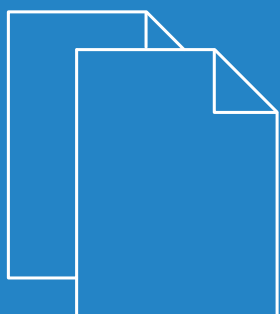


LCOS 10.0

Addendum



Inhalt

1 Addendum zur LCOS-Version 10.0	4
2 Routing und WAN-Verbindungen	5
2.1 Der Bonjour-Proxy.....	5
2.1.1 Bonjour-Grundlagen.....	5
2.1.2 Konfiguration mit LANconfig.....	6
2.1.3 Ergänzungen im Setup-Menü.....	9
2.1.4 Ergänzungen im Status-Menü.....	18
3 WLAN	20
3.1 Steuerung von WLAN-Sessions mittels RADIUS CoA.....	20
3.1.1 Steuerung von WLAN-Sessions mittels RADIUS CoA mit LANconfig konfigurieren.....	20
3.1.2 Ergänzungen im Setup-Menü.....	22
4 WLAN-Management	29
4.1 WLC-Skript-Rollout für bestimmte LCOS-Versionen.....	29
4.1.1 WLC-Skript-Rollout mit LANconfig konfigurieren.....	29
4.1.2 Ergänzungen im Setup-Menü.....	29
5 Public Spot	31
5.1 Anfordern der Benutzer-E-Mail-Adresse beim Login nach Einverständniserklärung.....	31
5.1.1 Adressanforderung mit LANconfig konfigurieren.....	31
5.1.2 Ergänzungen im Setup-Menü.....	32
5.1.3 Ergänzungen im Status-Menü.....	33
5.2 Konfigurieren der Überschrift der Public Spot-Login-Seite.....	34
5.2.1 Individueller Text oder Login-Titel auf der Anmeldeseite.....	34
5.2.2 Ergänzungen im Setup-Menü.....	36
5.3 Bestätigung der Nutzungsbedingungen auf der PMS-Login-Seite.....	36
5.3.1 Bestätigung der Nutzungsbedingungen auf der PMS-Login-Seite mit LANconfig konfigurieren.....	37
5.3.2 Ergänzungen im Setup-Menü.....	37
5.4 Tx- und Rx-Bandbreiten für Tarife im PMS-Modul konfigurierbar.....	38
5.4.1 Tx- und Rx-Bandbreiten für Tarife im PMS-Modul mit LANconfig konfigurieren.....	38
5.4.2 Ergänzungen im Setup-Menü.....	39
5.5 Unterstützung von RADIUS CoA.....	40
5.5.1 Annahme von RADIUS-CoA-Requests im Public Spot aktivieren.....	40
5.5.2 Ergänzungen im Setup-Menü.....	41
6 RADIUS	43
6.1 Unterstützung von Tunnel-Passwort- und LCS-Routing-Tag Attributen.....	43
6.1.1 Tunnel-Passwort und Routing-Tag-Attribute mit LANconfig konfigurieren.....	43
6.1.2 Ergänzungen im Setup-Menü.....	44
6.2 WAN-Zugriff auf den RADIUS-Server einschränken.....	45
6.2.1 Ergänzungen im Setup-Menü.....	45

7 Voice over IP - VoIP.....	47
7.1 Clientseitige Unterstützung von SIPS/SRTP.....	47
7.1.1 Unterstützung von SIPS/SRTP mit LANconfig konfigurieren.....	47
7.1.2 Ergänzungen im Setup-Menü.....	49
7.2 Einschränkung der Verarbeitung eingehender UDP-Pakete auf SIP-Leitungen.....	52
7.2.1 Einschränkung der Verarbeitung eingehender UDP-Pakete mit LANconfig konfigurieren.....	52
7.2.2 Ergänzungen im Setup-Menü.....	54
7.3 Terminieren eines SIP-Trunks im LAN.....	55
8 LANCOM Management Cloud (LMC).....	57
8.1 Grundlagen der LANCOM Management Cloud.....	57
8.2 Koppeln von Geräten mit der LANCOM Management Cloud.....	57
8.2.1 Koppeln von Bestandsgeräten via LANconfig.....	57
8.2.2 Koppeln von Bestandsgeräten via Kommandozeile.....	58
8.2.3 Koppeln von Bestandsgeräten via WEBconfig.....	59
8.3 Auslieferung der LMC-Domain durch den LCOS-DHCP-Server.....	59
8.3.1 Konfiguration der DHCP-Option 43 zur Auslieferung der LMC-Domain mit LANconfig.....	60
8.3.2 Ergänzungen im Setup-Menü.....	60
8.4 Manuelles Vorabkonfigurieren Ihres Gerätes für die Verwaltung durch die LANCOM Management Cloud.....	61
8.5 Ergänzungen im Status-Menü.....	62
8.5.1 LMC.....	62
8.6 Ergänzungen im Setup-Menü.....	66
8.6.1 LMC.....	66
9 Diagnose.....	70
9.1 Layer-7-Anwendungserkennung.....	70
9.1.1 Layer-7-Anwendungserkennung mit LANconfig konfigurieren.....	71
9.1.2 Ergänzungen im Setup-Menü.....	74
9.1.3 Ergänzungen im Status-Menü.....	81

1 Addendum zur LCOS-Version 10.0

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.0 gegenüber der vorherigen Version.

2 Routing und WAN-Verbindungen

2.1 Der Bonjour-Proxy

Ab Version 10.0 steht im LCOS ein Bonjour-Proxy zur Verfügung.


Mit Apple Bonjour haben Endgeräte die Möglichkeit, freigegebene Dienste innerhalb eines lokalen Netzwerkes automatisch und ohne vorherige Konfiguration zu finden und zu verwenden. Dieses Verfahren ist auch bekannt als "Zero Configuration Networking" (ZeroConf).

Zu den gängigsten Diensten zählen z. B.:

- > Druckerdienste (mit oder ohne Apple Airprint Unterstützung)
- > Dateidienste (Ordner- oder Dateifreigaben)
- > Apple Airplay
- > iTunes

2.1.1 Bonjour-Grundlagen

Bonjour nutzt zum Informationsaustausch einzelne Multicast-DNS-Pakete (mDNS) laut [RFC 6762](#) und DNS-Based Service Discovery (DNS-SD) laut [RFC 6763](#). Dabei tauschen Clients die Bonjour-Informationen über die Multicast-Adresse 224.0.0.251 (IPv4) oder ff02::fb (IPv6) auf dem Port 5353 aus. Bonjour-Pakete werden nicht geroutet (Multicast Paket, TTL = 1), was die Nutzung auf das aktuelle lokale Netzwerk beschränkt.

 Bitte beachten Sie, dass der Bonjour-Proxy lediglich zum Auffinden von Bonjour-Diensten dient. Für das entsprechende Routing zwischen den Kommunikationspartnern erfolgt eine separate Konfiguration oder Limitierung, z. B. über Routing- oder Firewall-Einträge.

Oft ist es nicht sinnvoll, alle Dienste in einem einzelnen Netzwerk bereitzustellen. Daher werden größere Netzwerke oft in mehrere Subnetze unterteilt. In diesem Fall kann Bonjour allerdings nicht eingesetzt werden.

Anwendungsbeispiel mit zwei Netzwerken

In einer Schule haben Schüler über ein eigenes IP-Netzwerk Zugang zum WLAN. Parallel dazu stehen in einem zweiten internen IP-Netzwerk die lokalen Drucker zur Verfügung. Generell wäre es einem Schüler durch das Routing und die Restriktionen möglich, von seinem Smartphone auf die lokalen internen Drucker zuzugreifen. Weil mDNS allerdings nur Link-Lokal definiert ist, ist es dem Schüler mit seinem Mobiltelefon allerdings nicht möglich, den gewünschten Drucker mit Bonjour zu ermitteln. Der LANCOM Bonjour Proxy fungiert als Vermittler zwischen zwei Netzwerken und ermöglicht es den Schülern somit, Drucker in anderen Netzwerken zu finden.

Grundsätzlich existieren zur Realisierung eines solchen Szenarios zwei Lösungsmöglichkeiten:

Multicast-Routing

Ein Router leitet Suchanfragen und Dienstanmeldungen zwischen den Netzwerken weiter.

 Diese Option verursacht unnötig Traffic und ist daher wenig effizient.

Caching von Diensten

Der Router speichert entdeckte mDNS-Service-Ankündigungen in seinem lokalen Cache. Erfolgt eine mDNS-Anfrage beim Router, antwortet dieser stellvertretend für den ursprünglichen Dienst. Vor der Verarbeitung der Ankündigung und bevor er aus dem Cache sendet, überprüft der Router anhand von definierten Richtlinien,

ob der Dienst akzeptiert (freigegeben) oder verworfen (gesperrt) wird. Die Policies steuern dabei, zwischen welchen Netzen welche Dienste gefunden werden dürfen.

⚠ Bitte beachten Sie, dass das Auslesen des mDNS-Cache-Inhalts über das SNMP-Protokoll nicht unterstützt wird.

Der Bonjour-Proxy unterstützt einen mDNS-Query-Client, der in festgelegten Zeitintervallen auf einer Schnittstelle bestimmte Dienste abfragt. Diese Abfrage stellt die Aktualität bestimmter Cache-Einträge von freigegebenen Diensten sicher. Damit der Cache stets aktuell gehalten werden kann, ist es sinnvoll, automatische Suchanfragen für die permanent bereitzustellenden Dienste zu aktivieren (z. B. Druckdienste).

⚠ Falls Sie für häufig benötigte Dienste keine automatischen Suchanfragen konfigurieren, kann das dazu führen, dass der Bonjour-Proxy entsprechende Suchanfragen nicht beantworten kann, obwohl diese Dienstanbieter aktiviert sind.

Die Verwendung des Bonjour-Proxies ist nur auf logischen LAN / WLAN-Schnittstellen oder in logischen Netzwerken mit einer IP-Adresse möglich. WAN-Schnittstellen / Gegenstellen oder Tunnel (außer WLC L3-Tunnel) sowie VLANs ohne Adressbindung werden nicht unterstützt.

2.1.2 Konfiguration mit LANconfig

Die Konfiguration des Bonjour-Proxies nehmen Sie in LANconfig unter **IP-Router > Bonjour** vor.

Bonjour-Proxy

Mit dem Bonjour-Proxy können Bonjour-Dienste zwischen unterschiedlichen Netzwerken genutzt werden.

Bonjour-Proxy aktiviert

In dieser Tabelle definieren Sie, zwischen welchen Netzwerken welche Dienste gefunden werden dürfen.

Netzwerk-Liste...

In diesen Tabellen können Sie Listen von Diensten erstellen, die in der Netzwerkliste des Bonjour-Proxies verwendet werden können.

Dienste-Liste... Dienste...

Damit der Bonjour-Proxy jederzeit aktuelle Cache-Einträge vorhalten kann, müssen regelmäßige Suchanfragen nach den gewünschten Diensten durchgeführt werden.

Dienste der Netzwerk-Liste automatisch anfragen

Suchanfragen...

Suchanfrage-Intervall: 15 Minuten

Max. Anzahl der Instanzen: 1.024

In dieser Ansicht stehen Ihnen folgende Einstellungen zur Verfügung:

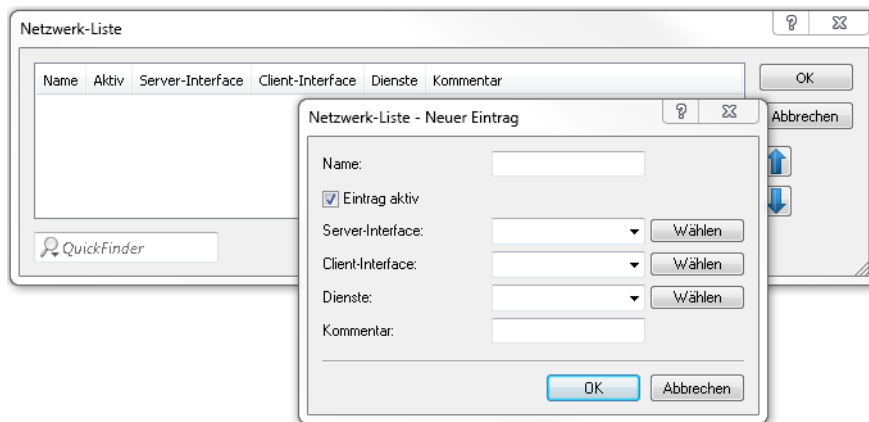
Bonjour-Proxy aktiviert

Aktivieren oder deaktivieren Sie mit dieser Checkbox den Bonjour-Proxy.

Netzwerk-Liste

In dieser Tabelle definieren Sie, zwischen welchen Netzwerken welche Bonjour-Dienste gefunden werden dürfen. Für die ordnungsgemäße Funktionalität ist es erforderlich, dass die Netzwerke oder Schnittstellen mit

einer entsprechenden IPv4- oder IPv6-Adresse konfiguriert sind. Innerhalb der Tabelle haben Sie weitere Einstellungsmöglichkeiten:



Name

Legen Sie einen eindeutigen Namen für diesen Tabelleneintrag fest.

Eintrag aktiv

Aktivieren oder deaktivieren Sie diesen Tabelleneintrag.

Server-Interface

Definieren Sie einen IPv4-Netzwerknamen oder einen IPv6-Interface-Namen, über den Server Bonjour-Dienste (z. B. Druckerdienste) anbieten.

Client-Interface

IPv4-Netzwerkname oder IPv6-Schnittstellen-Name über den Bonjour-Clients Dienste aus dem Server-Netzwerk finden dürfen

Dienste

Referenziert einen Eintrag aus der Dienste-Liste. Clients können nur diese Dienste aus dieser Liste finden. Nicht gelistete Dienste werden abgelehnt.

! Wird kein Eintrag konfiguriert, so sind alle Dienste erlaubt.

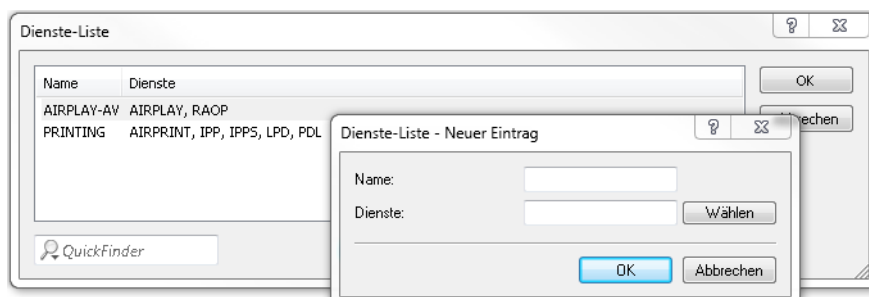
Kommentar

Geben Sie einen Kommentar für diesen Tabelleneintrag ein.

Dienste-Liste

Erstellen Sie in dieser Tabelle eine Liste aus Bonjour-Diensttypen, die in der Bonjour-Netzwerkliste verwendet werden kann.

Hierfür stehen Ihnen folgende Einstellungsmöglichkeiten zur Verfügung:



Name

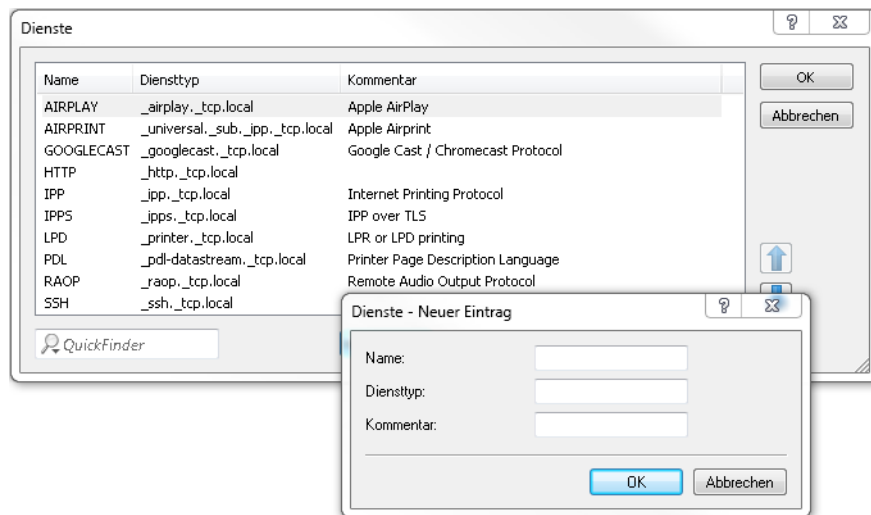
Definieren Sie einen eindeutigen Namen für diesen Tabelleneintrag.

Dienste

Definieren Sie mit einer kommaseparierten Liste die Dienste, die aus der Tabelle **Dienste** verwendet werden sollen.

Dienste

In dieser Tabelle definieren Sie die Typen von Bonjour-Diensten, die in der Dienste-Liste verwendet werden können. Es stehen Ihnen folgende weitere Einstellungsmöglichkeiten zur Verfügung:

**Name**

Legen Sie einen eindeutigen Namen für diesen Tabelleneintrag fest.

