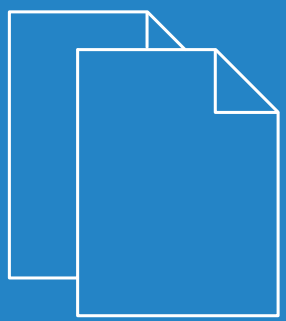
SICHER. **VERNETZT.**

LCOS 10.32

Addendum



08/2019

LANCOM
Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS-Version 10.32

Dieses Dokument beschreibt die Änderungen und Ergänzungen in den LCOS-Versionen 10.30 und 10.32 gegenüber der vorherigen Version.

2 Konfiguration

2.1 Software zur Konfiguration

2.1.1 WEBconfig mit TLS 1.3

Ab LCOS 10.30 unterstützt Ihr Gerät TLS 1.3 für den Zugriff auf WEBconfig. TLS 1.3 stellt die neueste Weiterentwicklung des TLS-Standards dar und bietet z. B. durch die ausschließliche Verwendung moderner Cipher-Suiten und Perfect Forward Secrecy eine verbesserte Sicherheit im Vergleich zu den Vorgängerversionen.

Bei einem LCOS-Update wird die TLS 1.3-Unterstützung für WEBconfig automatisch zur Konfiguration hinzugefügt. Entfernen Sie gegebenenfalls ältere Verfahren, die für WEBconfig nicht mehr angeboten werden sollen.

Ergänzungen im Setup-Menü

Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.21.40.3

Pfad Konsole:

Setup > **HTTP** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default-Wert:

TLSv1.2

TLSv1.3

2.1.2 Befehle für die Konsole

Ab LCOS 10.30 unterstützt Ihr Gerät die folgenden neuen Befehle bzw. Optionen.

Tabelle 1: Übersicht aller neuen Befehle auf der Kommandozeile

Befehl	Beschreibung
`clear`	Löscht die aktuelle Konsolenausgabe. Im Log lassen sich weiter alle bisher eingegebenen Befehle einsehen.

Neue Optionen des ping-Befehls

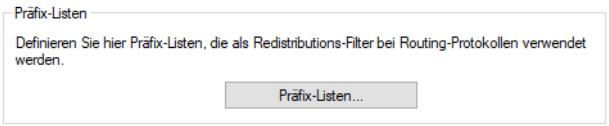
Ab LCOS 10.30 unterstützt Ihr Gerät die folgenden neuen Parameter für den ping-Befehl:

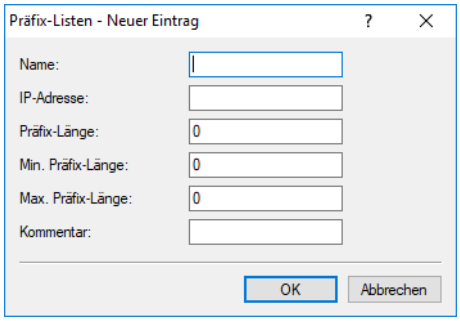
Parameter	Bedeutung
`-b`	Nicht aufhören zu pingen, wenn ein PacketTooBig(DF) empfangen wird, damit man „Path MTU Discovery“ hat.
`[-x x]`	Atomare Fragmente: (n)ever, (f)orce, (a)utomatic
`%scope`	Name des Interfaces über welches das Paket bei der Verwendung von Link-Lokalen-Adressen als Ziel versendet werden soll.
`%scope@rtg-tag`	Name des Interfaces über welches das Paket bei der Verwendung von Link-Lokalen-Adressen als Ziel versendet werden soll mit zusätzlicher Angabe des Routing-Tags.
`%%interface`	Name des Ziel-Interfaces. Das Paket wird direkt und ohne Berücksichtigung der Routing-Tabelle an das Interface gesendet.
`@rtg-tag`	Routing-Tag, das zum Senden des Pakets verwendet werden soll.

3 Routing und WAN-Verbindungen

3.1 Filterliste für Redistribution in BGP

Mit Hilfe von Filterlisten für die Redistribution bei BGP können bestimmte Präfixe für die Redistribution erlaubt oder verweigert werden. Dazu legen Sie die Präfix-Filterliste unter **IP-Router** > **Allgemein** > **Präfix-Listen** an.





Name

Geben Sie hier diesem Eintrag einen Namen.

IP-Adresse

Geben Sie hier die IPv4- oder IPv6-Adresse des Netzwerkes an.

Präfix-Länge

Enthält die Netzmaske oder Präfix-Länge des Netzwerkes. Dieser Eintrag legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind. Die Präfix-Länge muss für eine Übereinstimmung diesem Wert exakt entsprechen, wenn nicht für **Min. Präfix-Länge** und **Max. Präfix-Länge** andere Werte vorgegeben sind.

Beim Wert „0" stimmt das Präfix für diese Regel dann überein, wenn es aus derselben IP-Adressfamilie stammt, die unter **IP-Adresse** vorgegeben ist.

Min. Präfix-Länge

Geben Sie hier die minimale Präfix-Länge an, die das Präfix für eine Übereinstimmung aufweisen darf.

Max. Präfix-Länge

Geben Sie hier die maximale Präfix-Länge an, die das Präfix für eine Übereinstimmung aufweisen darf.

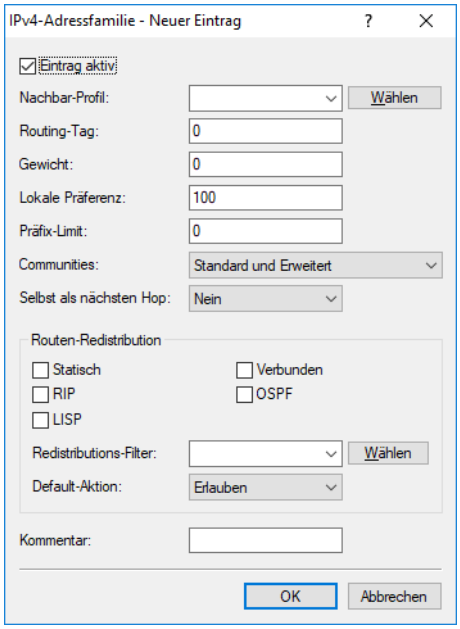
Kommentar

Kommentar zu diesem Eintrag.

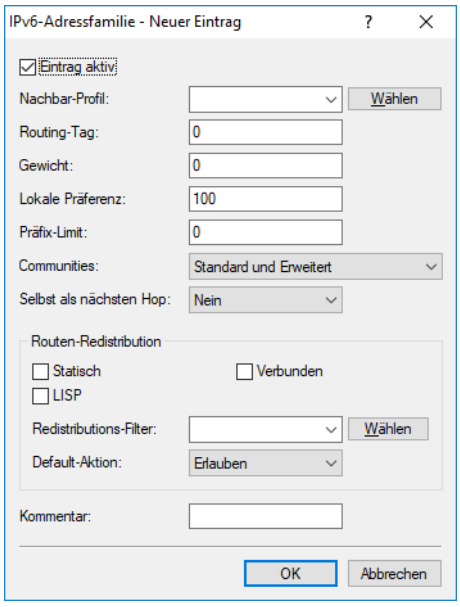
Verwendung der Präfix-Listen bei BGP

Diese **Präfix-Listen** können Sie dann bei den IPv4- und IPv6-Adressfamilien des BGP-Protokolls referenzieren sowie definieren, ob diese Präfix-Listen erlaubt oder abgelehnt werden sollen.

Routing Protokolle > **BGP** > **IPv4-Adressfamilie**



Routing Protokolle > **BGP** > **IPv6-Adressfamilie**



Redistributions-Filter

Name der Präfix-Filterliste.

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die nicht in der Präfix-Liste konfiguriert sind. Mögliche Werte:

Erlauben

Verweigern

3.1.1 Ergänzungen im Setup-Menü

Redistributions-Filter

Name der Präfix-Filterliste aus **Setup** > **Routing-Protokolle** > **Filter** > **Praefix-Liste**.

SNMP-ID:

2.93.1.4.1.11

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`

Default-Wert:

leer

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind.

SNMP-ID:

2.93.1.4.1.12

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Erlauben

Redistributions-Filter

Name der Präfix-Filterliste aus **Setup** > **Routing-Protokolle** > **Filter** > **Praefix-Liste**.

SNMP-ID:

2.93.1.4.2.11

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`

Default-Wert:

leer

Default-Aktion

Definiert, wie Präfixe standardmäßig behandelt werden sollen, die in der Präfix-Liste konfiguriert sind.

SNMP-ID:

2.93.1.4.2.12

Pfad Konsole:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

Erlauben
Ablehnen

Default-Wert:

Erlauben

Filter

Mit Hilfe von Filterlisten für die Redistribution bei BGP können bestimmte Präfixe für die Redistribution erlaubt oder verweigert werden.

SNMP-ID:

2.93.5

Pfad Konsole:

Setup > **Routing-Protokolle**

Praefix-Liste

Hier wird eine Präfix-Liste definiert, die bei BGP referenziert werden kann.

SNMP-ID:

2.93.5.1

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.93.5.1.1

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter** > **Praefix-Liste**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`

Default-Wert:

leer

IP-Adresse

Enthält die IPv4- oder IPv6-Adresse des Netzwerkes.

SNMP-ID:

2.93.5.1.2

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter** > **Praefix-Liste**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

Default-Wert:

leer

Praefix-Laenge

Enthält die Netzmaske oder Präfix-Länge des Netzwerkes. Dieser Eintrag legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind. Die Präfix-Länge muss für eine Übereinstimmung diesem Wert exakt entsprechen, wenn nicht für **Laenge-Min** und **Laenge-Max** andere Werte vorgegeben sind.

Beim Wert „0" stimmt das Präfix für diese Regel dann überein, wenn es aus derselben IP-Adressfamilie stammt, die unter **IP-Adresse** vorgegeben ist.

SNMP-ID:

2.93.5.1.3

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter** > **Praefix-Liste**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

leer

Laenge-Min

Enthält die minimale Präfix-Länge, die das Präfix für eine Übereinstimmung aufweisen darf.

SNMP-ID:

2.93.5.1.4

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter** > **Praefix-Liste**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

leer

Laenge-Max

Enthält die maximale Präfix-Länge, die das Präfix für eine Übereinstimmung aufweisen darf.

SNMP-ID:

2.93.5.1.5

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter** > **Praefix-Liste**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.5.1.6

Pfad Konsole:

Setup > **Routing-Protokolle** > **Filter** > **Praefix-Liste**

Mögliche Werte:

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

Default-Wert:

leer

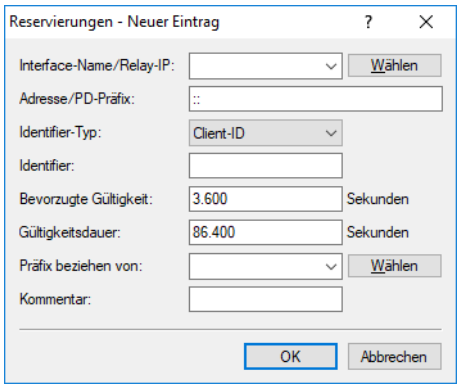
4 IPv6

4.1 DHCPv6

4.1.1 DHCPv6-Server

Erweiterung bei Client-Reservierungen im DHCPv6-Server

Ab LCOS 10.30 wird der Parameter **Client-ID** durch die beiden neuen Parameter **Identifier** und **Identifier-Typ** ersetzt. Dadurch können im DHCPv6-Server ab sofort Client-Adressen bzw. Präfixe wahlweise anhand von DUID, MAC-Adresse, Interface-ID (nach RFC 3315) oder Remote-ID (nach RFC 4649) zugewiesen werden. Die entsprechenden Einstellungen erfolgen in LANconfig unter **IPv6** > **DHCPv6** > **Reservierungen**:



Identifier-Typ

Dieser Typ gibt an, wie der **Identifier** zu interpretieren ist.

Client-ID

Der Identifier gibt die Client-DUID an, z. B. 0003000100a057000001.

MAC-Adresse

Der Identifier gibt eine MAC-Adresse an, z. B. 00a057000001. Wenn der Client direkt mit dem Server kommuniziert, dann wird die MAC-Adresse aus dem DHCPv6-Paket genommen. Wenn Relay-Agents dazwischen sind, dann wird sie aus der Client-Link-Layer-Address-Option (Code 79, RFC 6939) der Relay-Forward-Message des client-nächsten Relay-Agents genommen.

Schnittstellen-ID

Der Identifier gibt die Schnittstellen-ID aus der Schnittstellen-ID-Option (Code 18) der Relay-Forward-Message des client-nächsten Relay-Agents an. Dies funktioniert nur mit einem Relay-Agent.

Remote-ID

Der Identifier gibt die Remote-ID aus der Remote-ID-Option (Code 37, RFC 4649) der Relay-Forward-Message des client-nächsten Relay-Agents an. Dies funktioniert nur mit einem Relay-Agent.

Identifier

Eindeutiger Bezeichner zur Identifizierung des DHCPv6-Clients. Der verwendete Typ zur Identifizierung wird durch den Parameter Identifier-Typ konfiguriert.

Mögliche Formate:

- Angabe als Client-DUID, z. B. 0003000100a057000001
- Angabe als MAC-Adresse z. B. 00a057000001
- Angabe als Interface-ID oder Remote-ID, z. B. „INTRANET"

Ergänzungen im Setup-Menü

Identifier

Eindeutiger Bezeichner zur Identifizierung des DHCPv6-Clients. Der verwendete Typ zur Identifizierung wird durch den Parameter Identifier-Typ konfiguriert.

Mögliche Formate:

- Angabe als Client-DUID, z. B. 0003000100a057000001
- Angabe als Mac-Adresse z. B. 00a057000001
- Angabe als Interface-ID oder Remote-ID, z. B. INTRANET

SNMP-ID:

2.70.3.1.6.3

Pfad Konsole:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Ein Hexstring mit max. 127 Zeichen aus `[a-z][0-9]:-`

Default-Wert:

leer

Identifier-Typ

Dieser Typ gibt an, wie der Identifier in **Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservierungen** > **Identifier** zu interpretieren ist.

SNMP-ID:

2.70.3.1.6.8

Pfad Konsole:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Client-ID

Der Identifier gibt die Client-DUID an, z. B. 0003000100a057000001.

Mac-Adresse

Der Identifier gibt eine MAC-Adresse an, z. B. 00a057000001. Wenn der Client direkt mit dem Server kommuniziert, dann wird die MAC-Adresse aus dem DHCPv6-Paket genommen. Wenn Relay-Agents dazwischen sind, dann wird sie aus der Client-Link-Layer-Address-Option (Code 79, RFC 6939) der Relay-Forward-Message des client-nächsten Relay-Agents genommen.

