet
  description  str.con_subnet
  never_empty  1
 entryfield_ipaddress inet_gateway
  description  str.con_gateway
  never_empty  1
 entryfield_ipaddress inet_dns
  description  str.con_dns
  never_empty  1
```



Der Assistent zeigt die Sektion PPPoE nur dann an, wenn die Variable select_inet den Wert '0' hat.

Auf dieser Seite fragt der Assistent vom Benutzer den Benutzernamen und das Passwort mit einer Länge von jeweils maximal 30 Zeichen ab.

```
section ;---PPPoE---
 only_if wizard.select_inet, "0", equal

 static_text   str.inet_pppoe

 entryfield_text inet_username
  description  str.con_username
  max_len   30
 entryfield_text inet_password
  description  str.con_password
  max_len   30
```

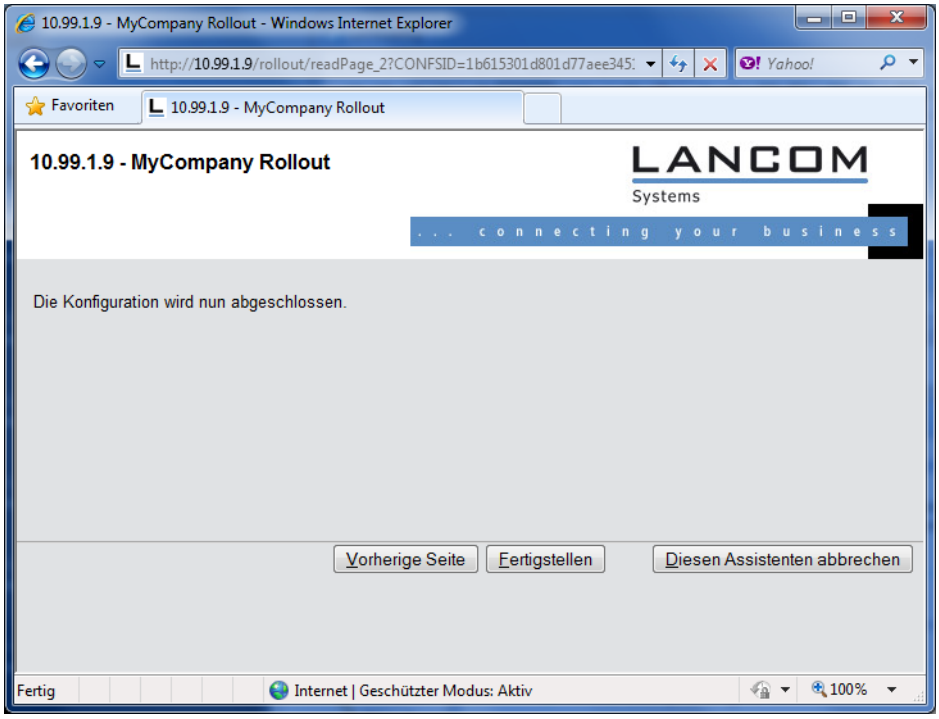


Auf der letzten Seite zeigt der Assistent zunächst einen zusammenfassenden, statischen Text an. Folge Aktionen führt der Assistent beim Fertigstellen des Assistenten aus:

- Wenn der Benutzer IPoE ausgewählt hat, legt der Assistent eine passende Gegenstelle und einen Eintrag in der Liste der IP-Parameter an.
- Wenn der Benutzer PPPoE ausgewählt hat, legt der Assistent eine passende Gegenstelle und einen Eintrag in der PPP-Liste an.
- Unabhängig von der Auswahl legt der Assistent eine Defaultroute an, die den Router 'INTERNET' verwendet.

```
section ;---ende---
 static_text   str.ende

on_init  ;---Befehle, die bei der Initialisierung des Wizards durchgeführt
 werden.---

on_apply ;---Befehle, die bei der Fertigstellung des Wizards durchgeführt
 werden.---

 ;---Wenn IPoE ausgewählt wurde, werden die entsprechenden Daten nun
eingetragen.
 ;---Gegenstelle
 set config.1.2.2.19, "INTERNET", "9999", "", "", "IPOE", "0",
"000000000000"
  only_if wizard.select_inet, "1", equal
 ;---IP-Parameter
 set config.1.2.2.20, "INTERNET", wizard.inet_ipaddress,
wizard.inet_subnet, "0.0.0.0", wizard.inet_gateway, wizard.inet_dns,
"0.0.0.0", "0.0.0.0", "0.0.0.0"
  only_if wizard.select_inet, "1", equal