Diensttyp

Geben Sie den Bonjour-Diensttyp als DNS SRV Record an, z. B. `_http._tcp.local`.

Kommentar

Geben Sie einen Kommentar für diesen Tabelleneintrag ein.

Dienste der Netzwerk-Liste automatisch anfragen

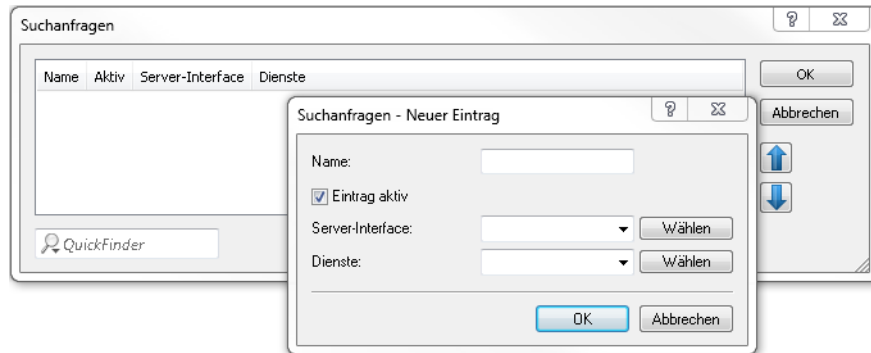
Dieser Eintrag aktiviert das Senden von regelmäßigen Suchanfragen nach den erlaubten Diensten der Netzwerk-Liste auf der entsprechenden Server-Schnittstelle. Als Standardwert ist diese Option aktiviert. Diese Einstellung wird zugleich empfohlen.



Sollte diese Einstellung deaktiviert sein, ist es erforderlich, die abzufragenden Dienste manuell in die Tabelle **Suchanfragen** einzutragen.

Suchanfragen

Damit der Bonjour-Proxy jederzeit aktuelle Dienste im Cache vorhalten kann, ist es erforderlich, dass Sie regelmäßige Suchanfragen nach gewünschten Diensten konfigurieren. Der Query Client fragt in regelmäßigen Abständen die konfigurierten Diensttypen nach deren Verfügbarkeit ab.



Name

Definieren Sie einen eindeutigen Namen für den entsprechenden Eintrag.

Eintrag aktiv

Aktiviert oder deaktiviert diesen Tabelleneintrag.

Server-Interface

Definieren Sie einen IPv4-Netzwerknamen oder einen IPv6-Interface-Namen, über den Server Bonjour-Dienste (z. B. Druckerdienste) anbieten und auf dem regelmäßig durch den Router Suchanfragen durchgeführt werden sollen.

Dienste

Referenziert einen Eintrag aus der Dienste-Liste. Diese Dienste werden regelmäßig durch den Router auf dem Server-Interface angefragt. Dieser Eintrag darf nicht leer sein.

Suchanfrage-Intervall

Legen Sie das Intervall in Minuten fest, in dem der Query-Client die in der Tabelle **Suchanfragen** konfigurierten Bonjour-Dienste abfragt. Als Default sind 15 Minuten definiert.

Max. Anzahl der Instanzen

Definieren Sie die maximale Anzahl an Dienstinstanzen, die der Bonjour-Proxy gleichzeitig speichert.

2.1.3 Ergänzungen im Setup-Menü

Bonjour-Proxy

Dieses Menü enthält die Einstellungsmöglichkeiten für den Bonjour-Proxy. Der Bonjour-Proxy ermöglicht das Auffinden von Bonjour-Diensten über Netzwerkgrenzen hinaus.

SNMP-ID:

2.104

Pfad Telnet:

Setup

Aktiv

Mit diesem Eintrag aktivieren oder deaktivieren Sie den Bonjour-Proxy.

SNMP-ID:

2.104.1

Pfad Telnet:

Setup > Bonjour-Proxy

Mögliche Werte:

nein

ja

Default-Wert:

nein

Query-Client-Intervall

Legen Sie das Intervall in Minuten fest, in dem der Query-Client die in der Tabelle **Query-Client** konfigurierten Bonjour-Dienste anfragt.

SNMP-ID:

2.104.2

Pfad Telnet:

Setup > Bonjour-Proxy

Mögliche Werte:

0 ... 999 Minuten

Default-Wert:

15

Besondere Werte:

0

Netzwerk-Liste

In dieser Tabelle definieren Sie, zwischen welchen Netzwerken welche Bonjour-Dienste gefunden werden dürfen.

SNMP-ID:

2.104.3

Pfad Telnet:

Setup > Bonjour-Proxy

Name

Legen Sie einen eindeutigen Namen für diesen Tabelleneintrag fest.

SNMP-ID:

2.104.3.1

Pfad Telnet:

Setup > Bonjour-Proxy > Netzwerk-Liste

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-,/:;<=>?[\]^_`~`

Default-Wert:

leer

Aktiv

Mit diesem Eintrag aktivieren oder deaktivieren Sie die Verwendung des Bonjour-Proxys für die jeweilige Kombination aus Client- und Server-Netzwerk.

SNMP-ID:

2.104.3.2

Pfad Telnet:

Setup > Bonjour-Proxy > Netzwerk-Liste

Mögliche Werte:

nein
ja

Default-Wert:

nein

Server-Interface

Definieren Sie einen IPv4-Netzwerknamen oder einen IPv6-Interface-Namen, über den Server Bonjour-Dienste (z. B. Druckerdienste) anbieten.

SNMP-ID:

2.104.3.3

Pfad Telnet:

Setup > Bonjour-Proxy > Netzwerk-Liste

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-,/:;<=>?[\]^_`~`

Default-Wert:*leer***Client-Interface**

IPv4-Netzwerkname oder IPv6-Schnittstellen-Name über den Bonjour-Clients Dienste aus dem Server-Netzwerk finden dürfen

SNMP-ID:


2.104.3.4

Pfad Telnet:**Setup > Bonjour-Proxy > Netzwerk-Liste****Mögliche Werte:**

max. 16 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Dienste**

Referenziert einen Eintrag aus der Dienste-Liste. Clients können nur diese Dienste aus dieser Liste finden. Nicht gelistete Dienste werden abgelehnt.

 Wird kein Eintrag konfiguriert, so sind alle Dienste erlaubt.

SNMP-ID:

2.104.3.5

Pfad Telnet:**Setup > Bonjour-Proxy > Netzwerk-Liste****Mögliche Werte:**

max. 16 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Kommentar**

Geben Sie einen Kommentar zu diesem Eintrag ein.

SNMP-ID:

2.104.3.6

Pfad Telnet:**Setup > Bonjour-Proxy > Netzwerk-Liste****Mögliche Werte:**

max. 64 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-./:;<=>[\]^_`~`

Default-Wert:*leer***Dienst-Liste**

Erstellen Sie in dieser Tabelle eine Liste aus Bonjour-Diensttypen, die in der Bonjour-Netzwerkliste verwendet werden kann.

SNMP-ID:

2.104.4

Pfad Telnet:**Setup > Bonjour-Proxy****Name**

Geben Sie hier einen Namen für diese Liste ein.

SNMP-ID:

2.104.4.1

Pfad Telnet:**Setup > Bonjour-Proxy > Dienst-Liste****Mögliche Werte:**

max. 36 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-./:;<=>[\]^_`~`

Default-Wert:*leer***Dienste**

In dieser Tabelle definieren Sie die Typen von Bonjour-Diensten, die in der Dienste-Liste verwendet werden können.



Geben Sie mehrere Dienste durch eine kommaseparierte Liste an.

SNMP-ID:

2.104.4.2

Pfad Telnet:

Setup > Bonjour-Proxy > Dienst-Liste

Mögliche Werte:

max. 252 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Dienste

Diese Tabelle enthält die Default-Dienste für die netzwerkübergreifende Kommunikation. Erweitern Sie die Tabelle Ihren Anforderungen entsprechend.

SNMP-ID:

2.104.5

Pfad Telnet:

Setup > Bonjour-Proxy

Name

Geben Sie hier den Dienstnamen an (z. B. "HTTP").

SNMP-ID:

2.104.5.1

Pfad Telnet:

Setup > Bonjour-Proxy > Dienste

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Dienst-Typ

Geben Sie hier den Typ dieses Dienstes an (z. B. `_http._tcp.local`).

SNMP-ID:

2.104.5.2

Pfad Telnet:

Setup > Bonjour-Proxy > Dienste

Mögliche Werte:

max. 252 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Kommentar

Geben Sie einen Kommentar zu diesem Dienst ein.

SNMP-ID:

2.104.5.6

Pfad Telnet:

Setup > Bonjour-Proxy > Dienste

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Query-Client

Die Tabelle enthält die Dienste, die in regelmäßigen Intervallen vom Router angefragt werden sollen.

SNMP-ID:

2.104.6

Pfad Telnet:

Setup > Bonjour-Proxy

Name

Legen Sie einen eindeutigen Namen für den entsprechenden Eintrag fest.

SNMP-ID:

2.104.6.1

Pfad Telnet:

Setup > Bonjour-Proxy > Query-Client

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Aktiv

Aktivieren oder deaktivieren Sie diesen Eintrag.

SNMP-ID:

2.104.6.2

Pfad Telnet:

Setup > Bonjour-Proxy > Query-Client

Mögliche Werte:

nein
ja

Default-Wert:

nein

Server-Interface

Geben Sie hier das Server-Interface an, über das die Client-Abfrage erfolgen soll.

SNMP-ID:

2.104.6.3

Pfad Telnet:

Setup > Bonjour-Proxy > Query-Client

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>[\]^_`~`

Default-Wert:

leer

Dienste

Geben Sie hier an, welche Dienste angefragt werden sollen.

SNMP-ID:

2.104.6.4

Pfad Telnet:

Setup > Bonjour-Proxy > Query-Client

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-./:;<=>[\]^_`~

Default-Wert:

leer

Instanz-Limit

Definieren Sie die maximale Anzahl an Dienstinstanzen, die der Bonjour-Proxy gleichzeitig speichert.

SNMP-ID:

2.104.7

Pfad Telnet:

Setup > Bonjour-Proxy

Mögliche Werte:

0 ... 4294967295

Default-Wert:

1024

Auto-Dienst-Abfrage

Aktivieren Sie die Checkbox, wenn der Query Client in regelmäßigen Abständen die konfigurierten Diensttypen nach deren Verfügbarkeit abfragen soll.

SNMP-ID:

2.104.8

Pfad Telnet:

Setup > Bonjour-Proxy

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.1.4 Ergänzungen im Status-Menü

Bonjour-Proxy

Dieses Menü enthält die aktuellen Werte des Bonjour-Proxies.

SNMP-ID:

1.104

Pfad Telnet:

Status

Instanz-Anzahl

Dieser Wert zeigt Ihnen die aktuelle Anzahl an Dienstinstanzen im Cache an.

SNMP-ID:

1.104.1

Pfad Telnet:

Status > Bonjour-Proxy

MDNS-Cache

Diese Tabelle enthält Cache-Informationen des Multicast Domain Name Systems (mDNS).

SNMP-ID:

1.104.2

Pfad Telnet:

Status > Bonjour-Proxy

Dienst-Weiterleitung

Diese Tabelle enthält Informationen über die weitergeleiteten Dienste.

SNMP-ID:

1.104.3

Pfad Telnet:

Status > Bonjour-Proxy

Cache-loeschen

Mit diesem Befehl löschen Sie den aktuellen mDNS Cache-Inhalt.

SNMP-ID:

1.104.4

Pfad Telnet:

Status > Bonjour-Proxy

3 WLAN

3.1 Steuerung von WLAN-Sessions mittels RADIUS CoA

Ab LCOS-Version 10.0 haben Sie mit RADIUS CoA (Change of Authorization) die Möglichkeit, die Attribute einer aktuellen WLAN-Verbindung zu modifizieren oder die Verbindung mittels der Methode "disconnect" zu trennen.

 RADIUS CoA wird vom LANCOM L-151gn Wireless nicht unterstützt.

Um die Anmeldung von WLAN-Verbindungen am CoA-Modul zu ermöglichen, können Sie CoA je WLAN-SSID aktivieren. Auf der Konsole haben Sie mit dem Befehl "`show wlan dynamic`" die Möglichkeit, sich die aktuell am CoA-Modul angemeldeten WLAN-Sessions anzeigen zu lassen

Folgende WLAN-Attribute lassen sich durch RADIUS CoA modifizieren:

- > LCS-TxRateLimit
- > LCS-RxRateLimit
- > VLAN-ID

 Für die Modifizierung der VLAN-ID sind folgende Attribute erforderlich:

Tunnel-Type=VLAN

Dieses Attribut ist vorgegeben

Tunnel-Medium-Type=IEEE-802

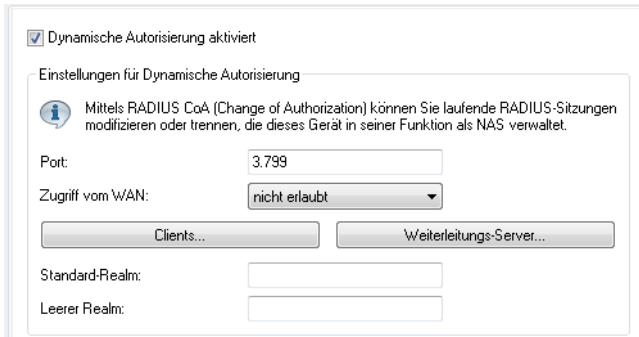
Dieses Attribut ist vorgegeben

Tunnel-Private-Group-Id=42

Definiert eine neue VLAN-ID

3.1.1 Steuerung von WLAN-Sessions mittels RADIUS CoA mit LANconfig konfigurieren

Um die dynamische Autorisierung (CoA) mit LANconfig zu konfigurieren, öffnen Sie die Ansicht **RADIUS > Dyn. Autorisierung**.



The screenshot shows a configuration window titled "Dynamische Autorisierung aktiviert". It contains a section "Einstellungen für Dynamische Autorisierung" with an information icon and a note: "Mittels RADIUS CoA (Change of Authorization) können Sie laufende RADIUS-Sitzungen modifizieren oder trennen, die dieses Gerät in seiner Funktion als NAS verwaltet." Below this, there are input fields for "Port" (3.799) and a dropdown for "Zugriff vom WAN" (nicht erlaubt). There are also buttons for "Clients..." and "Weiterleitungs-Server...". At the bottom, there are empty input fields for "Standard-Realm:" and "Leerer Realm:".

Dynamische Autorisierung aktiviert

Hier aktivieren oder deaktivieren Sie die dynamische Autorisierung.

Port

Enthält den Standard-Port, auf dem CoA-Nachrichten angenommen werden.

Zugriff vom WAN

Dieser Eintrag legt fest, ob Nachrichten vom WAN zugelassen sind, nur über VPN angenommen werden oder verboten sind.

Clients

Tragen Sie hier alle CoA-Clients ein, die Nachrichten an das NAS senden dürfen.

Weiterleitungs-Server

Sollen CoA-Nachrichten weitergeleitet werden, ist es erforderlich, die Weiterleitungen hier anzugeben.

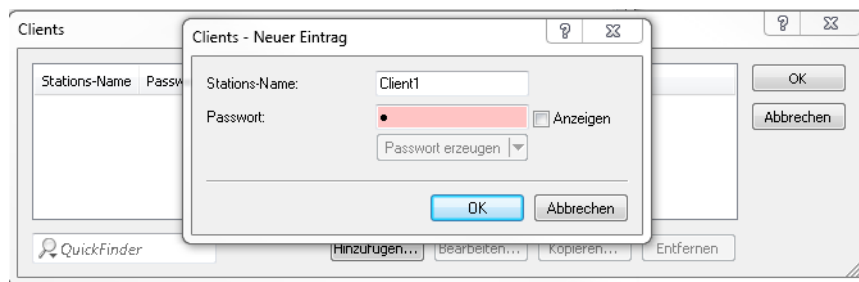
Standard-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername einen unbekanntem Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

Leerer Realm

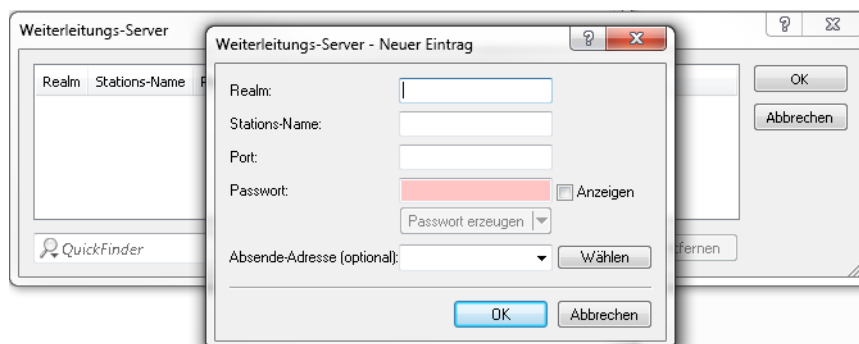
Dieser Realm gilt alternativ, wenn der übermittelte Benutzername keinen Realm enthält.