Interface-ID

Der Identifier gibt die Interface-ID aus der Interface-ID-Option (Code 18) der Relay-Forward-Message des client-nächsten Relay-Agents an. Dies funktioniert nur mit einem Relay-Agent.

Remote-ID

Der Identifier gibt die Remote-ID aus der Remote-ID-Option (Code 37, RFC 4649) der Relay-Forward-Message des client-nächsten Relay-Agents an. Dies funktioniert nur mit einem Relay-Agent.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

SNMP-ID:

2.70.3.1.6.9

Pfad Konsole:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

5 Firewall

5.1 SD-WAN Application Routing / Layer-7-Applikationskontrolle

Profitieren Sie von einem deutlichen Performance-Gewinn bei der Nutzung moderner Business-Anwendungen in der Cloud (z. B. Microsoft Office 365, AWS, etc). Application Routing leitet anhand definierter Regeln vertrauenswürdige Anwendungen von der Filiale direkt ins Internet. Dies entlastet sowohl die VPN-Strecke zur Zentrale als auch die Internetleitung in der Zentrale.

Microsoft empfiehlt diese Betriebsart explizit für Office 365. Da diese Web-basierten Dienste häufig keine feste IP-Adresse haben, ist nur eine Erkennung anhand der DNS-Namen möglich. Zu diesem Zweck können entsprechende DNS-Ziele in der Firewall mit einem passenden Wildcardausdruck erstellt werden, sodass diese Pakete mit einem anderen Routingtag markiert werden, um dann später im Router direkt ins Internet geroutet zu werden. Alternativ kann an dieser Stelle auch eine Layer-7-Applikationskotrolle in der Firewall realisiert werden. Somit bewahren Sie die Kontrolle über die Nutzung internetbasierter Anwendungen in Ihrem Netzwerk. Durch die Definition von Regeln für DNS-basierte Anwendungen entscheiden Sie selbst, welche Dienste erlaubt, gesperrt, limitiert oder priorisiert werden.

Wenn nun ein Benutzer ein solches DNS-Ziel in seinem Browser aufruft, dann schickt sein Rechner eine DNS-Anfrage für diese Domäne. Der DNS-Forwarder im LANCOM Router leitet diese Anfrage dann an den Internet Service Provider weiter. Wenn die Antwort kommt, dann speichert der Router die zurückgelieferte IP-Adresse und diese Auflösung steht fortan der Firewall zur Verfügung. Anschließend geht die Antwort an den ursprünglich anfragenden Rechner weiter. Somit kann der Browser die Verbindung zu der zurückgelieferten IP-Adresse öffnen. Die Firewall erkennt die gerade vorher gelernte IP-Adresse und kann ein entsprechendes Routing-Tag zuweisen. Daneben sind auch andere definierte Firewall-Aktionen wie Erlauben, Sperren, Limitieren oder Priorisieren für dieses Ziel anwendbar.

Dadurch, dass die Firewall sich über die DNS-Auflösung genau die Adresse merkt, die der Benutzer für die Domäne anschließend verwendet, funktioniert dieser Mechanismus auch, wenn der Domänenname auf viele unterschiedliche oder zeitlich wechselnde IP-Adressen auflöst.

Einsatzempfehlungen

Der LANCOM Router muss als DNS-Server bzw. DNS-Forwarder im Netz dienen, d. h. Clients im lokalen Netzwerk müssen den Router als DNS-Server verwenden. Zusätzlich muss die direkte Nutzung von DNS-over-TLS und DNS-over-HTTPS (ggf. browserintern) mit externen DNS-Servern durch Clients verhindert werden.

Dies kann wie folgt erreicht werden:

- Der DHCP-Server muss die IP-Adresse des Routers als DNS-Server verteilen (wird standardmäßig vom Internet-Wizard eingerichtet)
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern verhindern, z. B. durch Sperrung des ausgehenden Ports 53 (UDP) für Clients aus dem entsprechenden Quellnetzwerk
- Einrichtung von Firewall-Regeln, die die direkte Nutzung von externen DNS-Servern mit Unterstützung von DNS-over-TLS verhindern, z. B. durch Sperrung des ausgehenden Ports 853 (TCP) für Clients aus dem entsprechenden Quellnetzwerk
- DNS-over-HTTPS (DoH) im Browser deaktivieren

Hinweise zur Synchronisierung der DNS-Datenbank der Firewall:

Da die Firewall ihre Informationen aus den DNS-Anfragen der Clients lernt, kann es in bestimmten Situationen dazu kommen, dass die DNS-Datenbank noch nicht vollständig ist. Dies kann in folgenden Situationen passieren:

- Es wird eine neue Firewall-Regel hinzugefügt, der Client hat aber noch einen DNS-Eintrag zwischengespeichert
- Kurz nach Neustart des Routers und der Client hat aber noch einen DNS-Eintrag zwischengespeichert

In diesen Fällen hilft ein Leeren des DNS-Cache auf dem Client, ein Reboot des Clients oder ein Timeout des DNS-Eintrags auf dem Client.

Eigene Dienste wie z. B. ping vom Router selbst laufen nicht über die erstellten Firewall-Regeln. Mit Hilfe von ping auf einen vollständigen DNS-Namen (nicht Wildcard-Ausdruck) kann die Erzeugung von Regelauflösungen (DNS zu IP-Adressen) bei Bedarf entweder auf der CLI (einmalig) oder per Cron-Job durchgeführt werden.

Wenn unterschiedliche DNS-Namen auf dieselbe IP-Adresse aufgelöst werden, dann können diese nicht unterschieden werden. In diesem Fall trifft immer die erste Regel zu, die einen dieser DNS-Namen referenziert. Das sollte bei großen Dienstanbietern kein Problem sein. Bei kleinen Websites, die vom selben Anbieter gehostet werden, könnte es jedoch auftreten.

show fw-dns-destinations

Dieser neue Parameter für den Kommandozeilen-Befehl `show` nimmt optional eine leerzeichen-separierte Liste von Namen der DNS-Ziele an. Er führt alle DNS-Ziele oder die in der Parameterliste angegebenen in ihrer Reihenfolge auf. Für jedes Ziel zeigt er die Zähler aus **Status** > **Firewall** > **DNS-Datenbank** > **Zielverwendung**, gefolgt von der Liste ihrer Wildcardausdrücke. Für jeden Wildcardausdruck zeigt er die aktuell aufgelösten Adressen und die direkt oder indirekt matchenden Datensätze.

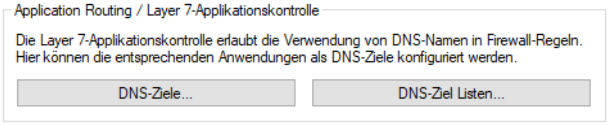
Trace

Für das anwendungsbasierte Routing gibt es den neuen Parameter `FW-DNS` für das trace-Kommando. Mit diesem können die Änderungen an der Firewall-Datenbank der DNS-Ziele überwacht werden:

- Wenn ein DNS-Paket eintrifft, werden das Paket und die betroffenen Wildcardausdrücke und Ziele ausgegeben.
- Wenn die TTL (Time-to-Live – Lebensdauer) eines Eintrags abläuft, dann werden dieser Datensatz und die betroffenen Wildcardausdrücke und Ziele ausgegeben.
- Wenn eine der beiden Firewalls ein DNS-Ziel registriert oder deregistriert, weil sich ihre Konfiguration geändert hat.
- Wenn sich die Tabellen **Setup** > **Firewall** > **DNS-Ziele** oder **Setup** > **Firewall** > **DNS-Ziel-Liste** ändern.

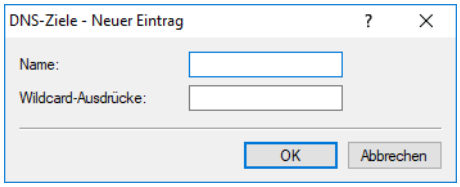
5.1.1 Konfiguration

Die Einstellungen zum anwendungsbasierten Routing bzw. der Layer-7-Applikationskontrolle finden Sie unter **Firewall / Qos** > **Allgemein** > **Application Routing / Layer 7-Applikationskontrolle**.



DNS-Ziele

Defninieren Sie in LANconfig unter **Firewall / Qos** > **Allgemein** > **Anwendungsbasiertes Routing** > **DNS-Ziele** die Namen und Wildcardausdrücke für die DNS-Ziele, die Sie in der Firewall gesondert behandeln wollen.



Name

Der Name für dieses DNS-Ziel. Dieser Name wird verwendet, um dieses Objekt zu referenzieren.

Wildcard-Ausdrücke

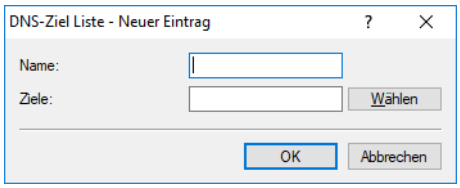
Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Wildcardausdrücken. Die Ausdrücke können beliebig viele ? (ein beliebiges Zeichen) und * (mehrere beliebige Zeichen) enthalten, z. B. „*.lancom.*“. Die Eingabe ist auf 252 Zeichen beschränkt. Wenn Sie für einen Dienst mehr DNS-Wildcard-Asudrücke benötigen, dann können Sie mehrere DNS-Ziele in der **DNS-Ziel-Liste** zu einem referenzierbaren Objekt zusammenfassen.

Unicodezeichen für internationalisierte Domainnamen können wie folgt eingegeben werden:

- UTF-8: Hier müssen ein bis vier Bytes einzeln als '\x', gefolgt von zwei hexadezimalen Ziffern, eintragen werden.
- UTF-16: Hier müssen ein oder zwei Doppelbytes als '\u', gefolgt von vier hexadezimalen Ziffern, eintragen werden.
- UTF-32: Hier muss der Wert als '\U', gefolgt von acht hexadezimalen Ziffern, eintragen werden.

DNS-Ziel-Liste

Defninieren Sie in LANconfig unter **Firewall / Qos** > **Allgemein** > **Anwendungsbasiertes Routing** > **DNS-Ziel-Liste** die DNS-Ziele in einer Liste, die Sie in der Firewall gemeinsam als ein Objekt referenzieren wollen.



Name

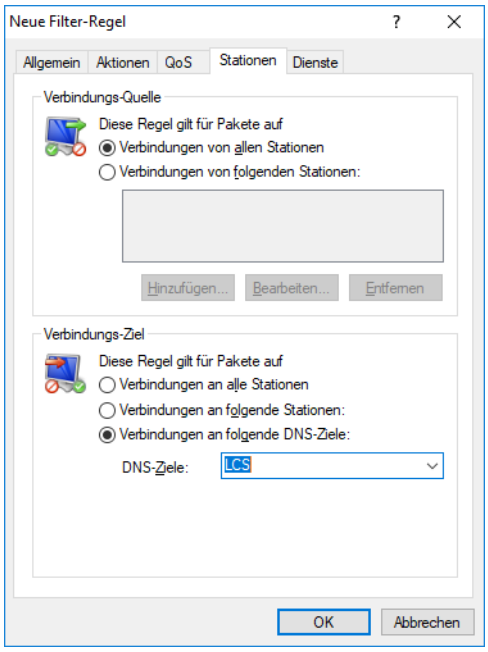
Name der Liste aus DNS-Zielen

Ziele

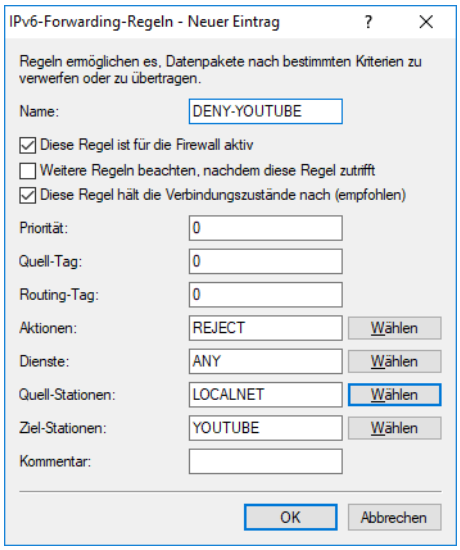
Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Namen der DNS-Ziele.

Referenzierung in den Firewall-Regeln

In **Firewall / Qos** > **IPv4-Regeln** > **Regeln** können Sie eine neue Filter-Regel anlegen und dort auf dem Reiter **Stationen** unter **Verbindungen an folgende DNS-Ziele** aus den konfigurierten DNS-Zielen auswählen.



In **Firewall / Qos** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** können Sie eine neue Regel anlegen. Als **Ziel-Stationen** können Einträge aus den Tabellen **DNS-Ziele** bzw. **DNS-Ziel-Liste** verwendet werden.



5.1.2 Ergänzungen im Setup-Menü

DSCP-Support

Wenn Sie diesen Parameter auf Ja setzen, dann wird das DiffServ-Feld im Header von IPv6-Paketen beachtet und folgendermaßen ausgewertet:

- **CSx (inklusive CS0 = BE)**: normal übertragen
- **AFxx**: gesichert übertragen

- **EF**: bevorzugt übertragen

SNMP-ID:

2.70.5.25

Pfad Konsole:

Setup > **IPv6** > **Firewall**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Firewall

Einstellungen der Firewall.

SNMP-ID:

2.110

Pfad Konsole:

Setup

DNS-Ziele

Ab LCOS 10.30 können DNS-Namen in der Firewall verwendet werden. DNS-Namen können vollständig definiert sein, z. B. „www.lancom.de“ oder als Wildcard-Ausdruck, z. B. „*lancom*“, definiert sein. Diese so definierten Objekte können als Ziele in Firewall-Regeln verwendet werden. Layer-7-(Web-)Applikationen können gesperrt, erlaubt, limitiert, priorisiert oder in einen anderen Routing-Kontext umgeleitet werden.

Weitere Informationen und Einsatzempfehlungen finden Sie im Referenzhandbuch im Kapitel Firewall.

SNMP-ID:

2.110.1

Pfad Konsole:

Setup > **Firewall**

Name

Der Name für dieses DNS-Ziel. Dieser Name wird verwendet, um dieses Objekt zu referenzieren.

SNMP-ID:

2.110.1.1

Pfad Konsole:

Setup > **Firewall** > **DNS-Ziele**

Mögliche Werte:

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

Default-Wert:

leer

Wildcard-Ausdruecke

Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Wildcardausdrücken. Die Ausdrücke können beliebig viele ? (ein beliebiges Zeichen) und * (mehrere beliebige Zeichen) enthalten, z. B. „*.lancom.*“. Die Eingabe ist auf 252 Zeichen beschränkt. Wenn Sie für einen Dienst mehr DNS-Wildcard-Asudrücke benötigen, dann können Sie mehrere DNS-Ziele in der **DNS-Ziel-Liste** zu einem referenzierbaren Objekt zusammenfassen.