 ;---Wenn PPPoE ausgewählt wurde, werden die entsprechenden Daten
eingetragen.
 ;---Gegenstelle
 set config.1.2.2.19, "INTERNET", "9999", "", "", "PPPOE", "0",
"000000000000"
```

```
 only_if wizard.select_inet, "0", equal
;---PPP-Liste
set config.1.2.2.5, "INTERNET", "none", "60", wizard.inet_password,
"5", "5", "10", "5", "2", wizard.inet_username, "1"
 only_if wizard.select_inet, "0", equal

;---Setzen der Default Route.
set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0",
"on", "Yes", ""
```



7 Zertifikate

7.1 OCSP Client zur Zertifikatsüberprüfung

7.1.1 Einleitung

Das Online Certificate Status Protocol (OCSP) bietet eine Möglichkeit, den Status von Zertifikaten z. B. für den Aufbau von VPN-Verbindungen zu prüfen. Die Geräte nutzen dieses Protokoll um zu untersuchen, ob der Herausgeber das verwendete Zertifikat evtl. schon vor dem Ablauf der Gültigkeit gesperrt und damit als ungültig markiert hat.

Der Herausgeber der Zertifikate pflegt den Status aller herausgegebenen Zertifikate auf einem speziellen Server, dem OCSP-Responder. Der OCSP-Client (also z. B. ein VPN-Router, der eine Verbindung aufbauen möchte) sendet einen OCSP-Request über das HTTP-Protokoll an den Responder, um den Status des Zertifikats zu ermitteln. Der Responder beantwortet diese Anfrage mit einer signierten Antwort, die der OCSP-Client auf ihre Gültigkeit hin prüft. Die Antwort des OCSP-Responders beschreibt einen der folgenden Zustände:

- good: Das überprüfte Zertifikat ist nicht gesperrt.
- evoked: Das überprüfte Zertifikat ist gesperrt und darf für den Aufbau von VPN-Verbindungen nicht mehr genutzt werden.
- unknown: Der OCSP-Responder kann den Status des Zertifikats nicht ermitteln, z. B. weil der OCSP-Responder den Herausgeber des Zertifikates nicht kennt oder weil das Zertifikat gefälscht und damit nicht in der Datenbasis des OCSP-Responders eingetragen ist.

Sie können das OCSP als Ergänzung oder als Ersatz für die Überprüfung der Zertifikate mit Zertifikatfsrückruflisten (Certificate Revocation Lists – CRL) verwenden. OCSP bietet gegenüber dem Ansatz der CRL folgende Vorteile:

- Die Herausgeber erstellen die CRLs in bestimmten zeitlichen Intervallen und sorgen idealerweise für die Verteilung der CRLs in die Geräte, welche die Zertifikate für den Aufbau der VPN-Verbindungen einsetzen. Die Zuverlässigkeit dieser Überprüfung ist daher an die zeitliche Aktualisierung der CRLs in den Geräten gekoppelt. Die Überprüfung der Zertifikate mit Hilfe eines OCSP-Responders ist dagegen immer "online", also automatisch auf dem aktuellen Stand. Der Betreiber des OCSP-Responders kann die dort vorgehaltenen Daten z. B. über eine automatische Synchronisierung mit den Daten der CA oder CAs abgleichen und so für einen jederzeit aktuellen Stand sorgen.
- Die Prüfung der Zertifikate gegen die Zertifikatfsrückruflisten belastet insbesondere bei großen CRLs den Speicher der Geräte. Die Abfrage des Zertifikatsstatus von einem OCSP-Responder ist dagegen unabhängig von der Anzahl der verwendeten CAs und Zertifikate und daher besser skalierbar.
- Das CRL-Verfahren liefert bei unbekannten Zertifikaten kein Ergebnis – damit kann dieses Verfahren keine gefälschten Zertifikate erkennen. Der OCSP-Responder beantwortet je nach Konfiguration die Anfrage nach unbekannten Zertifikaten mit einer negativen Bewertung.

7.1.2 Ergänzungen im Menüsystem

Responder-Profiltabelle

Diese Tabelle enthält die Informationen über die Certificate Authorities (CAs), deren Zertifikate der OCSP-Client mit einer Anfrage an einen OCSP-Responder prüft.

SNMP-ID: 2.39.6.2

Pfad Telnet: /Setup/Zertifikate/OCSP-Client

Profilname

Geben Sie hier den Namen eines OCSP-Responder-Profils ein, das der OCSP-Client in der CA-Profiltabelle referenziert.

SNMP-ID: 2.39.6.2.1

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- Maximal 32 alphanumerische Zeichen

Default: leer

URL

Geben Sie hier den URL an, über welchen der OCSP-Client den OCSP-Responder erreicht.