Um CoA-Clients für die dynamische Autorisierung hinzuzufügen, klicken auf die Schaltfläche **Clients** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Tragen Sie einen Stationsnamen für den Client ein und definieren Sie ein Passwort, das der Client für den Zugang zum NAS benötigt.

Um neue Weiterleitungs-Server für die dynamische Autorisierung hinzuzufügen, klicken Sie auf die Schaltfläche **Weiterleitungs-Server** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Realm

Tragen Sie hier den Realm ein, mit dem der RADIUS-Server das Weiterleitungs-Ziel identifiziert.

- i Verwenden Sie ggf. bereits vorhandene Weiterleitungs-Server, die unter **RADIUS > Server > Weiterleitung > Weiterleitungs-Server** definiert sind.

Stations-Name

Geben Sie den Hostnamen des Weiterleitungs-Servers an.

Port

Legen Sie den Port des Servers fest, über den die Anfragen weitergeleitet werden.

Passwort

Legen Sie ein Passwort fest, das der Client für den Zugang zum RADIUS-Server benötigt.

Absende-Adresse (optional)

Geben Sie optional eine Absendeadresse an.

Legen Sie fest, welche logischen WLAN-Schnittstellen die dynamische Autorisierung verwenden dürfen. Aktivieren oder deaktivieren Sie hierfür im Reiter "Netzwerk" unter **Wireless-LAN > Allgemein > Logische WLAN-Einstellungen** beim jeweiligen Interface die Checkbox **RADIUS CoA aktiviert**.

3.1.2 Ergänzungen im Setup-Menü

Dyn-Auth

Dieses Menü enthält die Einstellungen für die dynamische Autorisierung durch RADIUS CoA (Change of Authorization). RADIUS CoA ist in [RFC5176](#) spezifiziert.

SNMP-ID:

2.25.19

Pfad Telnet:

Setup > RADIUS

Aktiv

Dieser Eintrag aktiviert oder deaktiviert die dynamische Autorisierung durch RADIUS.

SNMP-ID:

2.25.19.1

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Mögliche Werte:

nein
ja

Default-Wert:

nein

Port

Dieser Eintrag legt den Port fest, auf dem CoA Nachrichten angenommen werden.

SNMP-ID:

2.25.19.2

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Mögliche Werte:

max. 5 Zeichen aus [0–9]

Default-Wert:

3799

WAN-Zugang

Dieser Eintrag legt fest, ob Nachrichten vom LAN, WAN oder über VPN angenommen werden.

SNMP-ID:

2.25.19.3

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Mögliche Werte:

nein
ja

Default-Wert:

nein

Clients

In diese Tabelle werden alle CoA-Clients eingetragen, die Nachrichten an das NAS senden.

SNMP-ID:

2.25.19.4

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

HostName

Dieser Eintrag enthält die eindeutige Bezeichnung des Clients, der Nachrichten an das NAS sendet.

SNMP-ID:

2.25.19.4.1

Pfad Telnet:

Setup > RADIUS > Dyn-Auth > Clients

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#@[|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Secret

Dieser Eintrag legt das Kennwort fest, das der Client für den Zugang zum NAS im Access Point benötigt.

SNMP-ID:

2.25.19.4.2

Pfad Telnet:

Setup > RADIUS > Dyn-Auth > Clients

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#@[|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

leer

Weiterleit-Server

Sollen CoA-Nachrichten weitergeleitet werden, ist es erforderlich, die Weiterleitungen hier anzugeben.

SNMP-ID:

2.25.19.5

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Realm

Dieser Eintrag enthält eine Zeichenkette, mit der der RADIUS-Server das Weiterleitungs-Ziel identifiziert.

SNMP-ID:

2.25.19.5.1

Pfad Telnet:**Setup > RADIUS > Dyn-Auth > Weiterleit-Server****Mögliche Werte:**

max. 16 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***HostName**

Geben Sie hier den Host-Namen des RADIUS-Servers an, an den der RADIUS-Client die Anfrage von WLAN-Clients weiterleiten soll.

SNMP-ID:

2.25.19.5.2

Pfad Telnet:**Setup > RADIUS > Dyn-Auth > Weiterleit-Server****Mögliche Werte:**

max. 64 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Port**

Dieser Eintrag enthält den Port, über den mit dem Weiterleitungs-Server kommuniziert werden kann.

SNMP-ID:

2.25.19.5.3

Pfad Telnet:**Setup > RADIUS > Dyn-Auth > Weiterleit-Server****Mögliche Werte:**

max. 10 Zeichen aus [0-9]

Default-Wert:

0

Secret

Dieser Eintrag legt das Kennwort fest, das für den Zugang zum Weiterleitungs-Server benötigt wird.

SNMP-ID:

2.25.19.5.4

Pfad Telnet:

Setup > RADIUS > Dyn-Auth > Weiterleit-Server

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#@[|}~!\$%&'()*+,-,/:;=>?[\]^_`~`

Default-Wert:

leer

Loopback

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

SNMP-ID:

2.25.19.5.5

Pfad Telnet:

Setup > RADIUS > Dyn-Auth > Weiterleit-Server

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#@[|}~!\$%&'()*+,-,/:;=>?[\]^_`~`

Default-Wert:

leer

Standard-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername einen unbekanntem Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

SNMP-ID:

2.25.19.6

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#@[|}~!\$%&'()*+,-,/:;=>?[\]^_`~`

Default-Wert:

leer

Leerer-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername keinen Realm enthält.

SNMP-ID:

2.25.19.7

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-,/:;<=>?[\]^_`~`

Default-Wert:

leer

Radclient

Verwenden Sie den Befehl `do Radclient [...]`, um CoA-Nachrichten versenden.

Das Radclient-Kommando ist wie folgt aufgebaut:

```
do Radclient <Server[:Port]> coa/disconnect <Passwort> <Attributliste>
```

Ausgabe aller bekannten und aktiven RADIUS-Sitzungen

Mit dem Befehl `show dynauth sessions` auf der Kommandozeile listen Sie die RADIUS-Sitzungen auf, die dem CoA-Modul bekannt sind. Die durch das Public Spot-Modul angemeldete Sitzung wird ausgegeben. Die bekannten Attribute dieser Sitzung finden Sie im Abschnitt "Context":

```
Session with MAC-Address: [a3:18:22:0c:ae:df] Context:
[NAS-IP-Address: 192.168.1.254, User-Name: user46909, NAS-Port-Id:
WLC-TUNNEL-1, Framed-IP-Address: 192.168.1.78]
```

Anhand der Attribute "NAS-IP-Address" und "User-Name" wird die aktive Sitzung identifiziert. Möchten Sie für die aktive Session z. B. ein Bandbreitenlimit festlegen, übergeben Sie dem Radclient-Kommando neben dieser Werte zusätzlich die Attribute "LCS-TxRateLimit" und "LCS-RxRateLimit" mit den entsprechenden Send- und Empfangs-Limitierungen in KBit/s :

```
do Radclient 192.168.1.254 coa password
"User-Name=user46909;NAS-IP-Address=192.168.1.254;LCS-TxRateLimit=5000;LCS-RxRateLimit=5000"
```



Bitte beachten Sie, dass sowohl die Identifikations-Attribute als auch die zu bearbeitenden Attribute innerhalb der Attributliste gleichberechtigt angegeben werden.

Beenden einer aktiven RADIUS-Sitzung

Versenden Sie mit dem Radclient-Kommando eine Disconnect-Message, um eine laufende RADIUS-Sitzung zu beenden:

```
do Radclient 192.168.1.254 disconnect password
"User-Name=user46909;NAS-IP-Address=192.168.1.254"
```



Das im LCOS integrierte Radclient-Kommando dient hauptsächlich Testzwecken. CoA-Nachrichten werden normalerweise von einem externen System an das NAS versandt.

SNMP-ID:

2.25.19.8

Pfad Telnet:

Setup > RADIUS > Dyn-Auth

Dyn-Auth

Mit diesem Eintrag aktivieren oder deaktivieren Sie für die jeweilige Schnittstelle die dynamische Autorisierung durch RADIUS CoA.

SNMP-ID:

2.23.20.1.28

Pfad Telnet:

Setup > Schnittstellen > WLAN > Netzwerk

Mögliche Werte:

nein
ja

Default-Wert:

nein

4 WLAN-Management

4.1 WLC-Skript-Rollout für bestimmte LCOS-Versionen

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, WLC-gesteuerte Skript-Rollouts für bestimmte LCOS-Versionen festzulegen und somit abweichende Konfigurationen unterschiedlicher LCOS-Versionen in eine WLAN-Installation zu integrieren.

4.1.1 WLC-Skript-Rollout mit LANconfig konfigurieren

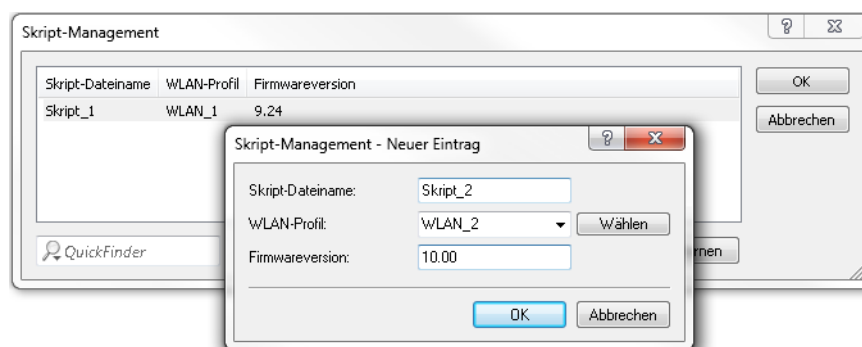
Unter Umständen ist es innerhalb einer WLAN-Installation erforderlich, die Konfigurationen mehrerer LCOS-Versionen berücksichtigen zu müssen. Mit LANconfig haben Sie mit dem Skript-Management die Möglichkeit, für Ihre WLAN-Profil Skripte mit bestimmten Firmware-Versionen auszurollen.

ⓘ Bitte beachten Sie, dass es nicht möglich ist, einem WLAN-Profil mehrere Skripte mit unterschiedlichen Firmware-Versionen zuzuweisen.

Die Skript-Management-Tabelle finden Sie in LANconfig unter **WLAN-Controller > AP-Update > Skript-Management**.

Fügen Sie der Tabelle einen neuen Eintrag hinzu, um für Ihre WLAN-Profil neue Skripte zu definieren.

Der Dialog in LANconfig hat sich wie folgt geändert:



> Firmwareversion

Mit der Angabe einer Firmwareversion legen Sie fest, für welche LCOS-Version das entsprechende Skript ausgerollt werden soll.

ⓘ Bitte beachten Sie, die Firmware in der Form **xx.yy** anzugeben, z. B. 10.00 oder 9.24.

4.1.2 Ergänzungen im Setup-Menü

Firmwareversion

Legen Sie hier die Firmwareversion fest, für welche das entsprechende Skript ausgerollt werden soll.

ⓘ Bitte beachten Sie, die Firmware in der Form **xx.yy** anzugeben, z. B. 10.00 oder 9.24.

SNMP-ID:

2.37.27.16.3

Pfad Telnet:

Setup > WLAN-Management > Zentrales-Firmware-Management > Skriptverwaltung

Mögliche Werte:

max. 6 Zeichen aus [0-9] .

Default-Wert:

leer

5 Public Spot

5.1 Anfordern der Benutzer-E-Mail-Adresse beim Login nach Einverständniserklärung

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, die Nutzung Ihres Public Spots von einer Benutzerregistrierung abhängig zu machen, indem Sie die E-Mail-Adresse der Nutzer abfragen.

5.1.1 Adressanforderung mit LANconfig konfigurieren

Für die Anmeldung am Public Spot haben Sie durch die Sie die Abfrage der E-Mail-Adresse des Benutzers die Möglichkeit, eine vorherige Registrierung für die Nutzung Ihres Public Spots zu verlangen. Diese Einstellungen für die Authentifizierung am Netzwerk legen Sie im Dialog **Public-Spot > Anmeldung** im Abschnitt "Login nach Einverständniserklärung" fest.

Der Dialog hat sich wie folgt geändert:

Authentifizierung für den Netzwerk-Zugriff

Anmeldungs-Modus:

Keine Anmeldung nötig

Keine Anmeldung nötig (Login nach Einverständniserklärung)

Anmeldung mit Name und Passwort

Anmeldung mit Name, Passwort und MAC-Adresse

Anmeldeinformationen werden über E-Mail versendet

Anmeldeinformationen werden über SMS versendet

Nutzungsbedingungen müssen akzeptiert werden

Verwendetes Protokoll der Login-Seite

Aufruf der Login-Seite über:

HTTPS - Login- und Statusseiten werden verschlüsselt übertragen

HTTP - Login- und Statusseiten werden unverschlüsselt übertragen

Login nach Einverständniserklärung

Maximal pro Stunde: Anfragen

Maximal pro Tag: Benutzer-Konten

Benutzernamenspräfix:

E-Mail-Adresse des Benutzers abfragen

Benutzerliste versenden an:

Benutzerliste versenden alle: Minuten

Personalisierung

Hier können Sie optional einen personalisierten Text eingeben, der auf der Login-Seite angezeigt wird.

- > **E-Mail-Adresse des Benutzers abfragen:** Aktivieren Sie diese Checkbox, um die E-Mail-Adresse des Nutzers für die Verwendung des Public Spot abzufragen. Die hier angegebene E-Mail-Adresse trägt das Gerät automatisch im Kommentarfeld des neu angelegten RADIUS-Benutzers ein. Eine Liste aller vorhandenen Adressen wird täglich einmal im Flash-Speicher des Gerätes abgelegt und bleibt auch im Falle eines Neustartes bestehen.
- > **Benutzerliste versenden an:** Geben Sie hier die E-Mail-Adresse an, an die die Adressliste gesendet werden soll. Es werden nur Informationen gesendet, die seit der letzten Übermittlung neu hinzugekommen sind. Die Übermittlung der Adressliste erfolgt als CSV-Datei.
- > **Benutzerliste versenden alle:** Legen Sie fest, in welchem Intervall die aktualisierte Adressliste an die angegebene E-Mail-Adresse übermittelt werden soll. Der Wert wird in Minuten angegeben.

Über den Setup-Wizard **Public Spot-gesammelte E-Mail-Adressen** in WEBconfig haben Sie die Möglichkeit, die registrierten Adressen einzusehen und als CSV-Datei zu exportieren.

! Beachten Sie bitte, dass der Wizard nur bei aktivierter E-Mail-Abfrage sichtbar ist. Ggf. ist eine erneute Anmeldung am Gerät erforderlich.

The screenshot shows the LANCOM Systems web interface for the IP address 192.168.8.104. The page title is "192.168.8.104 - Public Spot-gesammelte E-Mail-Adressen". There is a button "Als CSV speichern" and a search field. Below is a table with columns "Benutzername", "Erstellt", and "E-Mail".

Benutzername	Erstellt	E-Mail
freeD5zoc	11/24/2016 13:17:06	Test@lancom.de
LCS8zpEP	11/24/2016 13:28:02	Neueruser@pspot.com
LCSa7PRB	11/24/2016 13:26:55	Neueruser@pspot.com
LCSIEkFR	11/24/2016 13:24:50	pspot@lancom.de

Below the table, it says "Angezeigt werden Einträge 1 bis 4 (4 Einträge)". A dialog box titled "Öffnen von freelloginusers.csv" is open, showing the file name "freelloginusers.csv", its type "Microsoft Excel-CSV-Datei", and the URL "http://192.168.8.104". The dialog asks how to handle the file, with options "Öffnen mit Microsoft Excel (Standard)", "Datei speichern", and "Für Dateien dieses Typs immer diese Aktion ausführen".

5.1.2 Ergänzungen im Setup-Menü

E-Mail-anfordern

Mit diesem Eintrag legen Sie fest, ob die E-Mail-Adresse des Benutzers abgefragt werden soll.

SNMP-ID:

2.24.41.4.4

Pfad Telnet:

Setup > Public-Spot-Modul > Authentifizierungs-Module > Login-nach-Einverstaendniserklaerung

Mögliche Werte:

nein
ja

Default-Wert:

nein

E-Mail-Listen-Empfänger

Dieser Eintrag enthält die E-Mail-Adresse, an die die Adressliste der E-Mail-Abfrage gesendet werden soll.



Sofern Sie die E-Mail-Adresse des Empfängers in LANconfig bereits festgelegt haben, wird diese Ihnen hier angezeigt.

SNMP-ID:

2.24.41.4.7

Pfad Telnet:

Setup > Public-Spot-Modul > Authentifizierungs-Module > Login-nach-Einverstaendniserklaerung

Mögliche Werte:

max. 150 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-/:;=>?[\\]^_`~`

Default-Wert:

leer

5.1.3 Ergänzungen im Status-Menü

Free-Login

In diesem Menü haben Sie die Möglichkeit, die Benutzer des Anmelde-Modus "Login nach Einverständniserklärung" einzusehen oder zu löschen.