Unicodezeichen für internationalisierte Domainnamen können wie folgt eingegeben werden:

- UTF-8: Hier müssen ein bis vier Bytes einzeln als '\x', gefolgt von zwei hexadezimalen Ziffern, eintragen werden.
- UTF-16: Hier müssen ein oder zwei Doppelbytes als '\u', gefolgt von vier hexadezimalen Ziffern, eintragen werden.
- UTF-32: Hier muss der Wert als '\U', gefolgt von acht hexadezimalen Ziffern, eintragen werden.

SNMP-ID:

2.110.1.2

Pfad Konsole:

Setup > **Firewall** > **DNS-Ziele**

Mögliche Werte:

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

Default-Wert:

leer

DNS-Ziel-Liste

In der DNS-Ziel-Liste können Sie mehrere DNS-Ziele zu einem referenzierbaren Objekt zusammenfassen.

SNMP-ID:

2.110.2

Pfad Konsole:

Setup > **Firewall**

Name

Der Name für diese DNS-Ziel-Liste. Dieser Name wird verwendet, um dieses Objekt zu referenzieren.

SNMP-ID:

2.110.2.1

Pfad Konsole:

Setup > **Firewall** > **DNS-Ziel-Liste**

Mögliche Werte:

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

Default-Wert:

leer

Ziele

Enthält eine mittels Kommata oder Leerzeichen separierte Liste von Namen der DNS-Ziele.

SNMP-ID:

2.110.2.2

Pfad Konsole:

Setup > **Firewall** > **DNS-Ziel-Liste**

Mögliche Werte:

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

Default-Wert:

leer

6 Wireless LAN – WLAN

6.1 Rückkehr auf den ursprünglichen 5 GHz-Kanal bei konfigurierter Bevorzugung

Ab LCOS 10.30 RU1 unterstützen alle LCOS-Geräte mit WLAN-Modul die Rückkehr auf den ursprünglichen 5 GHz-Kanal, wenn eine Bevorzugung konfiguriert ist. Dieses Feature ermöglicht die weitestgehende Einhaltung eines Kanalplans auch für Installationen, die nicht den Indoor-only-Modus verwenden und daher von Kanalwechseln durch Radarerkennung betroffen sein könnten.

Konfiguriert man für ein auf 5 GHz betriebenes und nicht im Indoor-Only-Modus befindliches WLAN-Modul einen WLAN-Kanal oder die WLAN-Kanalliste, dann werden die dort eingetragenen Kanäle bevorzugt verwendet. Nur wenn die dort eingestellten Kanäle durch Radarerkennung blockiert wurden, wird von diesen abgewichen.

Mit dem hier beschriebenen Feature wird der Access Point nach Ablauf der DFS-Sperrzeit versuchen, wieder auf den eingestellten Kanal zurückwechseln. Ist dieser Kanal weiterhin nicht verfügbar, wird ein ggf. in der Kanalliste konfigurierter Kanal verwendet. Die DFS-Sperrzeit tritt in Kraft, sobald ein Kanal wegen Radarerkennung gesperrt wurde und sie beträgt in der Regel 30 Minuten.

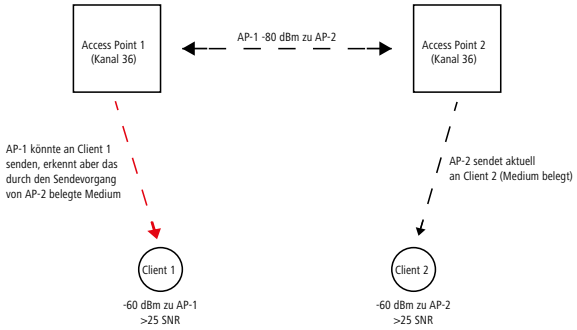
Ist kein dedizierter Kanal für das WLAN-Modul konfiguriert (Kanalliste leer und Radio-Kanal „0“ bzw. „Automatisch“), ändert sich das bisherige Verhalten nicht. Bei einem durch Radarerkennung ausgelösten Kanalwechsel wird der neue Kanal beibehalten und nicht auf den zuletzt verwendeten Kanal zurückgewechselt.

Diese Bevorzugung hilft dabei, feste Kanalschemata in 5 GHz nutzen zu können, da nach DFS-Events schneller wieder die volle Kapazität des Netzwerkes genutzt werden kann.

Es gibt keine Konfigurationsmöglichkeit. Falls Sie für ein auf 5 GHz betriebenes und nicht im Indoor-Only-Modus befindliches WLAN-Modul einen WLAN-Kanal oder die WLAN-Kanalliste konfigurieren, dann ist dieses Feature automatisch aktiv.

6.2 Reduzierung der Empfindlichkeit für empfangene Pakete

In High Density-Szenarien wie Stadien, Messehallen oder Auditorien kommt es unausweichlich zu einer hohen Auslastung des Mediums durch Access Points, die den gleichen Kanal benutzen. Dadurch kann eine Situation entstehen, bei der die Access Points ihre Übertragungen an die Clients zurückhalten, weil der Kanal häufiger als belegt erkannt wird.



Durch eine ab LCOS 10.30 RU1 mögliche Reduzierung der Empfangssempfindlichkeit kann ein Access Points künstlich „tauber" eingestellt werden. Hierdurch werden Übertragungen, die weiter entfernt sind, vom Access Point „überhört" und der Kanal wird somit öfter als „frei" erkannt. Es sind somit vereinfacht gesprochen mehr gleichzeitige Übertragungen auf dem gleichen Kanal möglich. Einserseits steigt dadurch der Gesamtdurchsatz eines Systems, aber auf der anderen Seite steigt auch die Interferenz auf Seiten der Clients.

Ein Client weiß nämlich nichts von der künstlichen Schwerhörigkeit. Er empfängt weiterhin die gewollten Signale seines Access Points sowie die Signale der anderen Access Points auf dem gleichen Kanal. Nur wenn der Signal-zu-Rauschabstand (SNR) weiterhin gut bleibt, werden die zusätzlichen Übertragungen dank dieses Features auch sauber vom Client empfangen. Ein weiterer Nebeneffekt des Unwissens der Clients ist, dass ein zu hoch eingestellter Wert den Effekt ins Gegenteil verkehren kann. Da der Access Point nicht zwischen Übertragungen von eigenen Clients und von anderen Geräten – sowohl Access Points als auch Clients – unterscheiden kann, wird nur das gehört, was über dem eingestellten Schwellenwert liegt – egal von wem es kommt. Es kann somit passieren, dass die Übertragung eines verbundenen Clients vom Access Point nicht mehr „gehört" wird. Hierduch ensteht eine asymmetrische Verbindung, der Client wird den Access Point möglicherweise noch gut empfangen und geht daher von einer guten Verbindung aus, während der Access Point vom Client nichts mehr mitbekommt und ihn somit ignoriert. Empfehlenswert ist, die Reduzierung so einzustellen, dass dadurch keine Benachteiligung von Clients entsteht.

Die Reduzierung stellen Sie über die Konsole im Wert **Setup** > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **Rx-Paket-Empf.-Reduktion** ein. Der Wertebereich von 0-20 entspricht dabei einer minimalen Empfangsstärke im Bereich von -95 dBm (0) bis -75 dBm (20). Prinzipiell treten bei den WLAN-Funkmodulen herstellungsbedingt Streuungen auf. Dadurch kann die reale Empfangsstärke geringfügig abweichen.

Für WLAN-Controller kann diese Einstellung ebenfalls über die Konsole im Profil eines Access Points vorgenommen werden. Also unter **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen** die Werte **Modul-1-Rx-Paket-Empf.-Reduktion** resp. **Modul-2-Rx-Paket-Empf.-Reduktion** entsprechend anpassen.

Dieses Feature ist für Experten! Wie in der Beschreibung bereits gesagt, kann es statt einem Mehrwert auch das Gegenteil bewirken und Übertragungen auf der Seite des Access Points stören. Einerseits sollte die Reduzierung mit einem Puffer zu den üblichen RSSI-Werten der Clients auf Seiten des Access Points konfiguriert werden. Andererseits sind die Retries bzw. die WLAN-Quality-Indizes zu beachten. Wenn diese sich nach Erhöhung dieses Wertes deutlich verschlechtern, dann deutet dies auf einen zu hohen Wert hin.

Unterstützte Geräte:

- Nur WLAN-2 bei LN-630, L-822, LN-830x, LN-86x, L-1302, L-1310, LN-170x
- WLAN-1 und WLAN-2 bei O/IAP-8xx, OAP-170x
- Alle WLAN-Controller mit LCOS 10.30 RU1

6.2.1 Ergänzungen im Setup-Menü

Rx-Paket-Empf.-Reduktion

Durch die hier einstellbare Reduzierung der Empfangssempfindlichkeit kann ein Access Points künstlich „tauber" eingestellt werden. Hierdurch werden Übertragungen, die weiter entfernt sind, vom Access Point „überhört" und der Kanal wird somit öfter als „frei" erkannt. Es sind somit vereinfacht gesprochen mehr gleichzeitige Übertragungen auf dem gleichen Kanal möglich. Einserseits steigt dadurch der Gesamtdurchsatz eines Systems, aber auf der anderen Seite steigt auch die Interferenz auf Seiten der Clients.

Ein Client weiß nämlich nichts von der künstlichen Schwerhörigkeit. Er empfängt weiterhin die gewollten Signale seines Access Points sowie die Signale der anderen Access Points auf dem gleichen Kanal. Nur wenn der Signal-zu-Rauschabstand (SNR) weiterhin gut bleibt, werden die zusätzlichen Übertragungen dank dieses Features auch sauber vom Client empfangen. Ein weiterer Nebeneffekt des Unwissens der Clients ist, dass ein zu hoch eingestellter Wert den Effekt ins Gegenteil verkehren kann. Da der Access Point nicht zwischen Übertragungen von eigenen Clients und von anderen Geräten – sowohl Access Points als auch Clients – unterscheiden kann, wird nur das gehört, was über dem eingestellten Schwellenwert liegt – egal von wem es kommt. Es kann somit passieren, dass die Übertragung eines verbundenen Clients vom Access Point nicht mehr „gehört" wird. Hierdurch ensteht eine asymmetrische Verbindung, der Client wird den

Access Point möglicherweise noch gut empfangen und geht daher von einer guten Verbindung aus, während der Access Point vom Client nichts mehr mitbekommt und ihn somit ignoriert. Empfehlenswert ist, die Reduzierung so einzustellen, dass dadurch keine Benachteiligung von Clients entsteht.

Der Wertebereich von 0-20 entspricht dabei einer minimalen Empfangsstärke im Bereich von -95 dBm (0) bis -75 dBm (20). Prinzipiell treten bei den WLAN-Funkmodulen herstellungsbedingt Streuungen auf. Dadurch kann die reale Empfangsstärke geringfügig abweichen.

Dieses Feature ist für Experten! Wie in der Beschreibung bereits gesagt, kann es statt einem Mehrwert auch das Gegenteil bewirken und Übertragungen auf der Seite des Access Points stören. Einerseits sollte die Reduzierung mit einem Puffer zu den üblichen RSSI-Werten der Clients auf Seiten des Access Points konfiguriert werden. Andererseits sind die Retries bzw. die WLAN-Quality-Indizes zu beachten. Wenn diese sich nach Erhöhung dieses Wertes deutlich verschlechtern, dann deutet dies auf einen zu hohen Wert hin.

SNMP-ID:

2.23.20.8.35

Pfad Konsole:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

0 … 20

Modul-1-Rx-Paket-Empf.-Reduktion

Durch die hier einstellbare Reduzierung der Empfangssempfindlichkeit kann ein Access Points künstlich „tauber" eingestellt werden. Hierdurch werden Übertragungen, die weiter entfernt sind, vom Access Point „überhört" und der Kanal wird somit öfter als „frei" erkannt. Es sind somit vereinfacht gesprochen mehr gleichzeitige Übertragungen auf dem gleichen Kanal möglich. Einserseits steigt dadurch der Gesamtdurchsatz eines Systems, aber auf der anderen Seite steigt auch die Interferenz auf Seiten der Clients.

Ein Client weiß nämlich nichts von der künstlichen Schwerhörigkeit. Er empfängt weiterhin die gewollten Signale seines Access Points sowie die Signale der anderen Access Points auf dem gleichen Kanal. Nur wenn der Signal-zu-Rauschabstand (SNR) weiterhin gut bleibt, werden die zusätzlichen Übertragungen dank dieses Features auch sauber vom Client empfangen. Ein weiterer Nebeneffekt des Unwissens der Clients ist, dass ein zu hoch eingestellter Wert den Effekt ins Gegenteil verkehren kann. Da der Access Point nicht zwischen Übertragungen von eigenen Clients und von anderen Geräten – sowohl Access Points als auch Clients – unterscheiden kann, wird nur das gehört, was über dem eingestellten Schwellenwert liegt – egal von wem es kommt. Es kann somit passieren, dass die Übertragung eines verbundenen Clients vom Access Point nicht mehr „gehört" wird. Hierdurch ensteht eine asymmetrische Verbindung, der Client wird den Access Point möglicherweise noch gut empfangen und geht daher von einer guten Verbindung aus, während der Access Point vom Client nichts mehr mitbekommt und ihn somit ignoriert. Empfehlenswert ist, die Reduzierung so einzustellen, dass dadurch keine Benachteiligung von Clients entsteht.

Der Wertebereich von 0-20 entspricht dabei einer minimalen Empfangsstärke im Bereich von -95 dBm (0) bis -75 dBm (20). Prinzipiell treten bei den WLAN-Funkmodulen herstellungsbedingt Streuungen auf. Dadurch kann die reale Empfangsstärke geringfügig abweichen.

Dieses Feature ist für Experten! Wie in der Beschreibung bereits gesagt, kann es statt einem Mehrwert auch das Gegenteil bewirken und Übertragungen auf der Seite des Access Points stören. Einerseits sollte die Reduzierung mit einem Puffer zu den üblichen RSSI-Werten der Clients auf Seiten des Access Points konfiguriert werden. Andererseits sind die Retries bzw. die WLAN-Quality-Indizes zu beachten. Wenn diese sich nach Erhöhung dieses Wertes deutlich verschlechtern, dann deutet dies auf einen zu hohen Wert hin.