SNMP-ID: 2.39.6.2.2

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- Gültige URL mit maximal 251 alphanumerische Zeichen

Default: leer

CA-Profiltabelle

Diese Tabelle enthält die Informationen über die Certificate Authorities (CAs), deren Zertifikate der OCSP-Client mit einer Anfrage an einen OCSP-Responder prüft.

SNMP-ID: 2.39.6.1

Pfad Telnet: /Setup/Zertifikate/OCSP-Client

Profilname

Geben Sie hier den Namen eines CA-Profils ein, welches der OCSP-Client für eine bestimmte CA verwendet.

SNMP-ID: 2.39.6.1.1

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- Maximal 32 alphanumerische Zeichen

Default: leer

CA-DN

Geben Sie hier den Distinguished Name der CA ein, deren Zertifikate der OCSP-Client mit diesem Profil prüft.

SNMP-ID: 2.39.6.1.2

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- maximal 251 alphanumerische Zeichen

Default: leer

AIA-Bevorzugen

Die Zertifikate für den VPN-Verbindungsaufbau führen optional den URL des zuständigen OCSP-Responders im Feld Auhority Info Access (AIA) mit. Stellen Sie hier ein, ob der OCSP-Client vorrangig den URL aus diesem Eintrag der CA-Profiltabelle verwendet oder den URL aus dem AIA-Feld sofern vorhanden.

SNMP-ID: 2.39.6.1.3

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- nein: Der OCSP-Client verwendet immer den URL aus diesem Eintrag der CA-Profiltabelle und lässt den URL im AIA-Feld unbeachtet.
- ja: Der OCSP-Client verwendet (sofern angegeben) den URL aus dem AIA-Feld und lässt den URL aus diesem Eintrag der CA-Profiltabelle unbeachtet.

Default: nein

Responder-Profilname

Wählen Sie hier das Responder-Profil aus, mit dem der OCSP-Client die Zertifikate dieser CA prüft.

SNMP-ID: 2.39.6.1.4

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- Auswahl aus der Liste der Profilnamen in der Tabelle *2.39.6.2 Responder-Profiltabelle*, maximal 32 alphanumerische Zeichen.

Default: leer

Wenn das Feld für den Responder-Profilnamen frei bleibt, prüft das Gerät die verwendeten Zertifikate für die in diesem Eintrag definierte CA nicht mit OCSP, sondern mit Hilfe einer CRL.

Quellinterface

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.39.6.1.5

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

Default: 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

Cert-Pruefung

Stellen Sie hier ein, wie sich das Gerät bei einer nicht erfolgreichen Prüfung des Zertifikats verhält. Der OCSP-Client fragt zunächst beim Verbindungsaufbau die Gültigkeit des verwendeten Zertifikats beim OCSP-Responder an.Wenn das Zertifikat in Kürze abläuft, fragt der OCSP-Client rechtzeitig vor dem Ablaufdatum automatisch die Gültigkeit erneut ab.

SNMP-ID: 2.39.6.1.6

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- Streng: Das Gerät blockiert den Verbindungsaufbau, wenn der OCSP-Responder die Anfrage für das verwendete Zertifikat beim Verbindungsaufbau in einer der folgenden Varianten beantwortet:
  - der OCSP-Responder sendet keine Antwort
  - der OCSP-Responder kennt das Zertifikat nicht (unknown)
  - der OCSP-Responder kennt das Zertifikat und kennzeichnet es als ungültig (revoked)
- Lose: Das Gerät blockiert den Verbindungsaufbau, wenn der OCSP-Responder die Anfrage für das verwendete Zertifikat beim Verbindungsaufbau in einer der folgenden Varianten beantwortet:
  - der OCSP-Responder sendet keine Antwort
  - der OCSP-Responder kennt das Zertifikat nicht (unknown)

Default: Streng

Überprüfen und protokollieren Sie die Ergebnisse der Zertifikatsprüfung beim OCSP-Responder bei Bedarf mit SYSLOG, SNMP-Traps und entsprechenden Traces.

Syslog-Events

Der OCSP-Client kann optional SYSLOG-Nachrichten mit Informationen über die Ergebnisse der Zertifikatsprüfungen beim OCSP-Responder erzeugen.

SNMP-ID: 2.39.6.1.7

Pfad Telnet: /Setup/Zertifikate/OCSP-Client/CA-Profiltabelle

Mögliche Werte:

- ja: Der OCSP-Client erzeugt SYSLOG-Nachrichten.
- nein: Der OCSP-Client erzeugt keine SYSLOG-Nachrichten.

Default: ja