SNMP-ID:

1.44.17

Pfad Telnet:

Status > Public-Spot

Benutzer

Dieser Eintrag zeigt alle aktiven Benutzer des Anmelde-Modus "Login nach Einverständniserklärung" an.

SNMP-ID:

1.44.17.1

Pfad Telnet:

Status > Public-Spot > Free-Login

Mögliche Werte:

Benutzername

Zeigt den Namen des angelegten Benutzers an.

Erstellt

Zeit den Zeitpunkt an, an dem der Benutzer angelegt wurde.

E-Mail

Zeigt die eingetragene E-Mail-Adresse des angelegten Benutzers an



Dieses Feld enthält nur Informationen, wenn die Option "E-Mail-Adresse des Benutzers abfragen" aktiviert ist.

Benutzer-loeschen

Mit diesem Eintrag haben Sie die Möglichkeit, die angelegten Benutzer des Anmelde-Modus "Login nach Einverständniserklärung" zu löschen.

SNMP-ID:

1.44.17.2

Pfad Telnet:

Status > Public-Spot > Free-Login

5.2 Konfigurieren der Überschrift der Public Spot-Login-Seite

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, der Login-Seite Ihres Public Spots eine Überschrift hinzuzufügen.

Definieren Sie den Titel Ihrer Login-Seite in sechs verschiedenen Sprachen. Hierbei stehen Ihnen Deutsch, Englisch, Französisch, Italienisch, Spanisch und Niederländisch zur Verfügung. Der Titel Ihrer Public Spot Login-Seite wird in Abhängigkeit der vom Benutzer eingestellten Browsersprache ausgegeben.

5.2.1 Individueller Text oder Login-Titel auf der Anmeldeseite

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuellen **Login-Text** und einen **Login-Titel** anzugeben, welche auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Sowohl Text als auch Titel sind in mehreren Sprachen definierbar (Deutsch, Englisch, Französisch, Italienisch, Spanisch und Niederländisch). Welche Sprache das Gerät letztlich ausgibt, hängt von den Spracheinstellungen des vom Benutzer verwendeten Webbrowsers ab. Wenn Sie für eine Sprache keinen individuellen Login-Text oder Titel spezifizieren, greift das Gerät auf den englischen Login-Text zurück (sofern vorhanden).



Bitte beachten Sie, dass es sich bei Login-Text und Login-Titel um unterschiedliche Elemente handelt!

Um einen individuellen Text oder einen Login-Titel auf der Anmeldeseite einzurichten, führen Sie die nachfolgenden Schritte aus.

1. Öffnen Sie in LANconfig den Konfigurationsdialog für das betreffende Gerät.

2. Wechseln Sie in den Dialog **Public Spot > Anmeldung**, klicken Sie auf die Schaltfläche **Login-Text** (alternativ **Login-Titel**) und wählen Sie eine Sprache aus.

Authentifizierung für den Netzwerk-Zugriff

Anmeldungs-Modus:

Keine Anmeldung nötig

Keine Anmeldung nötig (Login nach Einverständniserklärung)

Anmeldung mit Name und Passwort

Anmeldung mit Name, Passwort und MAC-Adresse

Anmeldeinformationen werden über E-Mail versendet

Anmeldeinformationen werden über SMS versendet

Nutzungsbedingungen müssen akzeptiert werden

Verwendetes Protokoll der Login-Seite

Aufruf der Login-Seite über:

HTTPS - Login- und Statusseiten werden verschlüsselt übertragen

HTTP - Login- und Statusseiten werden unverschlüsselt übertragen

Login nach Einverständniserklärung

Maximal pro Stunde: Anfragen

Maximal pro Tag: Benutzer-Konten

Benutzernamenspräfix:

E-Mail-Adresse des Benutzers abfragen

Benutzerliste versenden an:

Benutzerliste versenden alle: Minuten

Personalisierung

Hier können Sie optional einen personalisierten Text eingeben, der auf der Login-Seite angezeigt wird.

3. Tragen Sie in dem sich öffnenden Dialog den Text ein, den Sie Ihren Public Spot-Nutzern anzeigen möchten. Erlaubt ist ein HTML-String mit max. 254 Zeichen, bestehend aus:

```
[Leerzeichen][0-9][A-Z[a-z] @{ | }~!$%&'()+-,/;:&lt;=>?[\]^_.*
```

LANconfig transformiert eingegebene Umlaute automatisch in ihre entsprechenden Umschreibungen (ü zu ue; ß zu ss; usw.). Um Umlaute einzugeben, müssen Sie deren HTML-Äquivalente verwenden (z. B. ü für ü), da der Text unmittelbar in die Webseite eingebunden wird. Über HTML-Tags haben Sie außerdem die Möglichkeit, den Text zusätzlich zu strukturieren und zu formatieren. Beispiel:

```
Herzlich Willkommen!<br/><i>Bitte füllen Sie das Formular aus.</i>
```

4. Klicken Sie **OK**, um die Eingabe abzuschließen, und laden Sie die Konfiguration zurück in das Gerät.

Nach dem erfolgreichen Schreiben der Konfiguration erscheinen Login-Text und Login-Titel beim nächsten Aufruf der Public Spot-Seite.

Dies ist der Login-Text

Dies ist der Login-Titel

Passwort anzeigen

Nutzungsbedingungen akzeptieren

Powered by
LANCOM
Systems

5.2.2 Ergänzungen im Setup-Menü

Login-Anweisungen

In diesem Menü legen Sie einen Login-Titel für Ihre Public Spot Seite fest. Den Titel können Sie in sechs Sprachen definieren (Deutsch, Englisch, Französisch, Italienisch, Spanisch und Niederländisch).

SNMP-ID:

2.24.61

Pfad Telnet:**Setup > Public-Spot-Modul**

Sprache

Dieser Eintrag zeigt die jeweils ausgewählte Sprache für den Login Titel an.

SNMP-ID:

2.24.61.1

Pfad Telnet:**Setup > Public-Spot-Modul > Login-Anweisungen**

Inhalt

Geben Sie hier den Login Titel für Ihren Public Spot an.

SNMP-ID:

2.24.61.1

Pfad Telnet:**Setup > Public-Spot-Modul > Login-Anweisungen****Mögliche Werte:**

max. 251 characters from [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`


Default-Wert:*leer*

5.3 Bestätigung der Nutzungsbedingungen auf der PMS-Login-Seite

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, den Benutzer die Nutzungsbedingungen Ihres Public Spots auch auf der PMS-Login-Seite bestätigen zu lassen.

5.3.1 Bestätigung der Nutzungsbedingungen auf der PMS-Login-Seite mit LANconfig konfigurieren

Aktivieren Sie in LANconfig unter **Public-Spot > PMS-Schnittstelle** im Abschnitt "Anmelde-Einstellungen" die Checkbox **Nutzungsbedingungen müssen akzeptiert werden**.

 Bitte beachten Sie, dass für die Nutzung dieser Option die PMS-Schnittstelle aktiv sein muss.

Der Dialog zur PMS-Schnittstelle hat sich wie folgt geändert:

PMS-Schnittstelle aktiviert

Verbindungs-Einstellungen

PMS-Protokoll: Micros Fidelio TCP/IP

PMS-Server-IP-Adresse:

PMS-Port:

Absende-Adresse (optional):

Accounting-Informationen im Flash-ROM ablegen

Anmelde-Einstellungen

Login-Seite:

Mehrfachanmeldung zulassen

Zusätzliche Anmeldung über Tickets anbieten

Nutzungsbedingungen müssen akzeptiert werden

Währung:

➤ **Nutzungsbedingungen müssen akzeptiert werden:** Aktivieren Sie diese Checkbox, um Hotelgäste die Nutzungsbedingungen zur Verwendung Ihres Hotspots bestätigen zu lassen.

Auf der PMS-Login-Seite erscheint nach aktivierter Option die Checkbox zum Bestätigen der Nutzungsbedingungen.

[Login mit vorhandenem Voucher](#)

Login mit Reservierungsdaten

▼

[Nutzungsbedingungen akzeptieren](#)

5.3.2 Ergänzungen im Setup-Menü

Benutzer-muss-AGBs-akzeptieren

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Bestätigung der Nutzungsbedingungen auf der PMS-Login-Seite.

SNMP-ID:

2.64.11.14

Pfad Telnet:

Setup > PMS-Interface > Login-Formular

Mögliche Werte:

nein

Der Benutzer wird nicht dazu aufgefordert, die Nutzungsbedingungen zu akzeptieren.

ja


Der Benutzer wird dazu aufgefordert, die Nutzungsbedingungen zu akzeptieren.

Default-Wert:

nein

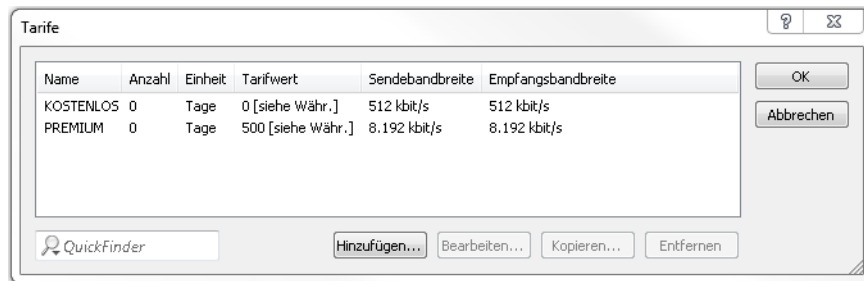
5.4 Tx- und Rx-Bandbreiten für Tarife im PMS-Modul konfigurierbar

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, für die im PMS-Modul konfigurierten Tarife jeweils eine Sende- und eine Empfangsbandbreitenlimitierung zu definieren und die Tarife namentlich zu benennen, z. B. "kostenlos" und "Premium". Bei der Tarifauswahl auf der Public Spot-Login-Seite werden dem Benutzer dann die Tarife mit den konfigurierten Namen angezeigt.

 Sollten bei einem Firmware-Update bereits Tarife in der Konfiguration enthalten sein, werden ihnen nach dem Muster **Tarif_1** bis **Tarif_n** automatisch einen Namen zugewiesen.

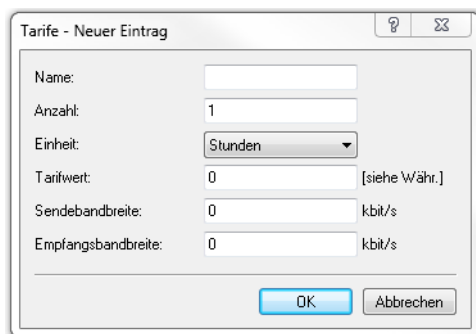
5.4.1 Tx- und Rx-Bandbreiten für Tarife im PMS-Modul mit LANconfig konfigurieren

Die Tarife in der PMS-Schnittstelle Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot > PMS-Schnittstelle > Tarife**.



Bearbeiten Sie bestehende Tarife oder fügen Sie der Tabelle neue Einträge hinzu. Der Dialog hat sich dabei wie folgt geändert:

- > **Tarife:** Sofern Sie einen kostenpflichtigen Internetzugang anbieten, verwalten Sie über diese Tabelle die Tarife für das Accounting.



- **Name:** Legen Sie hier einen aussagekräftigen Tarifnamen fest.
- **Anzahl:** Geben Sie hier die Höhe des Zeitkontingents ein, z. B. 1. In Kombination mit der Einheit entspricht dies im oben gezeigten Screenshot z. B. 1 Stunde.
- **Einheit:** Wählen Sie aus der Liste eine Einheit für das Zeitkontingent aus. Mögliche Werte sind: *Minuten, Stunden, Tage*
- **Tarifwert:** Geben Sie hier die Höhe des Betrags ein, mit dem Sie die Zeitkontingente vergelten. In Kombination mit der in den Anmelde-Einstellungen gewählten Währung entspricht dies z. B. 50 Cent.
- **Sendebandbreite:** Definieren Sie hier die maximal zulässige Sendebandbreite für diesen Tarif.
- **Empfangsbandbreite:** Definieren Sie hier die maximal zulässige Empfangsbandbreite für diesen Tarif.



Eine temporäre Abmeldung vom Public Spot verschiebt nicht den Ablaufzeitpunkt eines eingekauften Zeitkontingents! Es nicht möglich, ein bereits gekauftes Zeitguthaben zu "pausieren", um es zu einem späteren Zeitpunkt erneut aufzunehmen. Die Herunterzählung der Zeit beginnt unabhängig vom Anmeldestatus ab Kauf des Kontingents.

5.4.2 Ergänzungen im Setup-Menü

Name

Definieren Sie mit diesem Eintrag einen Namen für diesen Tarif

SNMP-ID:

2.64.15.4

Pfad Telnet:

Setup > PMS-Interface > Tarif

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{ | }~!$%&'()*+,-./:;<=>?[\]^_`~``

Default-Wert:

leer

Tx-Bandbreite

Begrenzen Sie mit diesem Eintrag eine Sendebandbreite (Tx).

SNMP-ID:

2.64.15.5

Pfad Telnet:

Setup > PMS-Interface > Tarif

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Default-Wert:

0

Besondere Werte:

0

Der Wert "0" deaktiviert die Limitierung der Sendebandbreite.

Rx-Bandbreite

Begrenzen Sie mit diesem Eintrag eine Empfangsbandbreite (Rx).

SNMP-ID:

2.64.15.6

Pfad Telnet:**Setup > PMS-Interface > Tarif****Mögliche Werte:**

max. 10 Zeichen aus [0–9]

Default-Wert:

0

Besondere Werte:

0

Der Wert "0" deaktiviert die Limitierung der Empfangsbandbreite.

5.5 Unterstützung von RADIUS CoA

Ab LCOS-Version 10.0 haben Sie im Public Spot-Modul die Möglichkeit, die Annahme von RADIUS CoA-Befehlen zu aktivieren.

 RADIUS CoA wird vom LANCOM L-151gn Wireless nicht unterstützt.

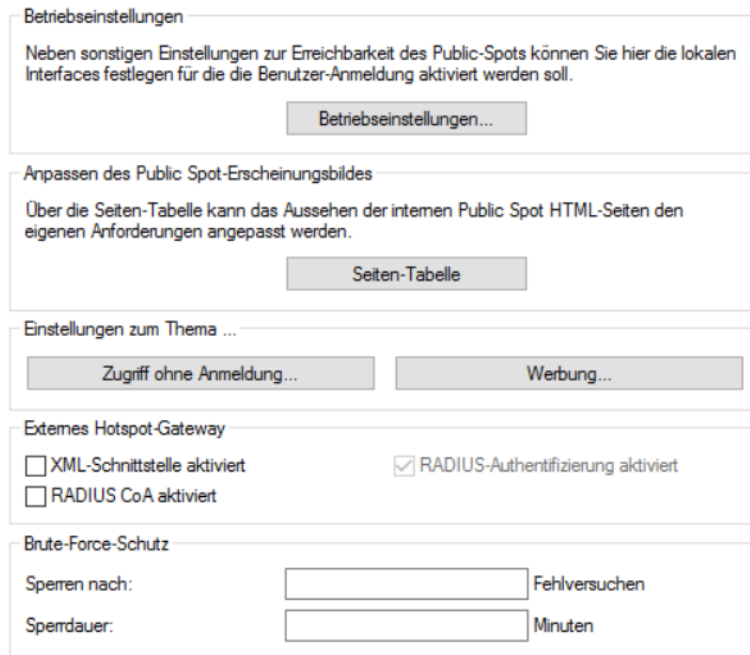
5.5.1 Annahme von RADIUS-CoA-Requests im Public Spot aktivieren

- > Die nachfolgenden Handlungsschritte setzen einen funktionierenden Public Spot voraus, welcher an ein externes Hotspot-Gateway angebunden werden kann.
- > Das externe Hotspot-Gateway befindet sich entweder in einem frei zugänglichen Netz des Public Spots oder seine Adresse gehört zur Liste der freien Hosts.

Alternativ zu einem XML-basierten `RADIUS_COA_REQUESTS` über das XML-Interface kann der Public Spot auch CoA-Requests über das RADIUS-Protokoll von einem externen Hotspot-Gateway oder einem externen RADIUS-Server entgegen nehmen. Sie haben jedoch auch die Möglichkeit, beide Formen der Befehlsübermittlung parallel zu nutzen.

Der folgende Abschnitt erläutert, wie Sie die RADIUS-CoA-Unterstützung nach RFC3576 im Public Spot aktivieren.

1. Öffnen Sie die Gerätekonfiguration in LANconfig und wechseln Sie in die Ansicht **Public-Spot > Server**.



2. Wählen Sie **RADIUS CoA aktiviert** an.
3. Schreiben Sie die Konfiguration zurück in das Gerät.

Der Public Spot verarbeitet fortan RADIUS-CoA-Requests, die von einem externen Hotspot-Gateway eingehen.