SNMP-ID:

2.37.1.4.37

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

0 … 20

Modul-2-Rx-Paket-Empf.-Reduktion

Durch die hier einstellbare Reduzierung der Empfangssempfindlichkeit kann ein Access Points künstlich „tauber" eingestellt werden. Hierdurch werden Übertragungen, die weiter entfernt sind, vom Access Point „überhört" und der Kanal wird somit öfter als „frei" erkannt. Es sind somit vereinfacht gesprochen mehr gleichzeitige Übertragungen auf dem gleichen Kanal möglich. Einserseits steigt dadurch der Gesamtdurchsatz eines Systems, aber auf der anderen Seite steigt auch die Interferenz auf Seiten der Clients.

Ein Client weiß nämlich nichts von der künstlichen Schwerhörigkeit. Er empfängt weiterhin die gewollten Signale seines Access Points sowie die Signale der anderen Access Points auf dem gleichen Kanal. Nur wenn der Signal-zu-Rauschabstand (SNR) weiterhin gut bleibt, werden die zusätzlichen Übertragungen dank dieses Features auch sauber vom Client empfangen. Ein weiterer Nebeneffekt des Unwissens der Clients ist, dass ein zu hoch eingestellter Wert den Effekt ins Gegenteil verkehren kann. Da der Access Point nicht zwischen Übertragungen von eigenen Clients und von anderen Geräten – sowohl Access Points als auch Clients – unterscheiden kann, wird nur das gehört, was über dem eingestellten Schwellenwert liegt – egal von wem es kommt. Es kann somit passieren, dass die Übertragung eines verbundenen Clients vom Access Point nicht mehr „gehört" wird. Hierdurch ensteht eine asymmetrische Verbindung, der Client wird den Access Point möglicherweise noch gut empfangen und geht daher von einer guten Verbindung aus, während der Access Point vom Client nichts mehr mitbekommt und ihn somit ignoriert. Empfehlenswert ist, die Reduzierung so einzustellen, dass dadurch keine Benachteiligung von Clients entsteht.

Der Wertebereich von 0-20 entspricht dabei einer minimalen Empfangsstärke im Bereich von -95 dBm (0) bis -75 dBm (20). Prinzipiell treten bei den WLAN-Funkmodulen herstellungsbedingt Streuungen auf. Dadurch kann die reale Empfangsstärke geringfügig abweichen.

Dieses Feature ist für Experten! Wie in der Beschreibung bereits gesagt, kann es statt einem Mehrwert auch das Gegenteil bewirken und Übertragungen auf der Seite des Access Points stören. Einerseits sollte die Reduzierung mit einem Puffer zu den üblichen RSSI-Werten der Clients auf Seiten des Access Points konfiguriert werden. Andererseits sind die Retries bzw. die WLAN-Quality-Indizes zu beachten. Wenn diese sich nach Erhöhung dieses Wertes deutlich verschlechtern, dann deutet dies auf einen zu hohen Wert hin.

SNMP-ID:

2.37.1.4.38

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

0 … 20

6.3 Separater Schalter zum Einschalten E-Mail-Benachrichtigung

Bisher wurden E-Mail-Benachrichtigungen immer dann gesendet, wenn eine E-Mail-Adresse in das entsprechende Feld der Konfiguration eingetragen wurde. Dieses implizite Verhalten wurde nun durch einen zusätzlichen Betriebsschalter, der das Senden der Benachrichtigungen steuert, abgelöst.

Sie finden den neuen Schalter unter **Wireless-LAN** > **Allgemein**. Über **E-Mails versenden** wird gesteuert, ob Benachrichtigungen an die in **E-Mail-Adr. für WLAN-Ereignisse** eingetragene Adresse versendet werden.

6.3.1 Ergänzungen im Setup-Menü

Mail-Adresse

An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet, wenn dies über den Schalter **Setup** > **WLAN** > **Send-Mails** eingeschaltet ist.

Zur Nutzung der E-Mail-Benachrichtigung muss ein SMTP-Konto eingerichtet sein.

SNMP-ID:

2.12.41

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

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

Default-Wert:

leer

Mails-senden

Bestimmt, ob an die in **Setup** > **WLAN** > **Mail-Adresse** angegebene E-Mail-Adresse Benachrichtigungen über WLAN-Ereignisse gesendet werden.

SNMP-ID:

2.12.141

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Nein
Ja

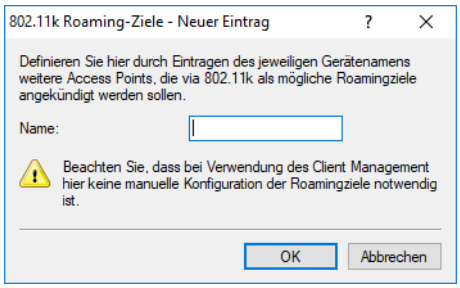
Default-Wert:

Nein

6.4 IEEE 802.11k-Roaming-Ziele

Der Standard IEEE 802.11k beschreibt einen Weg, WLAN-Clients über potentielle Roaming-Ziele, also weitere Access Points der selben SSID in Reichweite, zu informieren. Diese Information an den Client erfolgt durch den im Standard definierten „Neighbour Report". Bisher kommt 802.11k bereits im Rahmen des Client Managements zum Einsatz – hierzu ist keine gesonderte Konfiguration erforderlich. In Einzelfällen bzw. speziellen Szenarien kann es notwendig sein, auf das automatische Client Management zu verzichten und das Teilfeature 802.11k separat zu verwenden.

Sie finden die neue Tabelle unter **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **802.11k Roaming-Ziele**. Tragen Sie hier die potentiellen Roaming-Ziele ein.



6.4.1 Ergänzungen im Setup-Menü

Roaming-Ziele

Wenn Client Management aktiviert ist, dann wird die Tabelle in `/Status/WLAN/Roaming-Ziele` automatisch befüllt. Zusätzlich werden die manuell in dieser Tabelle hinzugefügten Ziele ebenfalls in die Liste der Nachbarn in einer 802.11k-Ankündigung aufgenommen, selbst wenn diese nicht in Reichweite sind. Die Anzahl der automatisch hinzugefügten Roaming-Ziele wird durch *2.12.87.11 Maximale-Anzahl-an-Nachbarn* beschränkt.

SNMP-ID:

2.12.132

Pfad Konsole:

Setup > **WLAN**

Name

Im Rahmen des Client Managements werden hier die Namen der Roaming-Ziele dieses Access Points nach einem Umgebungsscan eingetragen. Dies ist ein Bestandteil des Standards IEEE 802.11k. In diesem Standard wird ein Weg

beschrieben, WLAN-Clients über potentielle Roaming-Ziele, also weitere Access Points der selben SSID in Reichweite, zu informieren. Diese Information an den WLAN-Client erfolgt über den im Standard definierten „Neighbour Report".

Im Rahmen des Client Managements erfolgen diese Eintragungen automatisch. In Einzelfällen bzw. speziellen Szenarien kann es notwendig sein, auf das automatische Client Management zu verzichten und das Teilfeature 802.11k separat zu verwenden. Geben Sie dann hier die Gerätemamen der potentiellen Roaming-Ziele an, also andere Access Points der gleichen SSID.

Der Gerätename wird verwendet, um via IAPP die weiteren benötigten Informationen zum potentiellen Roaming-Ziel zu ermitteln (z. B. die Kanalnummer). Es ist daher erforderlich, dass die beteiligten Access Points via IAPP miteinander kommunizieren können.

Je nach Szenario kann es gewünscht sein, dass das jeweils zweite (eigene) WLAN-Modul eines Dual Radio Access Points ebenfalls als potentielles Roaming-Ziel kommuniziert wird. In diesem Fall kann der eigene Gerätename ebenfalls in die Tabelle eingetragen werden.

SNMP-ID:

2.12.132.1

Pfad Konsole:

Setup > **WLAN** > **Roaming-Ziele**

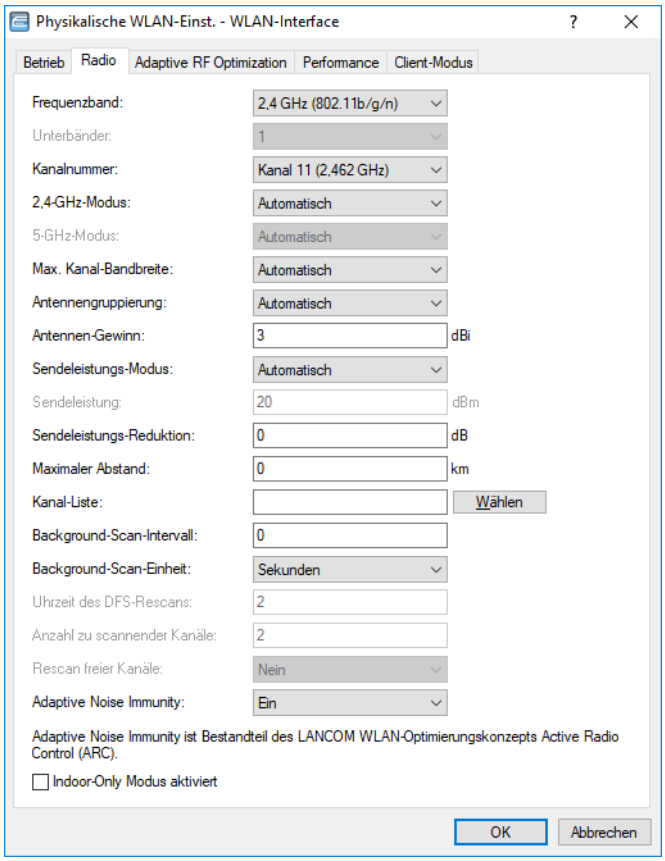
Mögliche Werte:

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

6.5 Ziel-EIRP einstellen

In Versionen vor LCOS 10.30 konnte die jeweils aktuelle WLAN-Sendeleistung um einen festen, konfigurierten Wert reduziert werden. Auf diese Weise konnte die WLAN-Zellgröße an die Anforderungen eines Szenarios angepasst werden. Dieses Verfahren stößt an seine Grenzen, wenn durch eine professionelle WLAN-Ausleuchtung eine maximal zu erreichende Sendeleistung festgelegt wurde und gleichzeitig auch ein automatischer Wechsel zwischen Kanälen der verschiedenen 5 GHz-Unterbändern gewünscht ist. So ist z. B. im 5 GHz-Unterband 2 eine höhere Sendeleistung erlaubt als im Unterband 1. Die fest eingestellte Sendeleistungsreduktion würde nun einfach die höhere Sendeleistung im Unterband 2 um genau den selben Wert reduzieren, wie die geringere erlaubte Sendeleistung im Unterband 1. Man erhält als Resultat unterschiedliche Zellgrößen, abhängig vom gewählten Unterband. Ab LCOS 10.30 kann die maximal zu erreichende Sendeleistung als absoluter Wert eingestellt werden, so dass unabhängig von der erlaubten maximalen Sendeleistung immer die gleiche Zellgröße erzielt wird.

Die Konfiguration erfolgt in LANconfig unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Radio** über die Einstellungen in den Feldern **Sendeleistungs-Modus** und **Sendeleistung**.



Der Modus **Automatisch** bezeichnet das bisherige Verhalten, während über **Manuell** im Feld **Sendeleistung** ein absoluter Wert in dBm angegeben werden kann.

In keinem Fall wird der Access Point die vom Gesetzgeber vorgegebenen Grenzen für die Sendeleistung überschreiten. Diese werden automatisch immer beachtet, unabhängig von der hier vorgenommenen Konfiguration.

6.5.1 Ergänzungen im Setup-Menü

Leistungs-Einstellung

In Versionen vor LCOS 10.30 konnte die jeweils aktuelle WLAN-Sendeleistung um einen festen, konfigurierten Wert reduziert werden. Auf diese Weise konnte die WLAN-Zellgröße an die Anforderungen eines Szenarios angepasst werden. Dieses Verfahren stößt an seine Grenzen, wenn durch eine professionelle WLAN-Ausleuchtung eine maximal zu erreichende Sendeleistung festgelegt wurde und gleichzeitig auch ein automatischer Wechsel zwischen Kanälen der verschiedenen 5 GHz-Unterbändern gewünscht ist. So ist z. B. im 5 GHz-Unterband 2 eine höhere Sendeleistung erlaubt als im Unterband 1. Die fest eingestellte Sendeleistungsreduktion würde nun einfach die höhere Sendeleistung im Unterband 2 um genau den selben Wert reduzieren, wie die geringere erlaubte Sendeleistung im Unterband 1. Man erhält als Resultat unterschiedliche Zellgrößen, abhängig vom gewählten Unterband. Ab LCOS 10.30 kann die maximal zu erreichende Sendeleistung als absoluter Wert eingestellt werden, so dass unabhängig von der erlaubten maximalen Sendeleistung immer die gleiche Zellgröße erzielt wird.

In keinem Fall wird der Access Point die vom Gesetzgeber vorgegebenen Grenzen für die Sendeleistung überschreiten. Diese werden automatisch immer beachtet, unabhängig von der hier vorgenommenen Konfiguration.

SNMP-ID:

2.23.20.8.33

Pfad Konsole:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

Automatisch

Die maximal erlaubte und von der Hardware des Access Point realisierbare Sendeleistung wird verwendet.

Manuell

Die gewünschte Sendeleistung ist im Feld EIRP in dBm einzustellen.

Ist die Hardware des Access Points nicht in der Lage, die gewünschte Sendeleistung einzustellen, wird automatisch der maximal mögliche Wert eingestellt. Der tatsächlich eingestellte Wert kann im LANmonitor oder auf der CLI mittels des Befehls `show wlan` überprüft werden.

Default-Wert:

Automatisch

EIRP

Falls die Einstellung der WLAN-Sendeleistung in **Setup** > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **Leistungs-Einstellung** auf Manuell eingestellt ist, dann wird der hier eingestellte Wert in dBm genommen.

SNMP-ID:

2.23.20.8.34

Pfad Konsole:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]-`

7 WLAN-Management

7.1 WLC-Funktionen im LANCOM vRouter

Ab LCOS 10.30 unterstützt der LANCOM vRouter zusätzlich die Funktionen eines WLAN-Controllers. Entscheiden Sie selbst und flexibel, welche Rolle Ihr LANCOM vRouter übernehmen soll: VPN-Gateway oder WLAN-Controller. Der LANCOM vRouter unterstützt ab sofort die Rolle eines virtuellen WLCs (vWLC) und kann somit Access Points verwalten. Damit können die WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi oder Microsoft Hyper-V virtualisiert werden. Die Anzahl der verwalteten Access Points ist abhängig von der Lizenzkategorie des vRouters. Alle vRouter-Lizenzen, die ab dem Release von LCOS 10.30 ausgestellt wurden, enthalten eine vWLC-Option.