5.5.2 Ergänzungen im Setup-Menü

CoA-zulassen

Alternativ zu einem XML-basierten `RADIUS_COA_REQUESTS` über das XML-Interface kann der Public Spot auch CoA-Requests über das RADIUS-Protokoll von einem externen Hotspot-Gateway oder einem externen RADIUS-Server entgegen nehmen. Sie haben jedoch auch die Möglichkeit, beide Formen der Befehlsübermittlung parallel zu nutzen.

Mit diesem Eintrag aktivieren oder deaktivieren Sie die dynamische Autorisierung von Public Spot-Benutzern mittels RADIUS CoA über ein externes Hotspot-Gateway.

SNMP-ID:

2.24.55

Pfad Telnet:

Setup > Public-Spot-Modul

Mögliche Werte:

Nein

Dynamische Autorisierung deaktiviert. Wenn sich die RADIUS-Verbindungsattribute ändern, bleiben autorisierte Benutzer davon unberührt, bis deren Sitzung abläuft.

Ja

Dynamische Autorisierung aktiviert. Das externe Gateway kann Verbindungsattribute autorisierter Benutzer modifizieren oder bestehende Sitzungen trennen.

Default-Wert:

Nein

6 RADIUS

6.1 Unterstützung von Tunnel-Passwort- und LCS-Routing-Tag Attributen

Ab LCOS-Version 10.0 unterstützen LANCOM RADIUS-Server die Attribute "Tunnel-Passwort" und "LCS-Routing-Tag", welche Sie in den Benutzerkonten definieren können.

Daraus ergibt sich die Möglichkeit, die Benutzerdaten innerhalb eines Unternehmens zentral im RADIUS-Server zu speichern und den Konfigurationsaufwand für VPN-Szenarien zu minimieren.

6.1.1 Tunnel-Passwort und Routing-Tag-Attribute mit LANconfig konfigurieren

Definieren Sie in LANconfig die Attribute "Tunnel-Passwort" und "Routing-Tag" unter **RADIUS > Server > Benutzerkonten**.

Fügen Sie der Tabelle einen neuen Eintrag hinzu oder bearbeiten Sie einen bestehenden Eintrag.

Legen Sie im Abschnitt "Tunnel-Parameter" die entsprechenden Attribute fest:

Tunnel-Passwort

Tragen Sie hier das Kennwort ein, mit dem sich der jeweilige Benutzer für eine VPN-Verbindung über IKEv2 oder L2TP authentifiziert.

Routing Tag

Definieren Sie das Routing-Tag, welches für die Verbindung genutzt werden soll.

6.1.2 Ergänzungen im Setup-Menü

Tunnel-Passwort

Legen Sie mit diesem Eintrag das Verbindungs-Kennwort für den jeweiligen Benutzer fest.

SNMP-ID:

2.25.10.7.23

Pfad Telnet:

Setup > RADIUS > Server > Benutzer

Mögliche Werte:

max. 32 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-./:;<=>?[\]^_`~

Default-Wert:

leer

LCS-Routing-Tag

Geben Sie hier das Routing-Tag für diese Verbindung an.

SNMP-ID:

2.25.10.7.24

Pfad Telnet:

Setup > RADIUS > Server > Benutzer

Mögliche Werte:

max. 5 Zeichen aus [0-9]

Default-Wert:

0

6.2 WAN-Zugriff auf den RADIUS-Server einschränken

Ab Version 10.0 lässt sich im LCOS der Zugriff aus dem IPv4-Netz einschränken.

RADIUS-Dienst
 Authentifizierungs-Port:
 Accounting-Port:
 Accounting-Interim-Intervall: Sekunden
 Zugriff vom WAN:

RADSEC-Dienst
 RADSEC-Port:

RADIUS-/RADSEC-Clients
 Tragen Sie in diese Tabellen die Clients ein, die mit dem Server kommunizieren können.


Bitte beachten Sie, dass in der IPv6-Firewall eine passende Inbound-Filterregel eingetragen werden muss, damit der RADIUS-Server für IPv6-Clients erreichbar ist!

Benutzer-Datenbank
 Tragen Sie in die folgende Tabelle die Daten der Benutzer ein, die von diesem Server authentifiziert werden sollen.
 Benutzertabelle automatisch bereinigen

Erweiterte Einstellungen

WAN-Zugriff auf den RADIUS-Server


Geben Sie hier an, auf welche Weise der RADIUS-Server aus dem WAN erreichbar ist.

 Gilt ausschließlich für Zugriffe aus dem IPv4-Netz. Zugriffe aus dem IPv6-Netz steuert die eingebundene Firewall. Standardmäßig verbietet die IPv6-Firewall den WAN-Zugriff auf den RADIUS-Server.

6.2.1 Ergänzungen im Setup-Menü

IPv4-WAN-Zugriff

Geben Sie hier an, auf welche Weise der RADIUS-Server aus dem WAN erreichbar ist.

 Gilt ausschließlich für Zugriffe aus dem IPv4-Netz. Zugriffe aus dem IPv6-Netz steuert die eingebundene Firewall. Standardmäßig verbietet die IPv6-Firewall den WAN-Zugriff auf den RADIUS-Server.

SNMP-ID:

2.25.10.22

Pfad Telnet:

Setup > RADIUS > Server

Mögliche Werte:

Nein

Der RADIUS-Server lehnt WAN-Zugriffe aus dem IPv4-Netz ab.

Ja

Der RADIUS-Server nimmt WAN-Zugriffe aus dem IPv4-Netz an.

VPN

Der RADIUS-Server nimmt ausschließlich WAN-Zugriffe aus dem IPv4-Netz an, die über eine VPN-Verbindung mit dem Gerät erfolgen.

Default-Wert:

Nein

7 Voice over IP - VoIP

7.1 Clientseitige Unterstützung von SIPS/SRTP

Ab LCOS-Version 10.0 haben Sie im Voice Call Manager die Möglichkeit, zur verschlüsselten Übertragung der Authentifizierungsdaten von SIP-Benutzern sowohl SIPS (Session Initiation Protocol Security) als auch SRTP (Secure Real-Time Transport Protocol) zu konfigurieren.

7.1.1 Unterstützung von SIPS/SRTP mit LANconfig konfigurieren

Konfigurieren Sie SIPS und SRTP mit LANconfig unter **Voice Call Manager > Benutzer > SIP-Benutzer**. Fügen Sie der Tabelle einen neuen Benutzer hinzu oder bearbeiten Sie bestehende Einträge.

Der Dialog für SIP-Benutzer wurde wie folgt erweitert:

SIP-Benutzer - Neuer Eintrag

Eintrag aktiv

Interne Rufnummer:

Kommentar:

Anmelde-Daten

Authentifizier.-Name:

Passwort: Anzeigen

Zugriff vom WAN:

Gerätetyp:

Die übrigen Einstellungen (z.B. Domäne) nehmen Sie bitte im SIP-Endgerät/Client vor.

Anzeige der eigenen Rufnummer beim Angerufenen unterdrücken (CLIR)

DTMF-Signalisierung:

Msg. Waiting (MWI) über:

Sicherheit

Transportprotokolle:

Sprach-Verschlüsselung:

SRTP-Verschlüsselungsliste

AES-CM-256 AES-CM-192

AES-CM-128 F8-128

SRTP-Authentifizierung

HMCA-SHA1-80 HMCA-SHA1-32

Abbildung 1: Neuen Eintrag in der SIP-Benutzer-Tabelle hinzufügen

Transportprotokolle

Wählen Sie ein Protokoll, mit dem dieser Benutzer mit dem lokalen SIP-Server kommunizieren darf. SIP-Anforderungen von diesem Benutzer werden mit einer SIP-Fehlerantwort (SIP/406) abgelehnt, sofern das entsprechende Protokoll nicht ausgewählt ist. Hierdurch wird sichergestellt, dass sich kein Benutzer über ein hier nicht erlaubtes Protokoll registrieren kann.

UDP

Alle SIP-Pakete an diesen SIP-Benutzer werden über das verbindungslose UDP übertragen. Die meisten SIP-Benutzer unterstützen diese Einstellung.

TCP

Alle SIP-Pakete an diesen SIP-Benutzer werden über das verbindungsorientierte TCP übertragen. Die TCP-Verbindung bleibt für die Dauer der Registrierung bestehen.

TLS

Alle SIP-Pakete an diesen SIP-Benutzer werden verbindungsorientiert übertragen. Zusätzlich werden alle SIP-Pakete verschlüsselt.

Sprach-Verschlüsselung

Legen Sie mit diesem Eintrag fest, über welches Protokoll die Sprachdaten eines Anrufes (RTP/SRTP) an den lokalen SIP-Server übermittelt werden.

Ablehnen

Es erfolgt kein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Gespräche von diesem Benutzer mit Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist niemals verschlüsselt.

Ignorieren

Es erfolgt kein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Allerdings werden Gespräche von diesem Benutzer auch mit Verschlüsselungsvorschlag akzeptiert. Der Sprachkanal ist jedoch niemals verschlüsselt.

Bevorzugt

Es erfolgt ein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Es werden auch Gespräche ohne Verschlüsselungsvorschlag von diesem Benutzer akzeptiert. Der Sprachkanal ist nur dann verschlüsselt, wenn der Benutzer Verschlüsselung unterstützt.

Erzwingen

Es erfolgt ein Verschlüsselungsvorschlag bei Gesprächen für diesen Benutzer. Gespräche von diesem Benutzer ohne entsprechenden Verschlüsselungsvorschlag werden ignoriert. Der Sprachkanal ist entweder verschlüsselt oder wird nicht aufgebaut.



Wenn Sie Sprachdaten sicher verschlüsselt übertragen möchten, ist es erforderlich, auch die Signalisierung über einen verschlüsselten Kanal zu übertragen. Andernfalls ist es u.U. möglich, dass die Schlüssel für die Sprachdaten im Falle eines Angriffes aus der ungesicherten Signalisierung ausgelesen werden. Beachten Sie, dass Ihr Provider möglicherweise Ihre Sprachdaten entschlüsselt und neu verschlüsselt oder unverschlüsselt weitervermittelt. Die Nutzung von SRTP garantiert keine Ende-zu-Ende-Verschlüsselung!

SRTP-Verschlüsselungsliste

Geben Sie hier an, mit welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt werden soll. Wählen Sie dazu eine oder mehrere der folgenden Methoden aus:

AES-CM-256

Die Verschlüsselung erfolgt mittels AES256. Die Schlüssellänge beträgt 256 Bit.

AES-CM-128

Die Verschlüsselung erfolgt mittels AES128. Die Schlüssellänge beträgt 128 Bit.

AES-CM-192

Die Verschlüsselung erfolgt mittels AES192. Die Schlüssellänge beträgt 192 Bit.

F8-128

Die Verschlüsselung erfolgt mittels F8-128. Die Schlüssellänge beträgt 128 Bit.

SRTP-Authentifizierung

Mit dieser Einstellung schränken Sie die verhandelte Menge der (vorgeschlagenen oder akzeptierten) SRTP Suites mit dem entsprechenden Benutzer ein. Sollten Sie eine oder mehrere der folgenden Cipher zur Verschlüsselung von SRTP Paketen nicht ausgewählt haben, schlägt das Gerät die entsprechenden SRTP Suites niemals vor und werden niemals ausgewählt. So erzwingen Sie die bestmögliche Verschlüsselung.

HMAC-SHA1-80

Die Authentifizierung des SIP-Benutzers erfolgt mit dem Hash-Algorithmus HMAC-SHA1-80. Die Hash-Länge beträgt 80 Bit.

HMAC-SHA1-32

Die Authentifizierung des SIP-Benutzers erfolgt mit dem Hash-Algorithmus HMAC-SHA1-32. Die Hash-Länge beträgt 32 Bit.

7.1.2 Ergänzungen im Setup-Menü

Transport

Mit diesem Eintrag wählen Sie ein Protokoll, mit dem dieser Benutzer mit dem lokalen SIP-Server kommunizieren darf.

SNMP-ID:

2.33.3.1.1.22

Pfad Telnet:

Setup > Call-Manager > User > SIP-User

Mögliche Werte:**UDP**

Alle SIP-Pakete an diesen SIP-Benutzer werden über das verbindungslose UDP übertragen. Die meisten SIP-Benutzer unterstützen diese Einstellung.

TCP

Alle SIP Pakete an diesen SIP-Benutzer werden über das verbindungsorientierte TCP übertragen. Dazu wird eine TCP-Verbindung aufgebaut und für die Dauer der Registrierung aufrecht erhalten.

TLS

Wie TCP, allerdings werden alle SIP-Pakete zusätzlich durch eine Verschlüsselung geheim gehalten.

Default-Wert:

UDP

TCP

TLS

SRTP

Mit diesem Eintrag konfigurieren Sie das Secure Real-Time Transport Protocol (SRTP) zur Verschlüsselung und Übertragung der Authentifizierungsdaten von SIP-Benutzern.

SNMP-ID:

2.33.3.1.1.23

Pfad Telnet:

Setup > Call-Manager > User > SIP-User

Mögliche Werte:

Ablehnen

Verschlüsselung wird bei Gesprächen für diesen Benutzer nicht vorgeschlagen. Gespräche von diesem Benutzer mit Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist niemals verschlüsselt.

Ignorieren

Verschlüsselung wird bei Gesprächen für diesen Benutzer nicht vorgeschlagen. Gespräche von diesem Benutzer werden auch mit Verschlüsselungsvorschlag akzeptiert. Der Sprachkanal ist jedoch niemals verschlüsselt.

Bevorzugt

Verschlüsselung wird bei Gesprächen für diesen Benutzer angeboten. Gespräche von diesem Benutzer ohne Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nur dann verschlüsselt, wenn der Benutzer Verschlüsselung unterstützt.

Erzwingen

Verschlüsselung wird bei Gesprächen für diesen Benutzer angeboten. Gespräche von diesem Benutzer ohne Verschlüsselungsvorschlag kommen nicht zustande. Der Sprachkanal ist entweder verschlüsselt oder wird nicht aufgebaut.

Default-Wert:

Ignorieren

SRTP-Cipher

Wählen Sie hier das Verschlüsselungsverfahren für die Kommunikation mit dem Benutzer.

SNMP-ID:

2.33.3.1.1.24

Pfad Telnet:

Setup > Call-Manager > User > SIP-User

Mögliche Werte:**AES-CM-256**

Die Verschlüsselung erfolgt mit dem Verfahren AES256 und einer Schlüssellänge von 256 Bit.

AES-CM-192

Die Verschlüsselung erfolgt mit dem Verfahren AES192 und einer Schlüssellänge von 192 Bit.

AES-CM-128

Die Verschlüsselung erfolgt mit dem Verfahren AES128 und einer Schlüssellänge von 128 Bit.

F8-128

Die Verschlüsselung erfolgt mit dem Verfahren F8-128 und einer Schlüssellänge von 128 Bit.

Default-Wert:

AES-CM-256

AES-CM-192

AES-CM-128

F8-128

SRTP-Message-Auth-Tags

Wählen Sie hier das Authentifizierungsverfahren für diesen Benutzer aus.

SNMP-ID:

2.33.3.1.1.25

Pfad Telnet:

Setup > Call-Manager > User > SIP-User

Mögliche Werte:**HMAC-SHA1-80**

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA1-80 (Hash-Länge 80 Bit).

HMAC-SHA1-32

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA1-32 (Hash-Länge 32 Bit).

Default-Wert:

HMAC-SHA1-80

HMAC-SHA1-32

7.2 Einschränkung der Verarbeitung eingehender UDP-Pakete auf SIP-Leitungen

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, den Empfang eingehender UDP-Pakete zu steuern, sofern die Providerleitung UDP zur Kommunikation mit dem Registrar verwendet.

7.2.1 Einschränkung der Verarbeitung eingehender UDP-Pakete mit LANconfig konfigurieren

Die Konfiguration erfolgt über **VoIP-Call-Manager > Leitungen** mit einem Klick auf die Schaltfläche **SIP-Leitungen** oder **SIP-PBX-Leitungen**.

Die Benutzeroberfläche hat sich wie folgt geändert:

The screenshot shows a dialog box titled "SIP-Leitungen - Neuer Eintrag" with a help icon and a close icon in the top right corner. The dialog has two tabs: "Allgemein" and "Erweitert", with "Erweitert" selected. The "Erweitert" tab contains several sections of configuration options:

- Eintrag aktiv:** A checked checkbox.
- Modus:** A dropdown menu set to "Einzel-Account".
- Provider-Name:** An empty text input field.
- Kommentar:** An empty text input field.
- Provider-Daten:** A section containing:
 - SIP-Domäne/Realm:** A dropdown menu.
 - Registrar (optional):** An empty text input field.
 - Port:** A text input field containing "0".
 - Vermitteln beim Provider aktiv:** An unchecked checkbox.
- Sicherheit:** A section containing:
 - Signalisierungs-Verschlüsselung:** A dropdown menu set to "Keine (UDP)".
 - Sprach-Verschlüsselung:** A dropdown menu set to "Ignorieren".
 - Server-Zert. prüfen bezüglich:** A dropdown menu set to "Nicht prüfen".
 - Erlaube eingehende UDP-Pakete:** A dropdown menu set to "über LAN, VPN und WAN".
 - SIP-Nachrichten nur vom Registrar erlauben:** A checked checkbox.
- Anmelde-Daten:** A section containing:
 - (Re-)Registrierung:** A checked checkbox.
 - SIP-ID/Benutzer:** An empty text input field.
 - Display-Name (opt.):** An empty text input field.
 - Authentifizier.-Name:** An empty text input field.
 - Passwort:** A text input field with a red background, followed by an unchecked "Anzeigen" checkbox and a "Passwort erzeugen" dropdown menu.
- Anruf-Präfix:** An empty text input field.
- Interne Ziel-Nummer:** An empty text input field.

At the bottom right of the dialog are two buttons: "OK" and "Abbrechen".

Erlaube eingehende UDP-Pakete

Wenn die Providerleitung UDP zur Kommunikation mit dem Registrar verwendet, empfangt Sie UDP-Pakete auf dem gewünschten lokalen Port. Mit dieser Einstellung definieren Sie, in welchem Netzwerk-Kontext ein UDP-Paket akzeptiert wird. Ein Paket aus dem WAN / VPN / LAN akzeptiert das Gerät nur, wenn Sie die entsprechende Einstellung aktiviert haben. Andernfalls wird das Paket verworfen.

SIP-Nachrichten nur vom Registrar erlauben

Aktivieren Sie diese Checkbox, wenn Sie nur SIP-Nachrichten durch den Registrar zulassen wollen.

7.2.2 Ergänzungen im Setup-Menü

Erlaube-UDP-Eingehend-Von

Mit dieser Einstellung definieren Sie, in welchem Netzwerk-Kontext das Gerät ein UDP-Paket akzeptiert.

SNMP-ID:

2.33.4.1.1.33

Pfad Telnet:

Setup > Call-Manager > Line > SIP-Provider > Line

Mögliche Werte:

LAN
VPN
WAN

Default-Wert:

LAN

VPN

WAN

Erlaube-UDP-Eingehend-Von

Mit dieser Einstellung definieren Sie, in welchem Netzwerk-Kontext ein UDP-Paket akzeptiert wird.

SNMP-ID:

2.33.4.2.1.22

Pfad Telnet:

Setup > Call-Manager > Line > SIP-PBX > PBX

Mögliche Werte:

LAN
VPN
WAN

Default-Wert:

LAN

VPN

7.3 Terminieren eines SIP-Trunks im LAN

Ab LCOS-Version 10.0 haben Sie die Möglichkeit, eine SIP-TK-Anlage über eine Trunk-Leitung mit Ihrem Gerät zu verbinden, sofern sich die Anlage im gleichen Netz befindet.

SIP-Benutzer

Benutzer, die über SIP an das LAN angeschlossen sind. Für die Konfiguration des Benutzers ist dabei unerheblich, ob das LAN lokal oder via VPN (über das Internet) erreichbar ist. Neben SIP-Telefonen haben Sie auch die Möglichkeit, eine SIP-TK-Anlage als Benutzer einzurichten (interne SIP-Trunk-Verbindung).

Abbildung 2: Neuen Eintrag in der SIP-Benutzer-Tabelle hinzufügen

Interne Rufnummer

- > Telefonnummer des SIP-Telefons
- > Name des Benutzers (SIP-URI)
- > Stammnummer der SIP-TK-Anlage, gefolgt von einem #. Ihre SIP-TK-Anlage muss sich dazu im selben Netz wie ihr Gerät befinden, wahlweise lokal oder via VPN (interne SIP-Trunk-Verbindung).

8 LANCOM Management Cloud (LMC)

Ab LCOS-Version 10.0 ist es möglich, LANCOM Geräte in die "LANCOM Management Cloud" zu integrieren.

Die LANCOM Management Cloud ist das weltweit erste hyper-integrierte Management-System, das Ihre gesamte Netzwerkarchitektur intelligent organisiert, optimiert und steuert. Die hochmoderne "Software-defined Networking-Technologie" vereinfacht die Bereitstellung eines integrierten Netzwerks drastisch, sodass die manuelle Einzelgerätekonfiguration entfällt.

Sie haben die Möglichkeit, eine Verbindung über die öffentliche LANCOM Management Cloud (Public) oder über eine privat gehostete LANCOM Management Cloud (Private) herzustellen.

8.1 Grundlagen der LANCOM Management Cloud

Die LANCOM Management Cloud (LMC) verwaltet beliebig große Netzwerke "software-defined". Die LMC übernimmt die Konfiguration sämtlicher Netzwerkkomponenten und minimiert so den Kontrollaufwand und aufwändige Konfigurationen.

Weitere Informationen zur LANCOM Management Cloud finden Sie unter <https://www.lancom-systems.de/cloud>.



Wenn Sie die LANCOM Management Cloud für die Konfiguration und zur Überwachung Ihres Gerätes verwenden möchten, ist es erforderlich, das Gerät mit der LMC zu koppeln.

8.2 Koppeln von Geräten mit der LANCOM Management Cloud

In diesem Kapitel werden unterschiedliche Vorgehensweisen für das Koppeln von LANCOM Geräten mit der LMC beschrieben. Hierzu wird zwischen Cloud-ready-Geräten und Bestandsgeräten unterschieden.

Cloud-ready-Geräte sind LANCOM Geräte mit einer bereits vom Hersteller ausgelieferten LCOS-Version 10.0 oder höher (LANCOM Switches: Switch OS 3.30) und besitzen eine PIN zur Kopplung mit der LMC.

Bestandsgeräte sind LANCOM Geräte, die von einer älteren LCOS-Version auf eine Version 10.0 (LANCOM Switches: Switch OS 3.30) oder höher aktualisiert wurden und mit dieser für die Verwaltung durch die LMC vorbereitet sind.

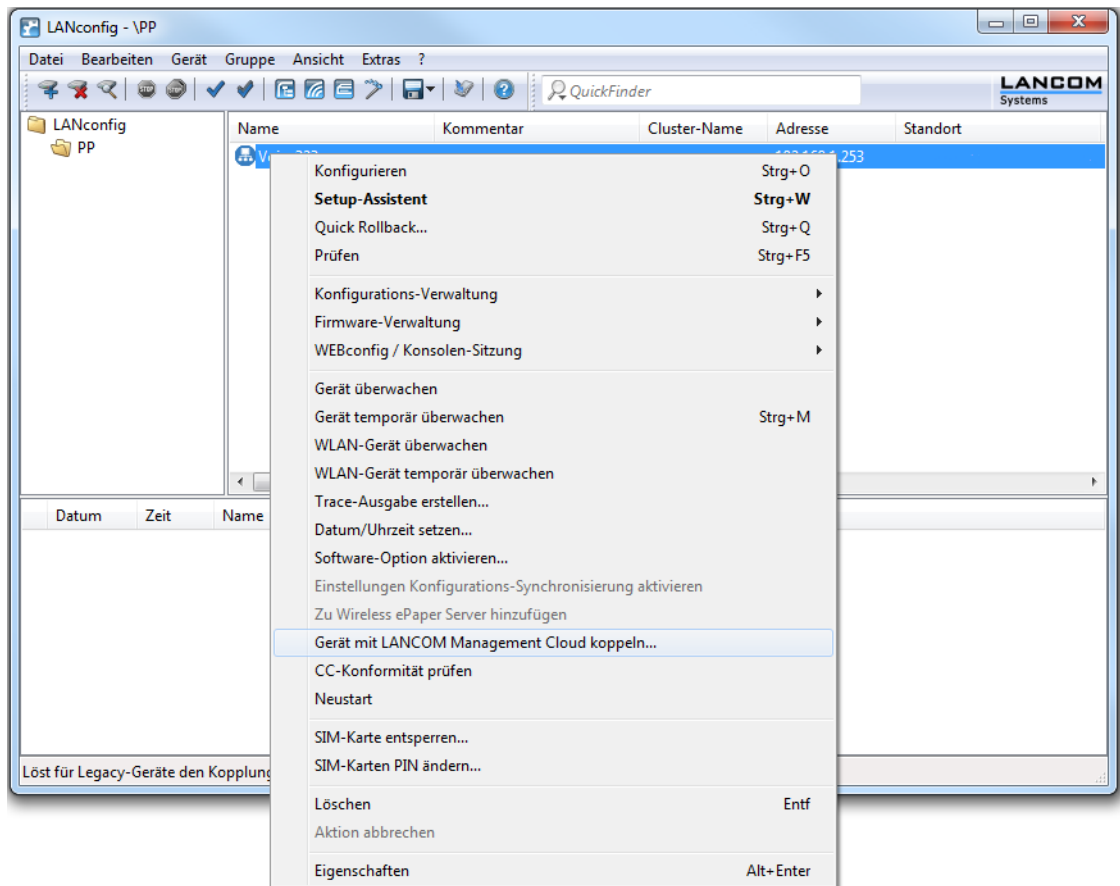
Besitzen Sie ein Cloud-Ready-Gerät, ist kein Pairing erforderlich. Fügen Sie in diesem Fall Ihr Gerät unter Angabe von Seriennummer und PIN Ihrem Konto in der LANCOM Management Cloud hinzu. Alternativ können Sie auch für Cloud-Ready-Geräte ein Pairing durchführen.

Möchten Sie ein Bestandsgerät mit der LANCOM Management Cloud verbinden, ist ein separates Pairing erforderlich, welches nachfolgend beschrieben ist.

8.2.1 Koppeln von Bestandsgeräten via LANconfig

1. Generieren Sie im ersten Schritt einen Aktivierungscode in der LANCOM Management Cloud.
2. Klicken Sie mit rechten Maustaste auf Ihr LANCOM Gerät.

3. Wählen Sie im Kontextmenü den Eintrag **Gerät mit LANCOM Management Cloud koppeln...** aus.



4. Folgen Sie den Anweisungen zur Eingabe des Aktivierungscodes. Hier stehen drei Optionen zur Auswahl:
- Public Cloud (Default): Sie verwenden die LANCOM-eigene Cloud.
 - Private Cloud: Sie verwenden Ihre eigene Cloud.
 - Aktuell im Gerät gespeicherte Einstellungen verwenden: Je nach bereits vorhandener Konfiguration des Gerätes wird eine Public bzw. Private Cloud verwendet.



8.2.2 Koppeln von Bestandsgeräten via Kommandozeile

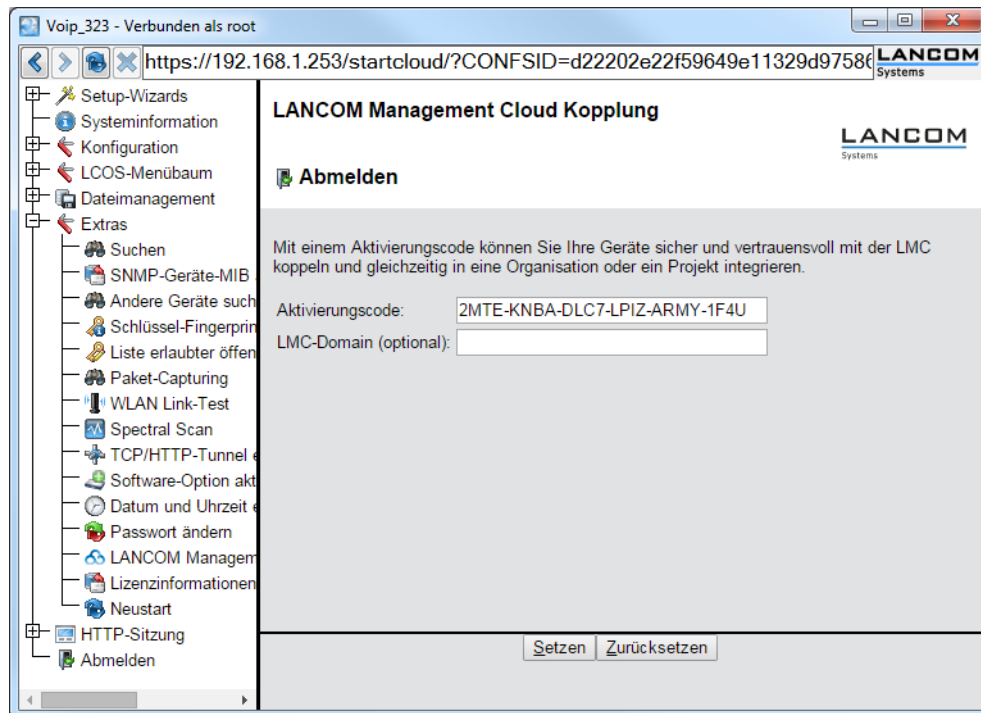
Das Pairing über die Kommandozeile erfolgt mit der Eingabe des Befehls `startlmc`.

1. Starten Sie ein Kommandozeilenprogramm.
2. Geben Sie den Pairing-Befehl mit dem Aktivierungscode als Parameter ein, z.B. `startlmc 2MTE-KNBA-DLC7-LPIZ-ARMY-1F4U`.

Sie erhalten eine Rückmeldung auf dem Bildschirm, ob der Pairing-Prozess erfolgreich gestartet wurde oder eine entsprechende Fehlermeldung.

8.2.3 Koppeln von Bestandsgeräten via WEBconfig

1. Starten Sie WEBconfig.
2. Geben Sie unter **Extras** > **LANCOM Management Cloud Kopplung** Ihren Aktivierungscode ein.



3. Klicken Sie die Schaltfläche **Setzen**.

8.3 Auslieferung der LMC-Domain durch den LCOS-DHCP-Server

Ab LCOS-Version 10.0 erhalten LCOS-Geräte bei der automatischen Zuweisung ihrer IP-Adresse durch den DHCP-Server zusätzlich eine in den DHCP-Paketen angegebene DHCP-Option 43.

Der DHCP-Server verteilt in seinen DHCP-Paketen auch die DHCP-Option 43 (Vendor Specific Option) an anfragende Clients im Netz. Hierin enthalten ist der Domain-Name, welcher für den Betrieb des Gerätes durch die LANCOM Management Cloud (LMC) erforderlich ist. Auf diese Weise kann ein Gerät direkt mit einer privaten LMC-Installation kommunizieren, ohne vorab konfiguriert zu sein.

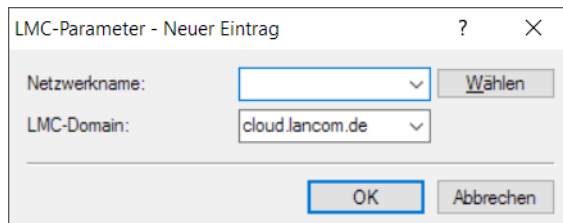
Wenn Sie ein LCOS-Gerät als DHCP-Server verwenden, hinterlegen Sie die LMC-Domain im Klartext in der Konfiguration. Der LCOS-interne DHCP-Server fügt die Domain der DHCP-Option 43 hinzu und liefert sie im Antwortpaket an anfragende LCOS-Geräte aus. Dazu wertet der DHCP-Server die DHCP-Option 60 (Vendor Class Identifier) in den DHCP-Requests der Clients aus. Eine so konfigurierte DHCP-Option 43 hat Vorrang vor einer in der DHCP-Options-Tabelle des DHCP-Servers manuell konfigurierten DHCP-Option 43.

! Der Vendor Class Identifier muss im Request LANCOM beinhalten. Stellt das Gerät eines anderen Herstellers einen Request an den LCOS-internen DHCP-Server, wird ihm die DHCP-Option 43 im Antwortpaket nicht angeboten.

8.3.1 Konfiguration der DHCP-Option 43 zur Auslieferung der LMC-Domain mit LANconfig

Konfiguration

Die LMC-Domain konfigurieren Sie für die einzelnen Netze in LANconfig unter **IPv4 > DHCPv4 > LMC-Parameter**.



Netzwerkname

Geben Sie hier das Netz an, in welches das Gerät die LMC-Domain über die DHCP-Option 43 ausliefert.

LMC-Domain

Geben Sie hier den Domain-Namen der LANCOM Management Cloud an.

Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen ("private Cloud" oder "on premise installation"), tragen Sie bitte die entsprechende LMC-Domain ein.

8.3.2 Ergänzungen im Setup-Menü

LMC-Optionen

In dieser Tabelle konfigurieren Sie die Cloud-Parameter für LMC (LANCOM Management Cloud).

SNMP-ID:

2.10.25

Pfad Telnet:

Setup > DHCP

Netzwerkname

Geben Sie hier das Netz an, in welches das Gerät die LMC-Domain über die DHCP-Option 43 ausliefert.

SNMP-ID:

2.10.25.1

Pfad Telnet:

Setup > DHCP > LMC-Optionen

Mögliche Werte:

max. 16 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-./:;<=>[\]^_`~

Default-Wert:

leer

LMC-Domain

Geben Sie hier den Domain-Namen der LANCOM Management Cloud an.

Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen ("private Cloud" oder "on premise installation"), tragen Sie bitte die entsprechende LMC-Domain ein.