Produkt	VPN-Lizenzen	AP-Lizenzen
vRouter 50	10	10
vRouter 250	50	50
vRouter 500	100	100
vRouter 1000	200	200
vRouter unlimited	1000	1000

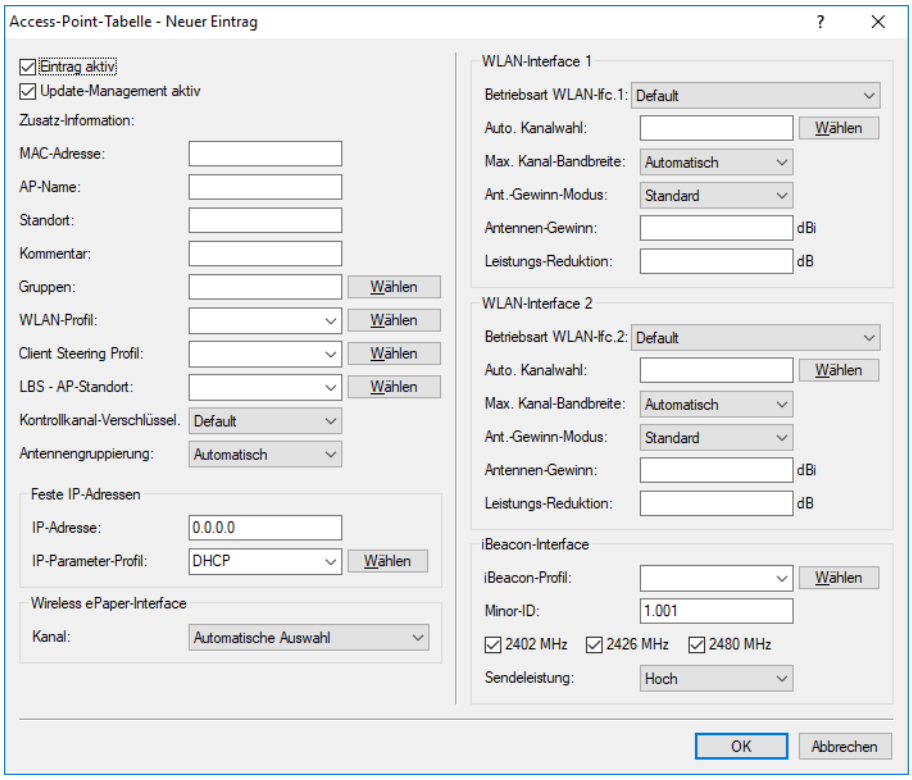
LANCOM Systems GmbH empfiehlt den Betrieb einer vRouter-Instanz entweder hauptsächlich als VPN-Gateway / Router oder als WLAN-Controller. Die empfohlene Nutzung kann auch anteilig erfolgen; zum Beispiel bei der Lizenzstufe „vRouter 1000“ (200 VPN-Lizenzen und 200 AP-Lizenzen):

- 100 gleichzeitige VPN-Verbindungen und 100 verwaltete APs oder
- 150 gleichzeitige VPN-Verbindungen und 50 verwaltete APs.

7.2 Neuer Modus für den Antennengewinn

Bei der Inbetriebnahme von Access Points an einem WLAN-Controller wurden diese bisher immer mit einem Antennengewinn von 3 dBi je Modul eingerichtet, da dieser Wert für die meisten Indoor-Access Points mit Standardantennen passend ist. Insbesondere für Outdoor-Access Points mit integrierten Antennen musste der Wert aber in der Vergangenheit manuell angepasst werden, die hier häufig interne Antennen mit einem hohen Antennengewinn zum Einsatz kommen. Ab LCOS 10.30 wird der Standard-Antennengewinn eines verwalteten Access Points an den WLAN-Controller übertragen und dort automatisch verwendet. Für diese Funktion müssen sowohl der Access Point als auch der WLAN-Controller, mindestens den Firmware-Stand 10.30 aufweisen. Mit dieser Einstellung für den Modus des Antennengewinns wird verhindert, dass man nach einem Rollout einige Access Points noch manuell korrigieren muss.

Die Konfiguration erfolgt in LANconfig unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** über die Einstellungen in den Feldern **Ant.-Gewinn-Modus** bei den WLAN-Interfaces.



Ant.-Gewinn-Modus

Mögliche Werte:

Standard

Der im Access Point voreingestellte Wert für den Antennengewinn wird verwendet.

Benutzerdefiniert

Der im Feld **Antennen-Gewinn** eingestellte Wert wird verwendet.

7.2.1 Ergänzungen im Setup-Menü

Module-1-Ant-Gewinn-Modus

Bei der Inbetriebnahme von Access Points an einem WLAN-Controller wurden diese bisher immer mit einem Antennengewinn von 3 dBi je Modul eingerichtet, da dieser Wert für die meisten Indoor-Access Points mit Standardantennen passend ist. Insbesondere für Outdoor-Access Points mit integrierten Antennen musste der Wert aber in der Vergangenheit manuell angepasst werden, die hier häufig interne Antennen mit einem hohen Antennengewinn zum Einsatz kommen. Ab LCOS 10.30 wird der Standard-Antennengewinn eines verwalteten Access Points an den WLAN-Controller übertragen und dort automatisch verwendet. Für diese Funktion müssen sowohl der Access Point als auch der WLAN-Controller, mindestens den Firmware-Stand 10.30 aufweisen. Mit dieser Einstellung für den Modus des Antennengewinns wird verhindert, dass man nach einem Rollout einige Access Points noch manuell korrigieren muss.

SNMP-ID:

2.37.1.4.35

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

Standard

Der im Access Point voreingestellte Wert für den Antennengewinn wird verwendet.

benutzerdefiniert

Der Wert aus **Module-1-Ant-Gewinn** wird verwendet.

Default-Wert:

Standard

Module-2-Ant-Gewinn-Modus

Bei der Inbetriebnahme von Access Points an einem WLAN-Controller wurden diese bisher immer mit einem Antennengewinn von 3 dBi je Modul eingerichtet, da dieser Wert für die meisten Indoor-Access Points mit Standardantennen passend ist. Insbesondere für Outdoor-Access Points mit integrierten Antennen musste der Wert aber in der Vergangenheit manuell angepasst werden, die hier häufig interne Antennen mit einem hohen Antennengewinn zum Einsatz kommen. Ab LCOS 10.30 wird der Standard-Antennengewinn eines verwalteten Access Points an den WLAN-Controller übertragen und dort automatisch verwendet. Für diese Funktion müssen sowohl der Access Point als auch der WLAN-Controller, mindestens den Firmware-Stand 10.30 aufweisen. Mit dieser Einstellung für den Modus des Antennengewinns wird verhindert, dass man nach einem Rollout einige Access Points noch manuell korrigieren muss.

SNMP-ID:

2.37.1.4.36

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

Standard

Der im Access Point voreingestellte Wert für den Antennengewinn wird verwendet.

benutzerdefiniert

Der Wert aus **Module-2-Ant-Gewinn** wird verwendet.

Default-Wert:

Standard

8 Virtual Private Networks – VPN

8.1 IKEv2

8.1.1 Elliptic Curve Digital Signature Algorithm (ECDSA)

Ab LCOS 10.30 unterstützt IKEv2 neben den Authentifizierungsverfahren RSA-Signature und Digital-Signature auch Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754.

ECDSA-Signaturen sind grundsätzlich kleiner als RSA-Signaturen bei vergleichbarer kryptografischer Stärke. ECDSA-Schlüssel und Zertifikate sind in Bezug auf Dateigröße ebenso deutlich kleiner als RSA-basierte Schlüssel und Zertifikate. Des Weiteren sind ECDSA-Operationen auf vielen Geräten grundsätzlich schneller in der Berechnung. Die folgenden Verfahren werden bei IKEv2 unterstützt:

- ECDSA with SHA-256 on the P-256 curve
- ECDSA with SHA-384 on the P-384 curve
- ECDSA with SHA-512 on the P-521 curve

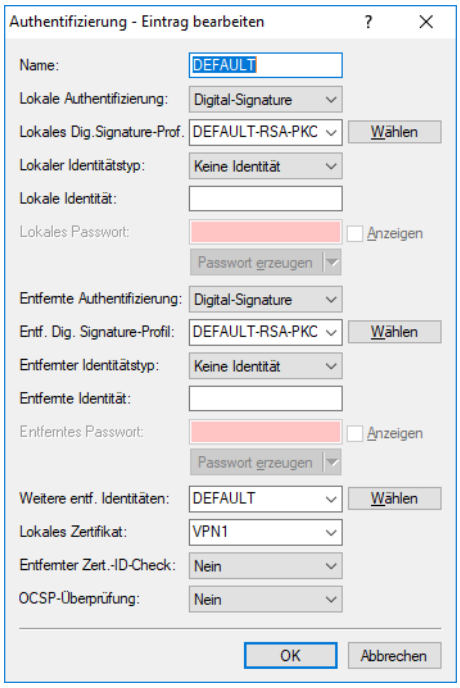
Bei Verwendung von OpenSSL zur Erzeugung von Zertifikaten müssen die folgenden vordefinierten Kurven als Parameter für ECDSA bei IKEv2 verwendet werden:

- prime256v1 bei ECDSA-256
- secp384r1bei ECDSA-384
- secp521r1 bei ECDSA-512

Folgende Einschränkungen gelten bei der Verwendung von ECDSA:

- Die Verhandlung von ECDSA innerhalb des Digital Signature Verfahrens wird nicht unterstützt.
- ECDSA-basierte Zertifikate können derzeit nicht von der LCOS-eigenen CA erzeugt werden. Ebenso ist der automatische Zertifikatsbezug per SCEP nicht möglich. ECDSA-Zertifikate müssen mit einer externen Anwendung, wie z. B. OpenSSL oder mit Hilfe von XCA erzeugt werden und anschließend ins Gerät geladen werden.

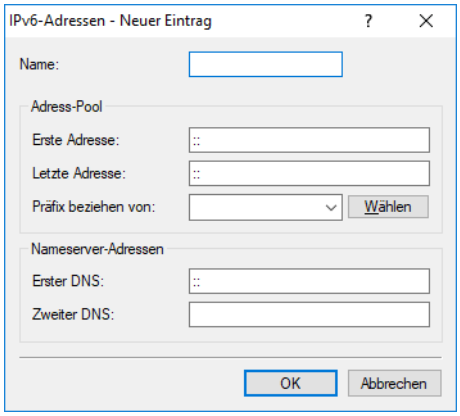
In LANconfig unter **VPN** > **IKEv2 / IPSec** > **Authentifizierung** können Sie diese Verfahren nun sowohl für die **Lokale Authentifizierung** als auch die **Entfernte Authentifizierung** auswählen.



8.1.2 IKEv2-Configuration-Payload mit Angabe einer Quelle für Präfix-Delegation

Ab LCOS 10.30 unterstützt IKEv2-Configuration-Payload die Angabe einer Quelle für Präfix-Delegation.

In LANconfig erfolgt die Konfiguration unter **VPN** > **IKEv2 / IPSec** > **IPv6-Adressen**.



Adress-Pool

Präfix beziehen von

Mit diesem Parameter können Sie den VPN-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix „2001:db8::/64" zugewiesen, dann können Sie beim Parameter **Erste Adresse** den Wert „::1" und bei **Letzte Adresse** den Wert „::9" eingeben. Zusammen mit dem vom Provider delegierten Präfix „2001:db8::/64" erhalten Clients dann Adressen aus dem Pool von „2001:db8::1" bis „2001:db8::9". Ist das Provider-Präfix größer als „/64", z. B. „/48" oder „/56", so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen.

Beispiel:

- Zugewiesenes Provider-Präfix: 2001:db8:abcd:aa::/56
- /64 als Präfix des logischen Netzwerks (Subnetzt-ID 1): 2001:db8:abcd:aa01::/64
- Erste Adresse: 0:0:0:0001::1
- Letzte Adresse: 0:0:0:0001::9

Derzeit wird kein Neighbor Discovery Proxy für IPv6 unterstützt. Deshalb darf der Adressbereich des Pools nicht mit Adressbereichen bzw. Präfixen überlappen, die bereits für andere Netze auf dem Router verwendet werden.

8.1.3 Split-DNS

Beim VPN Split Tunneling werden nur Anwendungen durch den VPN-Tunnel gesendet, welche bestimmte Endpunkte hinter dem VPN-Tunnel erreichen sollen. Der gesamte andere Datenverkehr wird am VPN-Tunnel vorbei direkt ins Internet gesendet. Die Definition, welche IP-Netze durch den Tunnel erreichbar sein sollen, lassen sich durch VPN-Regeln definieren.

Split-DNS ermöglicht die DNS-Auflösung bestimmter interner Domänen, z. B. „*.firma.de“ über den VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird. Hierbei weist der IKE-Config-Mode-Server dem Client eine oder mehrere Split-DNS-Domänen dynamisch über das Attribut INTERNAL_DNS_DOMAIN beim Verbindungsaufbau zu. Die empfangene Domain-Liste trägt der Client in seine lokale DNS-Weiterleitungsliste ein. Der Client muss dieses Attribut unterstützen.

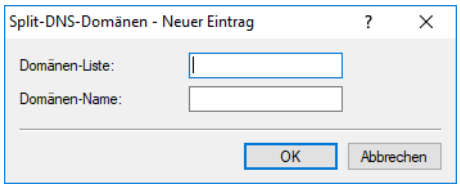
Split-DNS für IKEv2 wird von LANCOM VPN-Routern in der Rolle IKE-Config-Mode Client und Server unterstützt. Bei Site-to-Site-VPN-Verbindungen wird die dynamische Split-DNS-Zuweisung im IKE-Protokoll nicht unterstützt und muss über statische DNS-Weiterleitungen auf den entsprechenden VPN-Endpunkten konfiguriert werden.

Die Split-DNS-Konfiguration wird in der IKEv2-Verbindungsliste als Split-DNS-Profil in der CFG-Mode-Betriebsart „Server“ zugewiesen.

In LANconfig definieren Sie zuerst die gewünschten Domänen unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Domänen**, dann weisen Sie diese unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Profile** einem Profil zu, welches Sie in der **Verbindungsliste** im IKE Config-Mode verwenden können, falls dort **IKE-CFG** auf **Server** eingestellt wird.

Split-DNS-Domänen

In LANconfig erfolgt die Konfiguration der Split-DNS-Domänen unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Domänen**.



Domänen-Liste

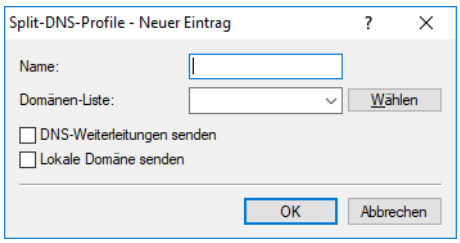
Vergeben Sie einen Namen für die Domänen-Liste.