SNMP-ID:

2.10.25.6

Pfad Telnet:

Setup > DHCP > LMC-Optionen

Mögliche Werte:

max. 64 Zeichen aus [A-Z][a-z][0-9]/?.-;:@&=\$_+!*'(),%

Default-Wert:

leer

8.4 Manuelles Vorabkonfigurieren Ihres Gerätes für die Verwaltung durch die LANCOM Management Cloud

Sie legen fest:

- > ob Ihr Gerät durch die LMC zu verwalten ist.
- > ob die LMC-Domain von einem DHCP-Server zu beziehen ist.
- > mit welcher Domain sich Ihr Gerät verbindet.
- > die Absende-Adresse (optional).

1. Navigieren Sie zu **Management > LMC**.

LANCOM Management Cloud

Wenn Sie die LANCOM Management Cloud zur Konfiguration und zum Monitoring des Gerätes nutzen möchten, dann müssen Sie hier die Domain der Services angeben.

Das Gerät mit LMC verwalten:

Konfiguration über DHCP

Geben Sie hier die Domain der Services an, mit denen sich das Gerät verbinden soll.

LMC-Domain:

Absende-Adresse (opt.):

2. Wählen Sie unter **Das Gerät mit LMC verwalten**: zwischen drei Optionen:

- > **Nein**: Das Gerät stellt keine Verbindung zur LMC her.
- > **Ja**: Das Gerät wird von der LMC verwaltet. (Default für Geräte ohne WLAN-Schnittstelle)

- > **Nur ohne WLC:** Geräte innerhalb eines von einem WLC verwalteten Netzes bauen keine Verbindung zur LANCOM Management Cloud auf. (Default für Geräte mit WLAN-Schnittstelle)
- 3. Um die LMC-Domain von einem DHCP-Server zu beziehen, setzen Sie ein Häkchen in **Konfiguration über DHCP**.
 - ! Um die LMC-Domain von einem DHCP-Server bereitzustellen, konfigurieren Sie am DHCP-Server innerhalb der DHCP-Option 43 die Sub-Option 18 mit der LMC-Domain. Weitere Informationen zur Konfiguration der LMC Parameter finden Sie im Abschnitt [Auslieferung der LMC-Domain durch den LCOS-DHCP-Server](#) auf Seite 59.
- 4. Wählen Sie unter **LMC-Domain** die Domain der LANCOM Management Cloud, mit der sich das Gerät verbinden soll.
- 5. Geben Sie optional unter **Absende-Adresse** eine Absendeadresse an, die statt der sonst automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. eine Loopback-Adresse konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

8.5 Ergänzungen im Status-Menü

8.5.1 LMC

Dieses Menü enthält alle Informationen über die LANCOM Management Cloud (LMC).

SNMP-ID:

1.98

Pfad Telnet:

Status

Transport-Status

Diese Tabelle enthält die Informationen zum Transportstatus der LMC-Dienste.

SNMP-ID:

1.98.1

Pfad Telnet:

Status > LMC

Loesche-Transport-Status

Mit dieser Aktion leeren Sie die Tabelle [1.98.1 Transport-Status](#).

SNMP-ID:

1.98.2

Pfad Telnet:

Status > LMC

Mögliche Argumente:

keine

Log-Tabelle

Diese Tabelle enthält Ereignisinformationen zu den einzelnen Diensten. Die Log-Einträge enthalten neben einer laufenden Nummer den genauen Zeitpunkt eines Ereignisses und den betreffenden Service.

SNMP-ID:

1.98.3

Pfad Telnet:

Status > LMC

Loesche-Log-Tabelle

Mit dieser Aktion leeren Sie die Tabelle [1.98.3 Log-Tabelle](#).

SNMP-ID:

1.98.4

Pfad Telnet:

Status > LMC

Mögliche Argumente:

keine

Kunden-Geraete-ID

Dieser Eintrag zeigt die ID des Gerätes, welches sich mit der LMC verbunden hat.

SNMP-ID:

1.98.5

Pfad Telnet:

Status > LMC

Antwortzeit

Dieser Eintrag zeigt die Antwortzeit des Gerätes, welches sich mit der LMC verbunden hat, in Millisekunden.

SNMP-ID:

1.98.6

Pfad Telnet:

Status > LMC

Pairing-Status

Dieser Eintrag zeigt den Pairing-Status zwischen Ihrem Gerät und der LANCOM Management Cloud.

SNMP-ID:

1.98.7

Pfad Telnet:

Status > LMC

Zertifikat-Anzeigen

Mit dieser Aktion lassen Sie sich das LMC-Zertifikat anzeigen.

SNMP-ID:

1.98.8

Pfad Telnet:

Status > LMC

Mögliche Argumente:

keine

Control-Status

Der Eintrag zeigt an, ob die Verbindung zum Control-Service der LMC betriebsbereit ist. Der Control-Service ist u. a. für Änderungen an der Gerätekonfiguration über die LMC zuständig.

SNMP-ID:

1.98.9

Pfad Telnet:

Status > LMC

Monitor-Status

Der Eintrag zeigt an, ob die Verbindung zum Monitoring-Service der LMC betriebsbereit ist. Der Monitoring-Service ist u. a. für das periodische Auslesen von Monitoring-Daten zuständig.

SNMP-ID:

1.98.10

Pfad Telnet:**Status > LMC****Config-Log**

Diese Tabelle enthält Informationen über die via LMC durchgeführten Änderungen der Gerätekonfiguration.

SNMP-ID:

1.98.11

Pfad Telnet:**Status > LMC****Zero-Touch-Unterstützung**

Dieser Eintrag zeigt an, ob das Gerät, welches sich mit der LMC verbunden hat, "Cloud-Ready" ist. Cloud-Ready-Geräte besitzen einen werkseitig vorkonfigurierten PSK (Pre-Shared-Key) und können mittels ihrer Seriennummer und PIN in der LMC registriert werden.

SNMP-ID:

1.98.12

Pfad Telnet:**Status > LMC****Pairing-Token-Vorhanden**

Dieser Eintrag zeigt an, ob Ihr Gerät den Aktivierungscode (Pairing Token) zur Kopplung mit der LMC temporär zwischengespeichert hat. Das temporäre Speichern erfolgt, um z. B. im Falle eines Absturzes oder Stromausfalls den Pairing-Vorgang nach dem Geräteeustart automatisch wieder aufzunehmen. Nachdem der Pairing-Vorgang abgeschlossen ist, entfernt das Gerät das Pairing-Token aus dem Speicher.

SNMP-ID:

1.98.13

Pfad Telnet:**Status > LMC****Mögliche Werte:**

ja

Pairing-Token vom Administrator akzeptiert und zwischengespeichert. Der Pairing-Vorgang dauert an.

nein

Kein Pairing-Token zwischengespeichert. Der Pairing-Vorgang wurde bereits beendet oder hat noch nicht stattgefunden.

8.6 Ergänzungen im Setup-Menü

8.6.1 LMC

In diesem Menü konfigurieren Sie die Cloud-Parameter für LMC (LANCOM Management Cloud).

SNMP-ID:

2.102

Pfad Telnet:

Setup

Aktiv

Mit diesem Eintrag aktivieren oder deaktivieren Sie die Möglichkeit der Verwaltung Ihres LANCOM Gerätes durch die LMC.

SNMP-ID:

2.102.1

Pfad Telnet:

Setup > LMC

Mögliche Werte:

nein

Das Gerät stellt keine Verbindung zur LMC her.

ja

Das Gerät wird mit LMC verwaltet. Sofern noch nicht erfolgt, ist eine erstmalige Verbindung des Gerätes mit der LANCOM Management Cloud erforderlich (Pairing). Dies ist die Standardeinstellung für Geräte ohne WLAN-Schnittstelle.



Bitte beachten Sie, dass das Gerät ohne entsprechendes Pairing nicht mit der Management Cloud kommunizieren kann.

Nur-Ohne-WLC

Geräte innerhalb eines von einem WLC verwalteten Netzes bauen keine Verbindung zur LMC auf. Dies ist die Standardeinstellung für Geräte mit WLAN-Schnittstelle.

Delete-Certificate

Mit dieser Aktion löschen Sie das LMC-Zertifikat.

SNMP-ID:

2.102.7

Pfad Telnet:

Setup > LMC

Mögliche Argumente:

keine

DHCP-Client-Auto-Erneuerung

Mit diesem Parameter legen Sie das Verhalten des Gerätes fest, wenn sich die DHCP-Einstellungen des Netzes ändern und der LMC-Client keine Verbindung zur LMC aufbauen kann.

Kann der LMC-Client die konfigurierte LMC nicht erreichen, hat sich wahrscheinlich der IP-Adressbereich des Netzes geändert. Geräte, die als DHCP-Client konfiguriert sind, behalten jedoch die zuvor zugewiesene IP-Adresse, bis deren DHCP-Lease-Time abgelaufen ist. Durch Aktivieren dieses Parameters fordert das Gerät unabhängig von der verbleibenden DHCP-Lease-Time die DHCP-Adresse erneut an (DHCP-Renew).

SNMP-ID:

2.102.8

Pfad Telnet:

Setup > LMC

Mögliche Werte:

nein

Wenn der LMC-Client die Verbindung zur LMC verliert, löst dies keinen DHCP-Renew aus.

ja

Wenn der LMC-Client die Verbindung zur LMC verliert, löst dies einen DHCP-Renew aus. Ist das DHCP-Renew nicht erfolgreich, wird der DHCP-Prozess komplett neu angestoßen. Das Gerät versucht dann, eine IP-Adresse von einem beliebigen DHCP-Server zu erhalten, um die Verbindung zur LMC wiederherzustellen.

Default-Wert:

ja

Loopback-Adresse

Legen Sie mit diesem Eintrag eine Loopback Adresse für die LANCOM Management Cloud fest.

SNMP-ID:

2.102.12

Pfad Telnet:

Setup > LMC

Mögliche Werte:

max. 16 Zeichen aus [0-9] .

Default-Wert:

leer

Konfiguration-Via-DHCP

Mit diesem Eintrag aktivieren oder deaktivieren Sie den Erhalt aller Informationen via DHCP-Option 43, die für eine Verbindung mit der LMC erforderlich sind.

SNMP-ID:

2.102.13

Pfad Telnet:

Setup > LMC

Mögliche Werte:

nein
ja

Default-Wert:

ja

DHCP-Status

Dieses Menü enthält die Status-Werte, die das Gerät zur LMC-Domain über die DHCP-Option 43 bezogenen hat.

SNMP-ID:

2.102.14

Pfad Telnet:

Setup > LMC

DHCP-LMC-Domain

Dieser Eintrag zeigt die LMC-Domain, welche das Gerät über die DHCP-Option 43 bezogen hat.

SNMP-ID:

2.102.14.5

Pfad Telnet:**Setup > LMC****Mögliche Werte:**

max. 255 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:

cloud.lancom.de

LMC-Domain

Geben Sie hier den Domain-Namen der LANCOM Management Cloud an.

Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen ("private Cloud" oder "on premise installation"), tragen Sie bitte die entsprechende LMC-Domain ein.

SNMP-ID:

2.102.15

Pfad Telnet:**Setup > LMC****Mögliche Werte:**

max. 255 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:


cloud.lancom.de

9 Diagnose

9.1 Layer-7-Anwendungserkennung


Ab LCOS-Version 10.0 haben Sie mit der Layer-7-Anwendungserkennung die Möglichkeit, bandbreitenintensive Dienste in Ihrem Netzwerk zu identifizieren.

Baut ein Client eine Verbindung über eine überwachte Schnittstelle auf, beginnt die Anwendungserkennung mit der Analyse und Aufzeichnung des Traffic-Volumens.

 Die Aufzeichnung und die daraus resultierende Nutzungsstatistik ist abhängig von der für diese Verbindung definierte Konfiguration.

Die Layer-7-Anwendungserkennung beobachtet den Ziel-Port einer Anwendung. Wird eine Verbindung über Port 80 oder 443 (HTTP oder HTTPS) erkannt, erfolgt eine weitere Analyse des Verbindungsaufbaus. Weicht der Ziel-Port davon ab, erfolgt die Zuordnung der Verbindung Port-abhängig über die in der Liste "Port-basiertes Tracking" festgelegten Anwendungen.

Bei einem erkannten HTTP/HTTPS-Aufbau wird diese Verbindung tiefer analysiert. Dazu extrahiert die Anwendungserkennung bei HTTP-Verbindungen den Ziel-Host aus der Ziel-URL des HTTP GET Requests.

 Es wird nur der Host-Anteil verwendet, weitere URL-Bestandteile werden abgeschnitten

Wird eine HTTPS-Verbindung erkannt, versucht die Layer-7-Anwendungserkennung den Ziel-Host durch Informationen in folgender Reihenfolge zu identifizieren:

- > Server Name Indication aus dem TLS Client Hello
- > Common Name aus dem übermittelten TLS-Server-Zertifikat
- > Reverse DNS Request auf die Server-IP-Adresse

Sowohl bei Verbindungen über HTTP als auch über HTTPS wird der ermittelte Ziel-Hostname mit der Liste "HTTP/HTTPS-Tracking" abgeglichen. Diese Liste enthält die am weitesten verbreiteten Web-Dienste/Anwendungen inklusive der Bestandteile ihrer Hostnamen.

Sollte der aufgerufene Dienst oder die gewählte Verbindung nicht in der Liste enthalten und deshalb eine Zuordnung nicht möglich sein, erfolgt eine Port-basierte Zuordnung zu dem generellen Dienst HTTP oder HTTPS.

 Für diese Zuordnung ist es erforderlich, dass die HTTP- und HTTPS-Einträge in der Liste für "Port-basiertes Tracking" enthalten sind.

Ist der Ziel-Dienst für jede über eine überwachte Schnittstelle geführte Verbindung bekannt, ist es gemeinsam mit dem verbindungsherstellenden Client möglich, die Verbindung zu tracken und so zu ermitteln, welcher Client wie viel Traffic von / zu einem Dienst verursacht hat.

Die ermittelten Werte finden Sie in den zugehörigen Tabellen im LCOS-Menübaum unter **Status > Layer-7-App-Erkennung**.

Sie haben die Möglichkeit, die Layer-7-Anwendungserkennung zentral oder dezentral in Ihrem Netzwerk einzusetzen. Beide Varianten verhindern, dass Traffic mehrfach gelistet wird:

Zentraler Einsatz

Die Layer-7-Anwendungserkennung wird auf einem zentralen Router im LAN aktiviert, auf allen anderen LANCOM Geräten ist sie deaktiviert.

Dezentraler Einsatz

Die Layer-7-Anwendungserkennung wird nur auf den letzten Bridges im LAN aktiviert, z. B. Access Points oder LANCOM-Router, an deren LAN-Schnittstellen die Clients direkt angeschlossen sind.

Um verfälschte Ergebnisse zu verhindern, achten Sie bitte darauf, dass der Traffic nur genau ein Gerät oder eine Bridge mit aktiver Layer-7-Anwendungserkennung durchläuft.

9.1.1 Layer-7-Anwendungserkennung mit LANconfig konfigurieren

Aktivieren und konfigurieren Sie die Layer-7-Anwendungserkennung mit LANconfig unter **Firewall/QoS > Allgemein > Layer-7-Anwendungserkennung**.

The screenshot shows a configuration window titled "Layer 7-Anwendungserkennung". It contains the following elements:

- A checkbox labeled "Layer 7-Anwendungserkennung aktiviert" which is currently unchecked.
- A text prompt: "Definieren Sie hier die zu überwachenden Schnittstellen." followed by a button labeled "Port-Tabelle...".
- A text prompt: "Entscheiden Sie hier, ob nur bestimmte VLANs überwacht werden sollen." followed by a button labeled "VLAN-Tabelle...".
- A text prompt: "Definieren Sie hier die Ziel-Anwendungen." followed by two buttons: "Port-basiertes Tracking..." and "HTTP/HTTPS-Tracking...".
- A text prompt: "Definieren Sie hier, in welchem Intervall die Nutzungsstatistiken aktualisiert werden." followed by a text input field containing the number "5" and the label "Minuten".
- At the bottom, there are two buttons: "OK" and "Abbrechen".

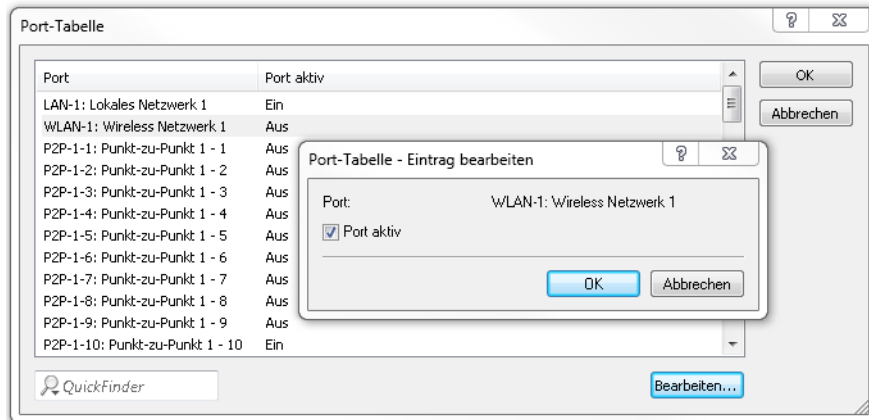
In diesem Abschnitt bestimmen Sie folgende Parameter:

Layer-7-Anwendungserkennung aktiviert

Aktivieren oder deaktivieren Sie die Layer-7-Anwendungserkennung.