Domänen-Name

Split-DNS-Domänen-Name, den das VPN-Gateway an VPN-Clients senden soll, z. B. „firma.intern“. Mehrere Domänen-Namen können durch mehrere Einträge mit dem gleichen Bezeichner der Domänen-Liste konfiguriert werden.

Split-DNS-Profile

In LANconfig erfolgt die Konfiguration der Split-DNS-Profile unter **VPN** > **IKEv2 / IPSec** > **Split-DNS-Profile**.



Name

Vergeben Sie einen Namen für dieses Profil.

Domänen-List

Name der Liste mit Split-DNS-Domänen, die das VPN-Gateway an VPN-Clients senden soll.

DNS-Weiterleitungen senden

Stellen Sie ein, ob das VPN-Gateway seine lokal konfigurierten DNS-Weiterleitungen an VPN-Clients senden soll.

Lokale Domäne senden

Stellen Sie ein, ob das VPN-Gateway seine eigene lokal konfigurierte Domäne an VPN-Clients senden soll.

8.1.4 IKEv2-Fragmentierung

Ab LCOS 10.30 wird die IKEv2-Fragmentierung nach RFC 7383 unterstützt. Dies ermöglicht die effiziente Fragmentierung von IKEv2-Nachrichten vom VPN-Router selbst, sodass IKE-Pakete vom Transportnetz nicht mehr fragmentiert werden müssen. Grundsätzlich werden zwei Verfahren der IKEv2-Fragmentierung unterstützt:

- Herstellerspezifische Fragmentierung, kompatibel zu Drittherstellern
- Fragmentierung nach RFC 7383

Das Gerät wählt automatisch das beste Verfahren. Unterstützt eine VPN-Gegenseite beide Verfahren, so wird die Fragmentierung nach RFC 7383 bevorzugt.

8.1.5 Regeln für IKEv2-Passwörter

Ab LCOS 10.32 wird die Durchsetzung von Passwortregeln für Pre-Shared Keys (PSK) unterstützt. Navigieren Sie zu den Einstellungen von **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und setzen Sie die Option **Preshared Key-Regeln erzwingen**. Die folgenden Regeln gelten dann für Pre-Shared Keys (PSK) mit IKEv2:

- Die Länge des Passworts muss mindestens 32 Zeichen betragen.
- Das Passwort muss mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten.

Diese Regeln gelten nicht für PSK, die von einem RADIUS-Server verwaltet und bezogen werden.

8.1.6 Ergänzungen im Setup-Menü

Split-DNS-Profil

Name des Split-DNS-Profils. Das Split-DNS-Profil ist nur aktiv, falls **IKE-CFG** den Wert **Server** hat.

SNMP-ID:

2.19.36.1.22

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Local-Auth

Legt die Authentifizierungsmethode für die lokale Identität fest.

SNMP-ID:

2.19.36.3.1.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-256 auf der P-256-Kurve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-384 auf der P-384-Kurve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-512 auf der P-521-Kurve.

Default-Wert:

PSK

Remote-Auth

Legt die Authentifizierungsmethode für die entfernte Identität fest.

SNMP-ID:

2.19.36.3.1.6

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-256 auf der P-256-Kurve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-384 auf der P-384-Kurve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-512 auf der P-521-Kurve.

Default-Wert:

PSK

Remote-Auth

Legt die Authentifizierungsmethode für die entfernte Identität fest.

SNMP-ID:

2.19.36.3.3.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-256 auf der P-256-Kurve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-384 auf der P-384-Kurve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) nach RFC 4754 mit SHA-512 auf der P-521-Kurve.

Default-Wert:

PSK

PD-Quelle

Mit diesem Parameter können Sie den VPN-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix „2001:db8::/64" zugewiesen, dann können Sie beim Parameter „Erste Adresse" den Wert „::1" und bei „Letzte Adresse" den Wert „::9" eingeben. Zusammen mit dem vom Provider delegierten Präfix „2001:db8::/64" erhalten Clients dann Adressen aus dem Pool von „2001:db8::1" bis „2001:db8::9". Ist das Provider-Präfix größer als „/64", z. B. „/48" oder „/56", so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen.

Beispiel:

- Zugewiesenes Provider-Präfix: 2001:db8:abcd:aa::/56
- /64 als Präfix des logischen Netzwerks (Subnetz-ID 1): 2001:db8:abcd:aa01::/64
- Erste Adresse: 0:0:0:0001::1
- Letzte Adresse: 0:0:0:0001::9

SNMP-ID:

2.19.36.7.2.6

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Mögliche Werte:

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

Default-Wert:

leer

Split-DNS

Beim VPN Split Tunneling werden nur Anwendungen durch den VPN-Tunnel gesendet, welche bestimmte Endpunkte hinter dem VPN-Tunnel erreichen sollen. Der gesamte andere Datenverkehr wird am VPN-Tunnel vorbei direkt ins Internet gesendet. Die Definition, welche IP-Netze durch den Tunnel erreichbar sein sollen, lassen sich durch VPN-Regeln definieren.

Split-DNS ermöglicht die DNS-Auflösung von bestimmten internen Domänen, z. B. „*.firma.de" über den VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird. Hierbei weist der IKE-Config-Mode-Server dem Client eine oder mehrere Split-DNS-Domänen dynamisch über das Attribut INTERNAL_DNS_DOMAIN beim Verbindungsaufbau zu. Die empfangene Domain-Liste trägt der Client in seine lokale DNS-Weiterleitungsliste ein. Der Client muss dieses Attribut unterstützen.

Split-DNS für IKEv2 wird von LANCOM VPN-Routern in der Rolle IKE-Config-Mode Client und Server unterstützt. Bei Site-to-Site VPN-Verbindungen wird die dynamische Split-DNS-Zuweisung im IKE-Protokoll nicht unterstützt und muss über statische DNS-Weiterleitungen auf den entsprechenden VPN-Endpunkten konfiguriert werden.

SNMP-ID:

2.19.36.7.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Domain-Listen

Definieren Sie hier die Domänen-Listen für Split-DNS.

SNMP-ID:

2.19.36.7.3.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

Domainname

Split-DNS-Domänen-Name, den das VPN-Gateway an VPN-Clients senden soll, z. B. „firma.intern“. Mehrere Domänen-Namen können durch mehrere Einträge mit dem gleichen Bezeichner der Domänen-Liste konfiguriert werden.

SNMP-ID:

2.19.36.7.3.1.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Listen**

Mögliche Werte:

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

Default-Wert:

leer

Domain-Liste

Vergeben Sie einen Namen für die Domänen-Liste.

SNMP-ID:

2.19.36.7.3.1.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Listen**

Mögliche Werte:

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

Default-Wert:

leer

Profile

Definieren Sie hier die Profile für Split-DNS.

SNMP-ID:

2.19.36.7.3.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

Name

Vergeben Sie einen Namen für dieses Profil.

SNMP-ID:

2.19.36.7.3.4.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

Sende-DNS-Forwardings

Stellen Sie ein, ob das VPN-Gateway seine lokal konfigurierten DNS-Weiterleitungen an VPN-Clients senden soll.

SNMP-ID:

2.19.36.7.3.4.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profile**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Sende-lokale-Domain

Stellen Sie ein, ob das VPN-Gateway seine eigene lokal konfigurierte Domäne an VPN-Clients senden soll.

SNMP-ID:

2.19.36.7.3.4.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profile**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Domain-Liste

Name der Liste mit Split-DNS-Domänen, die das VPN-Gateway an VPN-Clients senden soll.

SNMP-ID:

2.19.36.7.3.4.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

Cookie-Challenge

IKEv2 bietet mit der Cookie Notification ein Challenge-Response-Verfahren, welches der IKEv2-Responder anstoßen kann, wenn auf diesem zu viele halboffene IKEv2-Verbindungen vorhanden sind. Dies dient dazu, DDoS-Angriffe auf den Responder zu erschweren.

Die Cookie Notification wurde zur Verbesserung der Kompatibilität mit VPN-fähigen Geräten anderer Hersteller implementiert und muss immer bei beiden VPN-Teilnehmern aktiviert sein, damit eine VPN-Verbindung zustande kommt.

Die IKEv2 Cookie Notification verhindert den massiven Aufbau von halboffenen VPN-Verbindungen und den damit verbundenen Angriff auf Ressourcen des VPN-Gateways (DDOS). Mit aktivierter Cookie Notification reagiert dieser auf eingehende VPN-Verbindungen erst, wenn die Gegenseite nach Überprüfung erreicht werden kann.

Das Aktivieren der IKEv2 Cookie Challenge verlängert den VPN-Verbindungsaufbau um zwei zusätzliche IKE-Nachrichten.

Der Schalter aktiviert die Cookie Challenge auf der Responder bzw. Gateway-Seite.

Auf der Initiator-Seite wird die Cookie Challenge automatisch gemacht, falls die Gegenseite dies anfordert. Der Schalter hat auf der Initiator-Seite bzw. Client-Seite keine Wirkung.

Bitte beachten Sie, dass sowohl Initiator als auch Responder das Feature Cookie Challenge unterstützen müssen. Unterstützt die aufbauende Gegenseite keine Cookie Challenge, so kann der VPN-Tunnel nicht aufgebaut werden. LANCOM VPN-Router müssen auf beiden Seiten mindestens LCOS 10.30 besitzen.

SNMP-ID:

2.19.36.12

Pfad Konsole:

Setup > **VPN** > **IKEv2**

Mögliche Werte:

aus
immer

Default-Wert:

aus

Pre-Shared-Key-Regeln-erzwingen

Mit diesem Eintrag haben Sie die Möglichkeit, das Erzwingen von Passwort-Regeln zu aktivieren oder zu deaktivieren. Es gelten dann die folgenden Regeln für die Pre-Shared Keys (PSK) bei IKEv2:

- Die Länge des Passworts muss mindestens 32 Zeichen betragen.
- Das Passwort muss mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten.

Diese Regeln gelten nicht für PSK, die von einem RADIUS-Server verwaltet und bezogen werden.

SNMP-ID:

2.19.36.14

Pfad Konsole:

Setup > **VPN** > **IKEv2**

Mögliche Werte:

Nein

Das Erzwingen von Passwort-Regeln ist deaktiviert.

Ja

Das Erzwingen von Passwort-Regeln ist aktiviert.

Default-Wert:

Nein

RSA-Padding-Methode

Definiert die RSA-Padding-Methode für ausgestellte Zertifikate der SCEP-CA.

SNMP-ID:

2.39.2.15

Pfad Konsole:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

PKCS1

Das Padding der Zertifikate wird mit dem Verfahren RSASSA-PKCS1-v1_5 durchgeführt.

PSS

Das Padding der Zertifikate wird mit dem Verfahren RSASSA-PSS durchgeführt

Default-Wert:

PKCS1

9 Public Spot

9.1 Doppelte Anzahl an Public Spot-Usern

Ab LCOS 10.30 können folgende Router der 178x- und 179x-Serie 128 statt 64 gleichzeitig angelegte Public Spot-Benutzer verwalten:

- LANCOM 179x-Serie
- LANCOM 1781Vx-Serie
- LANCOM 1781EF+
- LANCOM 1781EW+
- LANCOM 1783-Serie
- LANCOM 88x-Serie

10 IoT – Das Internet der Dinge (Internet of Things – IoT)

Um die Konfiguration der vom LCOS unterstützten IoT-Technologien zu konsolidieren, werden diese unter dem neuen Menüpunkt „IoT" zusammengefasst. Diese Änderung wird nicht nur in LANconfig, sondern auch im LCOS-Menü vollzogen. Daher ändern sich die entsprechenden Pfade für die Funktionen Wireless ePaper, iBeacon und Bluetooth Low Energy nach:

- **Setup** > **IoT** > **Wireless-ePaper**
- **Status** > **IoT** > **Wireless-ePaper**
- **Setup** > **IoT** > **Bluetooth** > **iBeacon** (nur Geräte der E-Serie)
- **Status** > **IoT** > **Bluetooth** > **iBeacon** (nur Geräte der E-Serie)
- **Setup** > **IoT** > **Bluetooth** (nur Geräte der B-Serie)
- **Status** > **IoT** > **Bluetooth** (nur Geräte der B-Serie)

Bestandsgeräte sind von dieser Umstellung auf der Kommandozeile nicht betroffen, um bestehende Konfigurationssicherungen weiter verwenden zu können, die noch die alte Menüstruktur beinhalten. Dies betrifft

- L-151E
- L-322E
- LN-830E

In LANconfig wird die neue Struktur für **alle** Geräte verwendet, da die Darstellung hier unabhängig von der Menüstruktur der Kommandozeile ist.

Beim IoT werden physische und virtuelle Gegenstände miteinander vernetzt und entstehende Daten und Informationen ausgetauscht. Sensoren, smarte Hausgeräte, digitale Raumbeschilderung oder auch elektronische Preisschilder im Einzelhandel sind typische Beispiele. Die Vernetzung von IoT-Geräten geschieht meist über Funk, zum Einsatz kommen die unterschiedlichsten Funktechnologien wie modifizierte ZigBee-Varianten (Retail IoT), Bluetooth Low Energy (BLE) oder diverse Mobilfunk-Ableger. Einen einheitlichen „IoT-Funkstandard" gibt es nicht, zudem tauchen in kurzen Zyklen neue IoT-Funktechnologien auf.

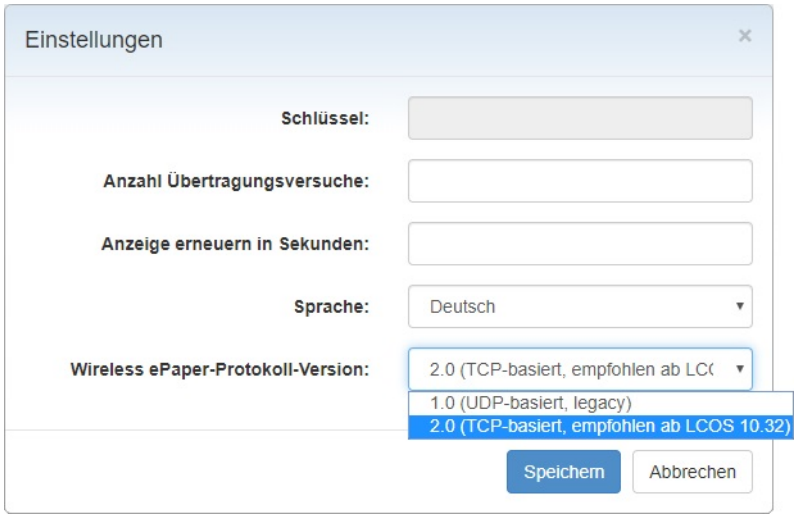
Die speziellen Einstellungen für IoT erfolgen in LANconfig unter **IoT**.

10.1 Wireless ePaper

Zentrale Verwaltung Ihrer Wireless ePaper-Infrastruktur

Ab LCOS 10.32 unterstützen die LANCOM Access Points mit Wireless ePaper-Unterstützung ein neues Protokoll, welches eine effizientere und zuverlässigere Kommunikation zwischen Wireless ePaper Server und Access Point gewährleistet. Dank der Unterstützung dieses neuen Protokolls können Sie Ihre LANCOM Wireless ePaper Displays nun auch remote über den Wireless ePaper Server in der Zentrale managen und über VPN ansteuern. Wenn beide Seiten das neue Protokoll unterstützen und es im Wireless ePaper Server aktiviert wurde, wird das neue Protokoll verwendet.

In der rechten, oberen Ecke der Wireless ePaper-Verwaltung können Sie auf das Zahnrad-Symbol und dann **Einstellungen** klicken, um allgemeine Einstellungsmöglichkeiten zum Wireless ePaper Server zu erreichen. Dort können Sie das neue Protokoll aktivieren.



Im LANmonitor in der Anzeige des entsprechenden Gerätes unter **IoT** > **Wireless ePaper** > **Protokollversion** wird das verwendete Protokoll angezeigt:

- Keine – Es besteht keine Verbindung zu einem Controller / Server
- ThinAP1.0/UDP – Protokollversion 1.0 (UDP-basiert, legacy)
- ThinAP2.0/TCP – Protokollversion 2.0 (TCP-basiert, empfohlen ab LCOS 10.32)

Der Wireless ePaper Server unterstützt „Protokollversion 2.0“ ab Version 1.91. Falls Sie diesen bereits einsetzen und trotzdem hier nur „Protokollversion 1.0“ sehen, dann wurde ggf. das Protokoll in den Einstellungen des Wireless ePaper Servers nicht aktiviert. Gehen Sie dann wie folgt vor, wobei die Aktivierung der neuen Protokollversion hier alternativ über die Kommandozeile gezeigt wird:

1. Überprüfen Sie die folgenden Voraussetzungen:
   - LANCOM Wireless ePaper Server in der Version 1.91 oder höher ist installiert
   - cURL ist installiert
2. Öffnen Sie in Ihrem Betriebsystem eine Kommandozeile und geben Sie den folgenden Befehl ein:

   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=true
   ```
3. Starten Sie den Wireless ePaper Server neu.
4. Geben Sie anschließend den folgenden Befehl ein, um zu überprüfen, ob die Aktivierung erfolgreich war:

   ```
   curl -X GET http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode
   ```

Eine erfolgreiche Aktivierung liefert die Ausgabe:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Configuration key="lancomUseTcpThinMode" type="BOOLEAN" defaultValue="false" value="true"/>
```

Der Befehl

```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=false
```

deaktiviert die Funktion des TCP-basierten Wireless ePaper Protokolls.

10.1.1 Installation und Konfiguration eines Wireless ePaper USB

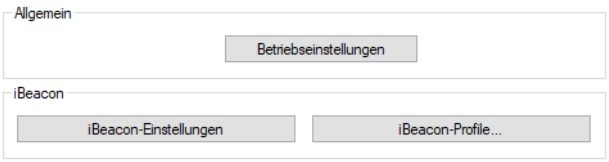
Ab LCOS 10.32 kann für LANCOM Geräte mit USB-Port, aber ohne direkte ePaper-Unterstützung über den LANCOM Wireless ePaper USB die ePaper-Unterstützung nachgerüstet werden. Mehr Informationen hierzu finden Sie im Benutzerhandbuch LANCOM Wireless ePaper Server.

10.2 BLE-Scanner und -Beacon

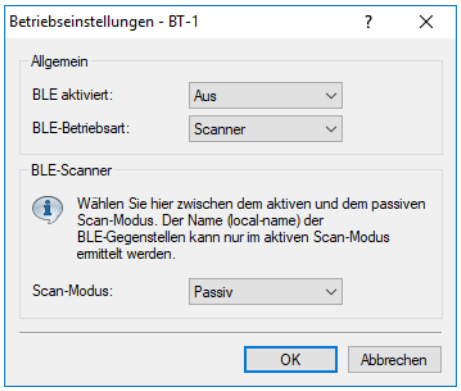
WLAN-Geräte der B-Serie verfügen über Bluetooth Low Energy-Unterstützung (BLE) für folgende Technologien: Aussenden von Beacons wie z. B. iBeacon sowie das Scannen der BLE-Umgebung, wodurch zusammen mit einem geeigneten Auswertungssystem Anwendungsfälle wie Asset Tracking oder Besucherzählung ermöglicht werden.

10.2.1 Einstellungen für BLE

Die Einstellungen für Bluetooth LE erfolgen in LANconfig unter **IoT** > **Bluetooth LE**.



Betriebseinstellungen



BLE aktiviert

Aktivieren Sie hier das BLE-Modul.

BLE-Betriebsart

Dieser Eintrag bietet Ihnen die Möglichkeit, die Betriebsart des BLE-Moduls einzustellen. Wählen Sie, ob die Bluetooth-Schnittstelle zum Aussenden von Beacons, oder zum Scannen der Umgebung verwendet werden soll.

Ein gleichzeitiger Betrieb der beiden Betriebsarten ist nicht möglich.

Scanner

Das BLE-Modul wird für den Umgebungsscan verwendet.

BLE-Beacon

Das BLE-Modul sendet Beacons aus.

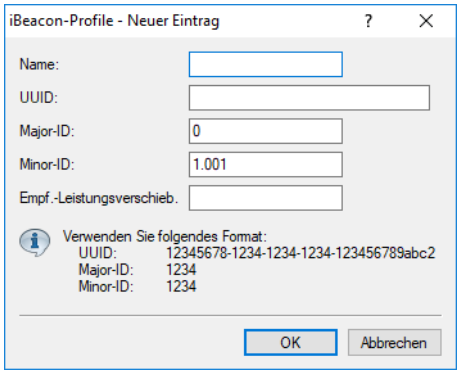
Scan-Modus

Wählen Sie hier, ob aktiv oder passiv gescannt werden soll. Beim aktiven Scan werden aktiv Scan Requests gesendet, welche die BLE-Clients in der Umgebung beantworten. Dies ist z. B. notwendig, um Namen der Clients zu ermitteln.

Beachten Sie, dass sich das ständige Beantworten der Scan Requests auf die Batterielaufzeit der Clients auswirken kann. Beim passiven Scan werden keine Scan Requests gesendet, sondern lediglich passiv gelauscht.

iBeacon-Profile

Definieren Sie Profile, welche Sie dann bei einem BLE-Interface zuordnen können.



Name

Geben Sie dem iBeacon-Profil einen Namen.

UUID

Ein 16 Byte langer Identifikator, der dazu dient, größere Gruppen von Beacons zusammenzufassen. Beispielhaft könnten alle iBeacons eines Unternehmens die gleiche iBeacon-UUID haben.

Major-ID

Ein 2 Byte langer Identifikator, der dazu dient, Untergruppen von iBeacons zu unterscheiden. Beispielhaft könnten alle iBeacons einer Filiale eines Unternehmens den gleiche Major-Identifikator haben.

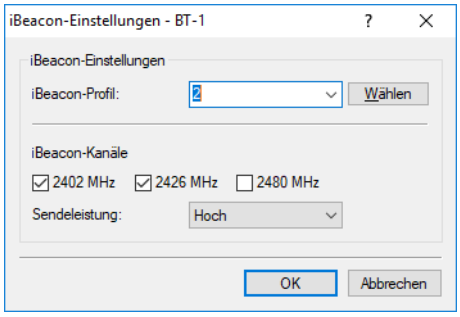
Minor-ID

Ein 2 Byte langer Identifikator, der dazu dient, einzelne iBeacons unterscheiden zu können. Beispielhaft könnte jedes einzele iBeacon in einer Filiale einen eigenen Minor-Identifikator haben.

Empfangsleistungsverschiebung

Normalerweise wird ein entsprechend der eingestellten Sendeleistung gemessener Leistungswert verwendet, um die Annäherung und exakte Entfernung von Geräten zu erkennen, die einen Beacon aussenden. Auf Basis vom entsprechenden Messreihen kann eine Abweichung zwischen gemessener Empfangsleistung und tatsächlicher Entfernung des Gerätes, welches den Beacon aussendet, festgestellt werden. Auf Basis dieser Abweichung kann hier von Experten eine Verschiebung des Referenzwertes des Gerätes angegeben werden, um die Messgenauigkeit zu erhöhen.

iBeacon-Einstellungen



iBeacon-Profil

Wählen Sie hier das iBeacon-Profil aus, um u. a. UUID, Major-ID und Minor-ID zu bestimmen.

iBeacon-Kanäle

Wählen Sie hier die Kanäle, auf denen das iBeacon ausgestrahlt werden soll.

Sendeleistung

Wählen Sie hier die Sendeleistung. Die genaue Bedeutung der auswählbaren Werte ist in der iBeacon-Spezifikation erläutert. Folgende Werte sind möglich:

Hoch

Das Modul sendet mit maximaler Leistung (Default).

Mittel

Das Modul sendet mit durchschnittlicher Leistung.

Gering

Das Modul sendet mit minimaler Leistung.

10.2.2 Monitoring

Monitoring auf der Kommandozeile

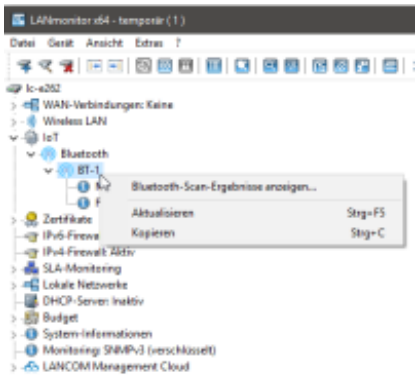
Im Scanning-Modus können die Scan-Ergebnisse in der Tabelle **Status** > **IoT** > **Bluetooth** > **Scan-Resultate** eingesehen werden.

Beachten Sie, dass die iBeacon betreffenden Werte nur gefüllt sind, wenn es sich bei dem gescannten Client tatsächlich um ein iBeacon handelt.

Zur Realisierung der meisten Anwendungsfälle, z. B. Asset Tracking, müssen diese Werte durch ein externes System ausgelesen werden. Hierzu können die üblichen Standardmethoden zum Zugriff auf LANCOM Geräte, vorzugsweise SNMP, verwendet werden.

Monitoring via LANmonitor

Im Scanning-Modus können die Scan-Ergebnisse im LANmonitor in Tabellenform eingesehen werden. Die Scanergebnis-Tabelle ist über das Kontextmenü des entsprechenden Bluetooth-Moduls erreichbar:



Beachten Sie, dass die iBeacon betreffenden Werte nur gefüllt sind, wenn es sich bei dem gescannten Client tatsächlich um ein iBeacon handelt.

Zur Realisierung der meisten Anwendungsfälle, z. B. Asset Tracking, müssen diese Werte durch ein externes System ausgelesen werden. Hierzu können die üblichen Standardmethoden zum Zugriff auf LANCOM Geräte, vorzugsweise SNMP, verwendet werden.

10.3 Ergänzungen im Setup-Menü

10.3.1 IoT

Einstellungen für vom LCOS unterstützte IoT-Technologien wie z. B. Wireless ePaper, iBeacon und Bluetooth Low Energy.

SNMP-ID:

2.111

Pfad Konsole:

Setup

Wireless-ePaper

Konfigurieren Sie hier die Einstellungen für das Wireless ePaper-Modul.

SNMP-ID:

2.111.88

Pfad Konsole:

Setup > IoT

Aktiv

Dieser Eintrag bietet Ihnen die Möglichkeit, die Betriebsart des Moduls festzulegen.

SNMP-ID:

2.111.88.1

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

Aus

Das Modul ist nicht aktiviert.

Manuell

Wireless ePaper Konfigurationen erfolgen manuell.

Verwaltet

Das Modul wird durch einen WLAN-Controller verwaltet.

Default-Wert:

Manuell

Port

Weisen Sie dem Wireless ePaper-Modul einen Port zu.

SNMP-ID:

2.111.88.2

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

2002

Kanal

Legen Sie fest, welchen Kanal das Wireless ePaper-Modul verwenden soll.

Falls Sie aufgrund von mehreren APs in gegenseitiger Reichweite *koordinierte Kanalwahl* verwenden möchten, so sollten Sie hier die automatische Kanalwahl auswählen.

SNMP-ID:

2.111.88.3

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default-Wert:

2425MHz

Koordinierte-Kanalwahl

Vemeidet Mehrfachbelegung von ePaper-Kanälen durch zueinander in Reichweite befindliche APs.

SNMP-ID:

2.111.88.4

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Aktiv

Hier wird die koordinierte Kanalwahl aktiviert bzw. deaktiviert.

SNMP-ID:

2.111.88.4.1

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

0
Nein

1
Ja

Default-Wert:

1

Netzwerk

Hier legen Sie das Netzwerk fest, in dem die Access Points miteinander kommunizieren sollen.

SNMP-ID:

2.111.88.4.2

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

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

Announce-Adresse

Hier legen Sie die Ankündigungs-Adresse fest.

SNMP-ID:

2.111.88.4.3

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

39 Zeichen aus nachfolgendem Zeichensatz: `[0-9 A-F a-f :.]`

Announce-Port

Hier legen Sie den Ankündigungs-Port fest.

SNMP-ID:

2.111.88.4.4

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

5 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Intervall

Hier legen Sie das Ankündigungs-Intervall fest.

SNMP-ID:

2.111.88.4.5

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Timeout-Faktor

Hier legen Sie den Ankündigungs-Timeout-Faktor fest.

SNMP-ID:

2.111.88.4.6

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

5 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Timeout-Intervall

Hier legen Sie das Akündigungs-Timeout-Intervall fest.

SNMP-ID:

2.111.88.4.7

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Master-Backoff-Intervall

Hier legen Sie das Ankündigungs-Master-Backoff-Intervall fest.

SNMP-ID:

2.111.88.4.8

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

3 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Koordination-Port

Hier legen Sie die Port-Koordination fest.

SNMP-ID:

2.111.88.4.9

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

5 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Koordination-Keep-Alive-Intervall

Hier legen Sie die Koordination des Keep-Alive-Intervalls fest.