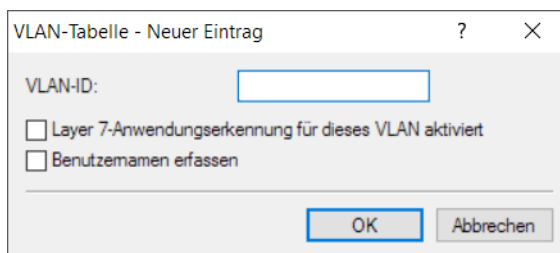
Port-Tabelle

Legen Sie hier fest, welche Verbindungen mit der Layer-7-Anwendungserkennung überwacht werden sollen. Aktivieren oder deaktivieren Sie dazu die zur Verfügung stehenden Ports.



VLAN-Tabelle

Geben Sie hier die zu überwachenden VLAN-IDs an und legen Sie fest, in welchem Umfang die Layer-7-Anwendungserkennung Traffic-Informationen erfasst.

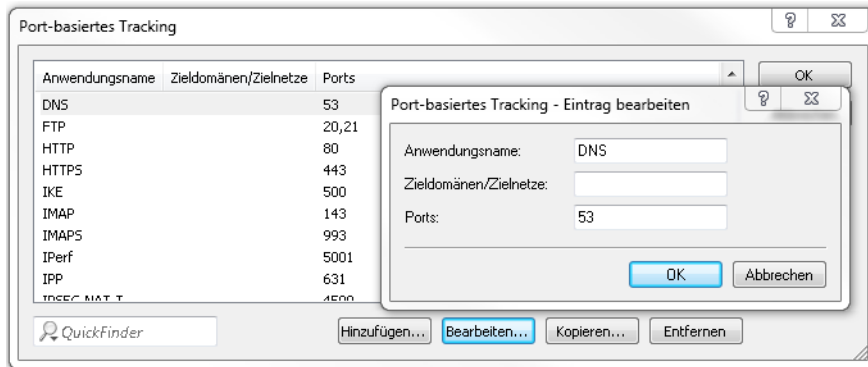


- > **Layer 7-Anwendungserkennung für dieses VLAN aktiviert:** Das Gerät erfasst allgemeine bzw. applikationsspezifische Daten.
- > **Benutzernamen erfassen:** Das Gerät erfasst in dem angegebenen VLAN benutzerspezifische Daten (Benutzer- oder Client-Name sowie MAC-Adresse).

! Damit die Layer-7-Anwendungserkennung im VLAN aktiv ist, muss das Gerät zumindest applikationsspezifischen Daten erfassen.

Port-basiertes Tracking

Wählen Sie hier die Anwendungen aus, die überwacht werden sollen. Sie haben dabei die Möglichkeit, aus Default-Anwendungen zu wählen oder eigene Anwendungen zu definieren. Geben Sie zusätzlich die Zieldomänen oder die Zielnetze der Anwendung an. Erweitern Sie die Liste nach Ihren Bedürfnissen.

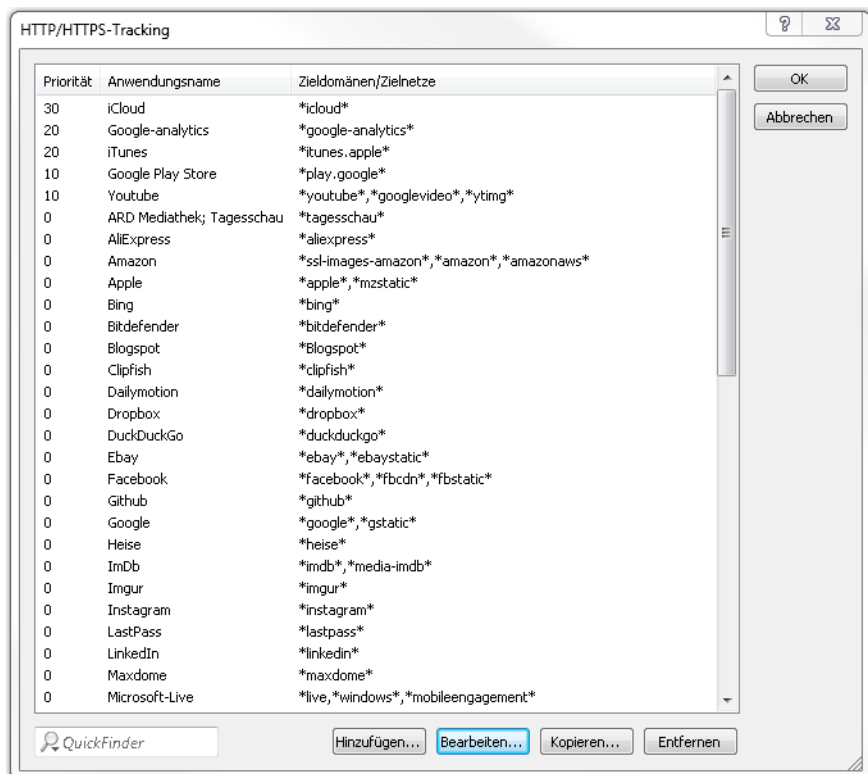



- ! Geben Sie mehrere Zieldomänen, Zielnetze oder Ports mittels einer kommaseparierteren Liste in CIDR-Notation (Classless Inter-Domain Routing) an. Dabei haben Sie die Möglichkeit, IPv4- oder IPv6-Zielnetze verwenden.

HTTP/HTTPS-Tracking

Legen Sie mit dieser Tabelle zu überwachende HTTP/HTTPS-Dienste fest. Geben Sie zusätzlich die Hostnamen-Bestandteile der Anwendung an.

- ! Verwenden Sie Wildcards ("*" für beliebig viele Zeichen oder "?" für genau ein Zeichen), um die Hostnamen-Bestandteile zu definieren.



 Geben Sie mehrere Hostnamen-Bestandteile mittels einer kommaseparierten Liste an.

Zusätzlich haben Sie mit der Angabe der Priorität die Möglichkeit festzulegen, in welcher Reihenfolge die jeweiligen Dienste ausgewertet werden, wenn bestimmte Hostnamen-Bestandteile in mehreren Einträgen definiert sind (z. B. *google).

Aktualisierungs-Intervall

Geben Sie einen Wert in Minuten an, nach dessen Ablauf die Nutzungsstatistik aktualisiert wird.

9.1.2 Ergänzungen im Setup-Menü

Layer-7-App-Erkennung

In diesem Menü haben Sie die Möglichkeit, die Layer-7-Anwendungserkennung zu konfigurieren.

SNMP-ID:

2.101

Pfad Telnet:

Setup

Aktiv

Mit diesem Eintrag aktivieren oder deaktivieren Sie die Layer-7-Anwendungserkennung.

SNMP-ID:

2.101.1

Pfad Telnet:

Setup > Layer-7-App-Erkennung

Mögliche Werte:

nein
ja

Default-Wert:

nein

IP-Port-Anwendungen

Bearbeiten Sie die Ziel-Ports für die Layer-7-Anwendungserkennung oder fügen Sie der Tabelle neue Einträge hinzu.

SNMP-ID:

2.101.2

Pfad Telnet:**Setup > Layer-7-App-Erkennung****Anwendungsname**

Geben Sie einen Namen für diese Anwendung an.

SNMP-ID:

2.101.2.1

Pfad Telnet:**Setup > Layer-7-App-Erkennung > IP-Port-Anwendungen****Mögliche Werte:**

max. 64 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Ziele**

Definieren Sie Ziele für diese Anwendung.



Geben Sie mehrere Ziele durch eine kommaseparierte Liste an.

SNMP-ID:

2.101.2.2

Pfad Telnet:**Setup > Layer-7-App-Erkennung > IP-Port-Anwendungen****Mögliche Werte:**

max. 254 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Ports**

Definieren Sie die zu überwachenden Schnittstellen.

SNMP-ID:

2.101.2.3

Pfad Telnet:**Setup > Layer-7-App-Erkennung > IP-Port-Anwendungen**

Mögliche Werte:

max. 32 Zeichen aus [A-Z][a-z][0-9]#@{|}~!\$%&'()*+,-./:;<=>?[\]^_`~

Default-Wert:

leer

Port-Tabelle

Aktivieren oder deaktivieren Sie hier die Schnittstellen, die mit der Layer-7-Anwendungserkennung überwacht werden sollen.



Der Inhalt der Tabelle ist abhängig vom eingesetzten Gerät.

SNMP-ID:

2.101.4

Pfad Telnet:

Setup > Layer-7-App-Erkennung

Port

Dieser Eintrag enthält den Namen der aus der Tabelle gewählten Schnittstelle.

SNMP-ID:

2.101.4.2

Pfad Telnet:

Setup > Layer-7-App-Erkennung > Port-Tabelle

Traffic-erfassen

Mit diesem Eintrag aktivieren oder deaktivieren Sie die Erfassung des Traffics für diese Schnittstelle.

SNMP-ID:

2.101.4.3

Pfad Telnet:

Setup > Layer-7-App-Erkennung > Port-Tabelle

Mögliche Werte:

nein
ja

Default-Wert:

nein

Status-Update-In-Minuten

Legen Sie mit diesem Eintrag ein Intervall in Minuten fest, in dem die Nutzungsstatistik aktualisiert wird.

SNMP-ID:

2.101.5

Pfad Telnet:

Setup > Layer-7-App-Erkennung

Mögliche Werte:

max. 5 Zeichen aus [0–9]

Default-Wert:

60

Max-Warteschlangenlaenge

Legen Sie mit diesem Eintrag die maximale Warteschlangenlänge für die Nutzungsstatistik fest.

SNMP-ID:

2.101.6

Pfad Telnet:

Setup > Layer-7-App-Erkennung

Mögliche Werte:

max. 5 Zeichen aus [0–9]

Default-Wert:

10000

Statistik-Zuruecksetzen

Löschen Sie mit diesem Eintrag die Nutzungsstatistik der Layer-7-Anwendungserkennung.

SNMP-ID:

2.101.7

Pfad Telnet:**Setup > Layer-7-App-Erkennung****HTTP-HTTPS-Erfassung**

Definieren Sie in diesem Menü Einträge für die Überwachung von HTTP / HTTPS-Verbindungen.

SNMP-ID:

2.101.8

Pfad Telnet:**Setup > Layer-7-App-Erkennung****Anwendungsname**

Name für die Überwachung von HTTP / HTTPS-Verbindungen (z. B. Youtube).

SNMP-ID:

2.101.8.1

Pfad Telnet:**Setup > Layer-7-App-Erkennung > HTTP-HTTPS-Erfassung****Mögliche Werte:**

max. 64 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Ziele**

Geben Sie hier die Ziele für die Überwachung von HTTP / HTTPS-Verbindungen an (z. B. youtube).

 Mehrere Ziele geben Sie durch eine kommaseparierte Liste an (z. B. youtube, googlevideo, ytimg)**SNMP-ID:**

2.101.8.2

Pfad Telnet:**Setup > Layer-7-App-Erkennung > HTTP-HTTPS-Erfassung****Mögliche Werte:**

max. 254 Zeichen aus [A-Z][a-z][0-9]#{|}~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default-Wert:*leer***Prio**

Legen Sie hier die Priorität der HTTP/HTTPS-Erfassung durch die Layer-7-Anwendungserkennung fest.

SNMP-ID:

2.101.8.3

Pfad Telnet:**Setup > Layer-7-App-Erkennung > HTTP-HTTPS-Erfassung****Mögliche Werte:**

max. 5 Zeichen aus [0-9]

Default-Wert:

0

VLAN

Geben Sie hier die zu überwachenden VLAN-IDs an und legen Sie fest, in welchem Umfang die Layer-7-Anwendungserkennung Traffic-Informationen erfasst.



Damit die Layer-7-Anwendungserkennung im VLAN aktiv ist, muss das Gerät zumindest applikationsspezifischen Daten erfassen.

SNMP-ID:

2.101.11

Pfad Telnet:**Setup > Layer-7-App-Erkennung****VLAN-Id**

Legen Sie mit diesem Eintrag eine VLAN-ID fest.

SNMP-ID:

2.101.11.1

Pfad Telnet:**Setup > Layer-7-App-Erkennung > VLAN****Mögliche Werte:**

0 ... 65535

Default-Wert:

0

Benutzer-Tracking

Mit diesem Eintrag aktivieren oder deaktivieren Sie die Erfassung von benutzerspezifischen Daten (Benutzer- oder Client-Name sowie MAC-Adresse).

SNMP-ID:

2.101.11.2

Pfad Telnet:

Setup > Layer-7-App-Erkennung > VLAN

Mögliche Werte:

nein
ja

Default-Wert:

nein

Tracking-Aktiv

Mit diesem Eintrag aktivieren oder deaktivieren Sie die Erfassung von allgemeinen bzw. applikationsspezifischen Daten.

SNMP-ID:

2.101.11.3

Pfad Telnet:

Setup > Layer-7-App-Erkennung > VLAN

Mögliche Werte:

nein
ja

Default-Wert:

nein

Speichern-In-Min

Geben Sie das Intervall in Minuten an, in dem Nutzungsstatistik der Layer-7-Anwendungserkennung gespeichert werden soll.

SNMP-ID:

2.101.12

Pfad Telnet:**Setup > Layer-7-App-Erkennung****Mögliche Werte:**

max. 5 Zeichen aus [0-9]

Default-Wert:

3600

9.1.3 Ergänzungen im Status-Menü

Layer-7-App-Erkennung

In diesem Menü erhalten Sie Informationen über die Anwendungen, die die Layer-7-Anwendungserkennung überwacht.

SNMP-ID:

1.95

Pfad Telnet:**Status**

Anwendungen

In dieser Tabelle wird angezeigt, welcher Client wie viel Traffic von / zu einem Dienst verursacht hat. Der Inhalt dieser Tabelle wird regelmäßig bootpersistent gespeichert.

Innerhalb dieser Tabelle wird der Name des Benutzers oder Clients angezeigt, sofern dieser zu ermitteln ist. Für "Benutzername" wird zuerst versucht, den 802.1X-Benutzernamen anzuzeigen. Wird kein 802.1X verwendet, wird der mittels DHCP-Snooping ermittelte Client-Hostname angezeigt.

Zusätzlich wird in der Spalte "PSpot-Benutzer" für angemeldete Public Spot-Benutzer deren Benutzername angezeigt.



Die Anzeige von Public Spot-Benutzernamen funktioniert nur, wenn das Public Spot-Modul auf demselben Gerät aktiv ist, auf dem auch die Layer-7-Anwendungserkennung aktiviert ist.

SNMP-ID:

1.95.1

Pfad Telnet:**Status > Layer-7-App-Erkennung**

Gesamter-Traffic-pro-Anwendung

In dieser Tabelle wird der Traffic nach Dienst Applikation gruppiert zusammengefasst dargestellt.

SNMP-ID:

1.95.2

Pfad Telnet:**Status > Layer-7-App-Erkennung****Gesamter-Traffic-pro-Benutzer**

In dieser Tabelle wird der Traffic nach Benutzern gruppiert dargestellt.

Innerhalb dieser Tabelle wird der Name des Benutzers oder Clients angezeigt, sofern dieser zu ermitteln ist. Für "Benutzername" wird zuerst versucht, den 802.1X-Benutzernamen anzuzeigen. Wird kein 802.1X verwendet, wird der mittels DHCP-Snooping ermittelte Client-Hostname angezeigt.

Zusätzlich wird in der Spalte "PSpot-Benutzer" für angemeldete Public Spot-Benutzer deren Benutzername angezeigt.



Die Anzeige von Public Spot-Benutzernamen funktioniert nur, wenn das Public Spot-Modul auf demselben Gerät aktiv ist, auf dem auch die Layer-7-Anwendungserkennung aktiv ist.

SNMP-ID:

1.95.3

Pfad Telnet:**Status > Layer-7-App-Erkennung****HTTP-HTTPS-Hit-Liste**

In dieser Tabelle werden die Treffer der Überwachung von HTTP/HTTPS-Verbindungen angezeigt.

SNMP-ID:

1.95.4

Pfad Telnet:**Status > Layer-7-App-Erkennung****Aktiv**

Dieser Eintrag zeigt Ihnen, ob die Layer-7-Anwendungserkennung aktiviert oder deaktiviert ist.

SNMP-ID:

1.95.5

Pfad Telnet:**Status > Layer-7-App-Erkennung****Statistik-Zuruecksetzen**

Löschen Sie mit diesem Eintrag die Nutzungsstatistik der Layer-7-Anwendungserkennung.

SNMP-ID:

1.95.6

Pfad Telnet:

Status > Layer-7-App-Erkennung