SNMP-ID:

2.111.88.4.10

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Koordination-Reconnect-Intervall

Hier legen Sie die Koordination des Reconnect-Intervalls fest.

SNMP-ID:

2.111.88.4.11

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Zuweisung-Wechsel-Grenzwert

Hier legen Sie den Grenzwert für den Zuweisungswechsel fest.

SNMP-ID:

2.111.88.4.12

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

3 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Distanz-Bewertung

Hier legen Sie die Bewertung für die Entfernung zum WLAN fest.

Ein höherer Wert bedeutet eine bessere Bewertung.

SNMP-ID:

2.111.88.4.13

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

0 … 255

Kanal-Bewertung

Hier legen Sie die Bewertung für einen ausgesuchten Kanal fest.

Ein höherer Wert bedeutet eine bessere Bewertung.

SNMP-ID:

2.111.88.4.14

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

0 … 255

Bluetooth

Dieses Menü bietet Ihnen die Möglichkeit, Bluetooth-Geräte zu konfigurieren.

SNMP-ID:

2.111.90

Pfad Konsole:

Setup > **IoT**

iBeacon

Dieser Eintrag ermöglicht es Ihnen, das iBeacon-Modul bei Geräten der E-Serie zu konfigurieren.

SNMP-ID:

2.111.90.1

Pfad Konsole:

Setup > **IoT** > **Bluetooth**

Aktiv

Dieser Eintrag bietet Ihnen die Möglichkeit, die Betriebsart des Moduls festzulegen.

SNMP-ID:

2.111.90.1.1

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

Aus

Das Modul ist nicht aktiviert.

Manuell

iBeacon Konfigurationen erfolgen manuell.

Verwaltet

Das Modul wird durch einen WLAN-Controller verwaltet.

Default-Wert:

Verwaltet

UUID

Dieser Eintrag bietet Ihnen die Möglichkeit, dem iBeacon-Modul einen „Universally Unique Identifier" (UUID) zuzuweisen.

SNMP-ID:

2.111.90.1.2

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

max. 36 Zeichen aus `[0-9][a-f][A-F]-`

Default-Wert:

00000000-0000-0000-0000-000000000000

Major

Weisen Sie dem iBeacon-Modul eine eindeutige Major-ID zu.

SNMP-ID:

2.111.90.1.3

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

1 … 65535 Integer-Wert

Default-Wert:

2002

Minor

Weisen Sie dem iBeacon-Modul eine eindeutige Minor-ID zu.

SNMP-ID:

2.111.90.1.4

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

1 … 65535 Integer-Wert

Default-Wert:

1001

Empfangsleistungsverschiebung

Legen Sie die Empfangsleistungsverschiebung fest.

SNMP-ID:

2.111.90.1.5

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]-`

-128 … 127

Default-Wert:

0

Sendeleistung

Legen Sie die Sendeleistung des iBeacon-Moduls fest.

SNMP-ID:

2.111.90.1.6

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

Gering

Das Modul sendet mit minimaler Leistung.

Mittel

Das Modul sendet mit durchschnittlicher Leistung.

Hoch

Das Modul sendet mit maximaler Leistung.

Default-Wert:

Hoch

Kanaele

Legen Sie fest, welche Sendekanäle das iBeacon-Modul verwenden soll.

SNMP-ID:

2.111.90.1.7

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

2402MHz
Das Modul sendet auf Kanal 2402.

2426MHz
Das Modul sendet auf Kanal 2426.

2480MHz
Das Modul sendet auf Kanal 2480.

2402MHz, 2426MHz, 2480MHz
Das Modul sendet auf allen Kanälen.

Default-Wert:

2402MHz, 2426MHz, 2480MHz

Koexistenz

Legen Sie hier fest, ob iBeacon parallel mit dem Wireless ePaper-Dienst betrieben werden soll.

SNMP-ID:

2.111.90.1.8

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Modulneustart

Mit diesem Befehl veranlassen Sie einen Neustart des iBeacon Moduls.

SNMP-ID:

2.111.90.1.9

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Betriebseinstellungen

Dieser Eintrag ermöglicht es Ihnen, die Betriebseinstellungen für das BLE-Modul bei Geräten der B-Serie zu konfigurieren.

SNMP-ID:

2.111.90.2

Pfad Konsole:

Setup > **IoT** > **Bluetooth**

Ifc

Wählen Sie aus den im Gerät verfügbaren BLE-Schnittstellen die Schnittstelle aus, auf die sich die Einstellungen beziehen, z. B. BT-1.

Die Auswahlmöglichkeiten hängen von der jeweiligen Ausstattung Ihres Gerätes ab.

SNMP-ID:

2.111.90.2.1

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Betriebseinstellungen**

Aktiv

Dieser Eintrag bietet Ihnen die Möglichkeit, das Modul zu aktivieren.

SNMP-ID:

2.111.90.2.2

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Betriebseinstellungen**

Mögliche Werte:

ja

Das Modul ist aktiviert.

nein

Das Modul ist nicht aktiviert.

Default-Wert:

nein

Betriebsart

Dieser Eintrag bietet Ihnen die Möglichkeit, die Betriebsart des BLE-Moduls einzustellen. Wählen Sie, ob die Bluetooth-Schnittstelle zum Aussenden von Beacons, oder zum Scannen der Umgebung verwendet werden soll.

Ein gleichzeitiger Betrieb der beiden Betriebsarten ist nicht möglich.

SNMP-ID:

2.111.90.2.3

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Betriebseinstellungen**

Mögliche Werte:

BLE-Beacon

Das BLE-Modul sendet Beacons aus.

Scanner

Das BLE-Modul wird für den Umgebungsscan verwendet.

Default-Wert:

Scanner

Scanart

Wählen Sie hier, ob aktiv oder passiv gescannt werden soll. Beim aktiven Scan werden aktiv Scan Requests gesendet, welche die BLE-Clients in der Umgebung beantworten. Dies ist z. B. notwendig, um Namen der Clients zu ermitteln.

Beachten Sie, dass sich das ständige Beantworten der Scan Requests auf die Batterielaufzeit der Clients auswirken kann. Beim passiven Scan werden keine Scan Requests gesendet, sondern lediglich passiv gelauscht.

SNMP-ID:

2.111.90.2.4

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Betriebseinstellungen**

Mögliche Werte:

Passiv
Aktiv

Default-Wert:

Passiv

Beacon-Einstellungen

Konfigurieren Sie hier weitere Parameter für iBeacon bei Geräten der B-Serie.

SNMP-ID:

2.111.90.3

Pfad Konsole:

Setup > **IoT** > **Bluetooth**

Ifc

Wählen Sie aus den im Gerät verfügbaren BLE-Schnittstellen die Schnittstelle aus, auf die sich die Einstellungen beziehen, z. B. BT-1.

Die Auswahlmöglichkeiten hängen von der jeweiligen Ausstattung Ihres Gerätes ab.

SNMP-ID:

2.111.90.3.1

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Einstellungen**

Beacon-Profile

Tragen Sie hier den Namen des in der Beacon-Profile-Tabelle angelegten iBeacon-Profils ein.

SNMP-ID:

2.111.90.3.2

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Einstellungen**

Mögliche Werte:

max. 17 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Kanaele

Wählen Sie hier die BLE-Kanäle, auf welchen das iBeacon ausgestrahlt werden soll.

SNMP-ID:

2.111.90.3.3

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Einstellungen**

Mögliche Werte:

2402MHz

Das Modul sendet auf Kanal 2402.

2426MHz

Das Modul sendet auf Kanal 2426.

2480MHz

Das Modul sendet auf Kanal 2480.

2402MHz, 2426MHz, 2480MHz

Das Modul sendet auf allen Kanälen.

Default-Wert:

2402MHz, 2426MHz, 2480MHz

Sendeleistung

Wählen Sie hier die Sendeleistung. Die genaue Bedeutung der auswählbaren Werte ist in der iBeacon-Spezifikation erläutert.

SNMP-ID:

2.111.90.3.4

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Einstellungen**

Mögliche Werte:

Gering

Das Modul sendet mit minimaler Leistung.

Mittel

Das Modul sendet mit durchschnittlicher Leistung.

Hoch

Das Modul sendet mit maximaler Leistung.

Default-Wert:

Hoch

Beacon-Profile

Konfigurieren Sie hier die Parameter für iBeacon bei Geräten der B-Serie.

SNMP-ID:

2.111.90.4

Pfad Konsole:

Setup > **IoT** > **Bluetooth**

Name

Konfigurieren Sie hier einen Namen für dieses Beacon-Profil.

SNMP-ID:

2.111.90.4.1

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Profile**

Mögliche Werte:

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

Default-Wert:

leer

iBeacon-UUID

Ein 16 Byte langer Identifikator, der dazu dient, größere Gruppen von Beacons zusammenzufassen. Beispielhaft könnten alle iBeacons eines Unternehmens die gleiche iBeacon-UUID haben.

SNMP-ID:

2.111.90.4.2

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Profile**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][a-f][0-9]-`

Default-Wert:

leer

iBeacon-Major

Ein 2 Byte langer Identifikator, der dazu dient, Untergruppen von iBeacons zu unterscheiden. Beispielhaft könnten alle iBeacons einer Filiale eines Unternehmens den gleiche Major-Identifikator haben.

SNMP-ID:

2.111.90.4.3

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Profile**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

leer

iBeacon-Minor

Ein 2 Byte langer Identifikator, der dazu dient, einzelne iBeacons unterscheiden zu können. Beispielhaft könnte jedes einzele iBeacon in einer Filiale einen eigenen Minor-Identifikator haben.

SNMP-ID:

2.111.90.4.4

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Profile**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

leer

Empfangsleistungsverschiebung

Normalerweise wird ein entsprechend der eingestellten Sendeleistung gemessener Leistungswert verwendet, um die Annäherung und exakte Entfernung von Geräten zu erkennen, die einen Beacon aussenden. Auf Basis vom entsprechenden Messreihen kann eine Abweichung zwischen gemessener Empfangsleistung und tatsächlicher Entfernung des Gerätes, welches den Beacon aussendet, festgestellt werden. Auf Basis dieser Abweichung kann hier von Experten eine Verschiebung des Referenzwertes des Gerätes angegeben werden, um die Messgenauigkeit zu erhöhen.

SNMP-ID:

2.111.90.4.5

Pfad Konsole:

Setup > **IoT** > **Bluetooth** > **Beacon-Profile**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]-`

-128 … 127

Default-Wert:

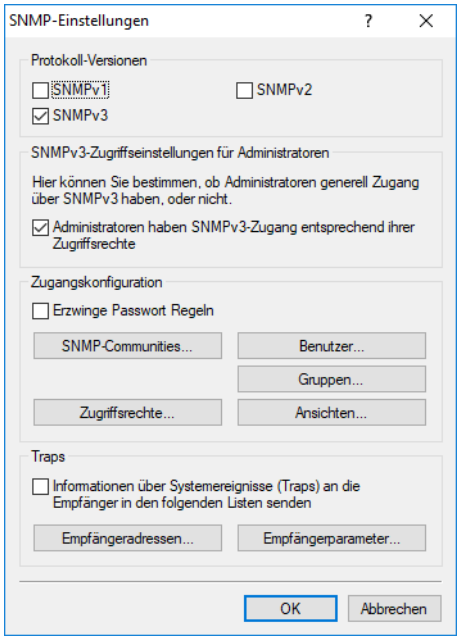
leer

11 Weitere Dienste

11.1 Simple Network Management Protocol (SNMP)

11.1.1 Regeln für SNMPv3-Passwörter

LCOS ab Version 10.32 unterstützt die Durchsetzung von Passwortregeln für die SNMPv3-Authentifizierung und das Passwort für SNMPv3-Verschlüsselung. Die Einstellung erfolgt unter **Management** > **Admin** > **SNMP-Einstellungen** > **Zugangskonfiguration** über die Option **Erzwinge Passwortregeln**.



Folgende Regeln werden dadurch aktiv:

- Die Länge des Passworts muss mindestens 16 Zeichen betragen.
- Das Passwort muss mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten.

Beachten Sie, dass beim Einschalten dieser Funktion die aktuellen Passwörter nicht unmittelbar überprüft werden. Nur bei zukünftigen Änderungen der Passwörter werden diese auf ihre Übereinstimmung mit der Richtlinie überprüft.

11.1.2 Ergänzungen im Setup-Menü

Password-Regeln-Erzwingen

Mit diesem Eintrag haben Sie die Möglichkeit, das Erzwingen von Passwort-Regeln zu aktivieren oder zu deaktivieren. Es gelten dann die folgenden Regeln für die SNMPv3-Authentifizierung und das Passwort für SNMPv3-Verschlüsselung:

- Die Länge des Passworts muss mindestens 16 Zeichen betragen.

- Das Passwort muss mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten.

Beachten Sie, dass beim Einschalten dieser Funktion die aktuellen Passwörter nicht unmittelbar überprüft werden. Nur bei zukünftigen Änderungen der Passwörter werden diese auf ihre Übereinstimmung mit der Richtlinie überprüft.

Damit bei SNMPv3 Passwörter verwendet werden, darf in der Tabelle **Setup** > **SNMP** > **Benutzer** keiner der beiden Einträge **Authentifizierungs-Protokoll** und **Verschluesselungs-Protokoll** auf **None** eingestellt sein.

SNMP-ID:

2.9.43

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

nein

Das Erzwingen von Passwort-Regeln ist deaktiviert.

ja

Das Erzwingen von Passwort-Regeln ist aktiviert.

Default-Wert:

nein

11.2 TACACS+

11.2.1 Konfiguration der TACACS+-Server

Zur Nutzung der TACACS+-Funktionen können zwei Server definiert werden. Dabei dient ein Server als Backup, falls der andere Server ausfällt. Beim Login über Telnet oder WEBconfig kann der Anwender den zu benutzenden Server auswählen.

TACACS+ unterstützt ab LCOS 10.30 IPv6, d. h. als Server-Adresse kann neben einem DNS-Namen und IPv4-Adresse auch eine IPv6-Adresse konfiguriert werden.

Die Parameter für die Konfiguration der TACACS+-Server finden Sie unter:

Kommandozeile: **Setup** > **TACACS+** > **Server**

Server-Adresse

Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Autorisierung und Accounting weitergeleitet werden sollen.

Mögliche Werte:

- Gültiger DNS-auflösbarer Name oder gültige IPv4- oder IPv6-Adresse.

Default

- Leer

Ergänzungen im Setup-Menü

Server-Adresse

DNS-Name, IPv4- oder IPv6-Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Authorisierung und Accounting weitergeleitet werden sollen.

SNMP-ID:

2.54.9.1

Pfad Konsole:

Setup > **Tacacs+** > **Server**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer