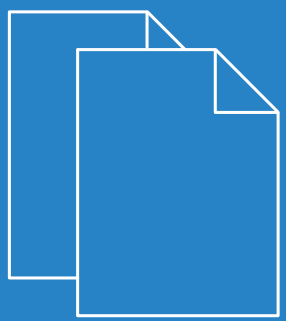
SICHER. **VERNETZT.**

LCOS 10.42

Addendum



12/2020

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS-Version 10.42

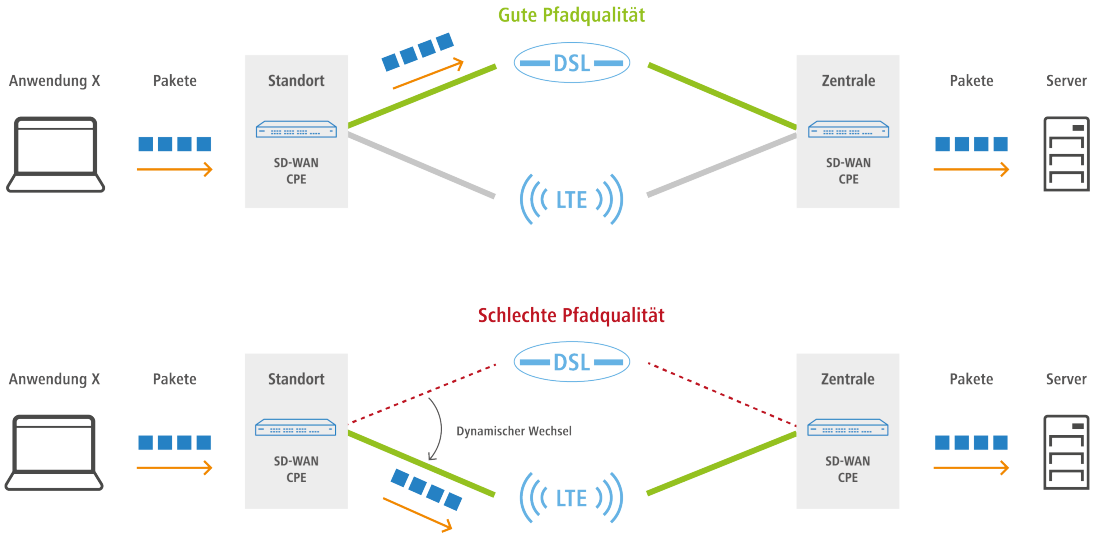
Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.42 gegenüber der vorherigen Version.

2 Routing und WAN-Verbindungen

2.1 SD-WAN Dynamic Path Selection

Dynamic Path Selection (DPS) erlaubt die Steuerung von Datenverkehr über die Leitung mit der besten Qualität basierend auf Metriken wie Last, Paketverlust, Latenz oder Jitter um die Anwendungsperformance bei mehreren verfügbaren Leitungen in einem SD-WAN-Szenario zu optimieren.

In SD-WAN-Szenarien sollen MPLS-Leitungen entweder ersetzt oder um kostengünstige Internetverbindungen wie DSL, Kabelinternet, Glasfaser oder 4G/5G ergänzt werden. Mithilfe von Load Balancing kann die Gesamtbandbreite aller zur Verfügung stehenden Leitungen ausgenutzt werden. Um die Performance geschäftskritischer Anwendungen sicherzustellen, kann Dynamic Path Selection eingesetzt werden. Dabei werden alle Leitungen kontinuierlich durch aktives Monitoring mithilfe von ICMP-Paketen überwacht und daraus Metriken für Last, Paketverlust, Latenz und Jitter berechnet. Durch Richtlinien werden Anforderungen der Business-Anwendungen wie z. B. Echtzeitdatenverkehr an Leitungen definiert, beispielweise der erlaubte Paketverlust oder die maximale Latenz eines möglichen Pfades. Der Algorithmus zur Dynamic Path Selection wählt für Sessions die Leitung mit der besten Qualität aus. Erfüllen mehrere Leitungen die geforderten Richtlinien, so wird ein Load Balancing im Round-Robin-Verfahren über diese Leitungen durchgeführt.



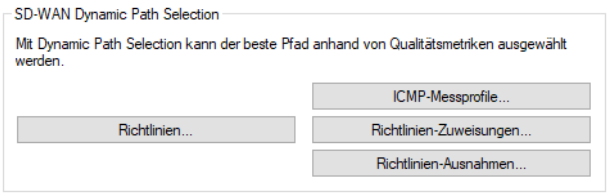
Richtlinien können als „kritisch" definiert werden. Falls keine Leitung diese Richtlinie erfüllt, wird der Datenverkehr über keine Leitung transportiert.

Dynamic Path Selection wird auf einem Load Balancer aktiviert. Ein Load Balancer kann entweder für Internetverbindungen oder SD-WAN-Overlay-Tunnel (VPN) definiert sein. Der Endpunkt für ICMP-Testpakete kann entweder eine beliebige IP-Adresse oder das zentralseitige SD-WAN-Gateway sein.

In der Firewall werden die definierten (Load-Balancer-)Richtlinien für die Anwendungen in entsprechenden Firewall-Regeln verwendet. Dort wird definiert für welchen Datenverkehr bzw. Anwendungen die Load-Balancer-Richtlinie gelten soll.

2.1.1 Konfiguration der Dynamic Path Selection

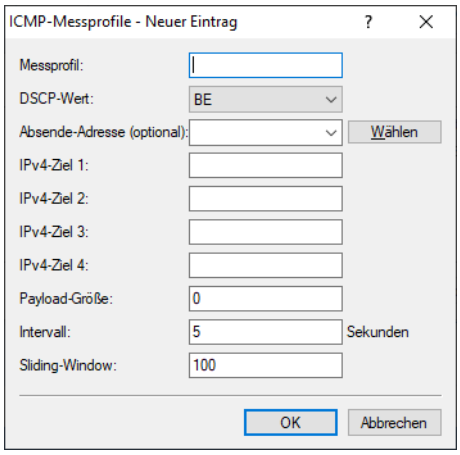
Um Dynamic Path Selection mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection**.



ICMP-Messprofile

ICMP-Messprofile definieren einen Parametersatz, nach dem Messungen auf Basis von ICMP-Pings durchgeführt werden. Aus den Messungen werden Interface-Metriken abgeleitet, die die Verbindungsqualität quantifizieren sollen. Diese Metriken sind: Mittlere Round Trip Time (RTT, Latenz), Jitter und Paketverlustrate (Packet Loss Rate).

Zur Konfiguration der ICMP-Messprofile wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP-Messprofile**.



Messprofil

Der Name des Profils. Über diesen Namen wird das Profil in DPS-Richtlinien referenziert.

DSCP-Wert

Definiert den DSCP-Wert, der im IP-Header der Messpakete gesetzt wird. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

Absende-Adresse (optional)

Referenziert eine benamte Loopback-Adresse, die bei den Messpaketen als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus, die zum Absende-Interface passt.

IPv4-Ziel 1-4

Bis zu 4 Messziele als gültige IPv4-Unicast-Adressen oder DNS Hostnamen. Wird 0.0.0.0 eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

Payload-Größe

Gibt die Größe der Daten nach dem ICMP-Header (Payload-Größe) der versendeten Pings an.

Intervall

Der Abstand in Sekunden zwischen 2 Messungen. Außerdem wird die maximale Round Trip Time vorgegeben. Pakete, die binnen eines Messintervalls nicht beantwortet wurden, zählen als Packet Loss.

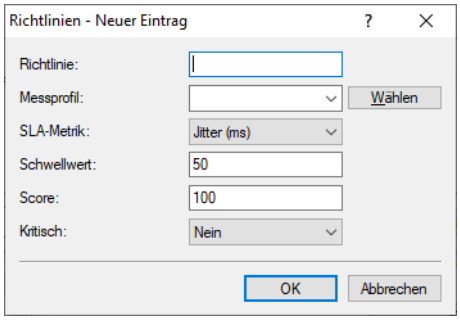
Sliding-Window

Maximale Anzahl an Messwerten, die für die Bestimmung der Interface-Metriken benutzt werden. Wird ein Messwert empfangen, obwohl bereits die hier angegebene Anzahl an Messwerten aufgezeichnet wurde, dann wird der älteste Messwert verworfen.

Richtlinien

Um die Verbindungsqualität von Interfaces für die dynamische Pfadauswahl bewerten zu können, können den aus den Messprofilen errechneten Metriken abhängig von Schwellenwerten Punktwerte zugewiesen werden. Diese Punktwerte werden aufsummiert, um das „beste" Interface zu bestimmen. Es ist ebenfalls möglich, einzelne Schwellenwerte als „kritisch" zu bewerten (z. B. ein Jitter <= 30 ms). Die Summe dieser Punkte (Gesamtergebnis) und die überschrittenen kritischen Schwellenwerte stellen die Grundlage für dynamische Load Balancer-Entscheidungen dar. Eine DPS-Richtlinie enthält die Sammlung der Schwellenwerte und Kritikalitätsmarkierungen, die für eine Berechnung der Punktsumme notwendig sind.

Zur Konfiguration der DPS-Richtlinien wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien**.



Richtlinie

Der Name der DPS-Richtlinie. Über diesen Namen wird die Richtlinie in Firewall-Regeln referenziert. Alle Zeilen in dieser Tabelle, die den selben Richtlinien-Namen tragen, werden zu einer Richtlinie zusammengefasst. Somit ist es möglich, u. a. die selbe Metrik mehrfach mit verschiedenen Schwellenwerten in der selben Richtlinie zu verwenden. So lässt sich eine abgestufte Punktebewertung vornehmen (z. B. 10 Punkte bei Latenz <= 100, weitere 10 Punkte bei Latenz <= 50).

Messprofil

Entweder leer oder der Name eines ICMP-Messprofils.

Das Feld muss genau dann leer sein, wenn als **SLA-Metrik** „Last(%)" ausgewählt wird. In allen anderen Fällen muss ein Messprofil angegeben werden.

SLA-Metrik

Die aus den Messungen des eingestellten Messprofils generierte Metrik, deren Wert gegen den Schwellenwert verglichen wird. Mögliche Werte:

- Latenz (ms)
- Jitter (ms)
- Paketverlust (%)
- Last (%)

Die Metrik „Last(%)“ bezeichnet die Auslastung des Interfaces in Prozent der Maximalbandbreite. Dieser Wert wird nicht über gesonderte Messungen ermittelt, daher muss in diesem Fall der Eintrag **Messprofil** leer bleiben.

Schwellwert

Der Schwellenwert, den die gewählte SLA-Metrik nicht unterschreiten darf.

Score

Wenn eine Metrik den gewählten Schwellenwert unterschreitet, dann wird diese Punktzahl zum Gesamtergebnis der Richtlinie dazuaddiert.

Kritisch

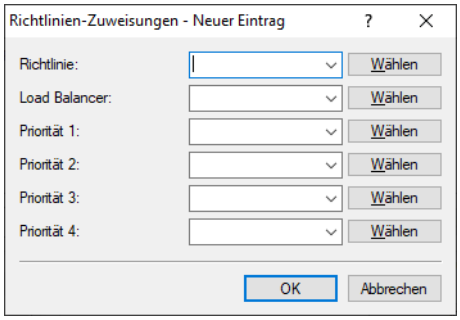
Markierung, ob ein Schwellenwert kritisch ist. Wenn ein als „kritisch“ markierter Schwellenwert nicht unterschritten wird, ist das Gesamtergebnis nicht definiert.

Ein Interface mit einem undefinierten Gesamtergebnis kann nicht durch eine dynamische Load Balancer-Entscheidung ausgewählt werden.

Richtlinien-Zuweisungen

Hier legen Sie fest, welche DPS-Richtlinie mit welchem Load Balancer verwendet werden soll, und welche Prioritäten bei Gleichstand des Gesamtergebnisses gelten sollen.

Zur Konfiguration der Richtlinien-Zuweisungen wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Zuweisungen**.



Richtlinie

Der Name einer existierenden DPS-Richtlinie aus *Richtlinien* auf Seite 7.

Load Balancer

Name eines Load Balancers, der mit dieser Policy bewertet werden soll. Auf allen Interfaces, die zu diesem Load Balancer gehören, werden automatisch Messungen entsprechend der in der Richtlinie referenzierten Messprofile gestartet.

Es ist möglich, das Starten der Messungen für einzelne Interfaces dieses Load Balancers zu unterdrücken. Siehe hierzu *Richtlinien-Ausnahmen* auf Seite 9.

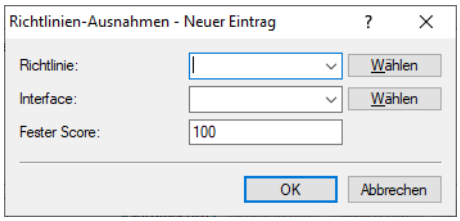
Priorität

Wenn im Rahmen der dynamischen Pfadauswahl mehrere Interfaces das gleiche Polixy-Gesamtergebnis erreichen, wird über die Einträge „Priorität“ bestimmt, welches Interface ausgewählt wird (1 – höchste Priorität, 4 – geringste Priorität). Wenn die Felder leer gelassen werden, dann wird ein Load Balancing nach der standardmäßigen Load-Balancer-Verteilungsstrategie „Round-Robin“ durchgeführt.

Richtlinien-Ausnahmen

Es ist möglich, einzelne Messprofile nicht auf bestimmte Interfaces anzuwenden, z. B. wenn diese per Volumentarif bezahlt werden.

Zur Konfiguration der Richtlinien-Ausnahmen wechseln Sie in die Ansicht **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Ausnahmen**.



Richtlinie

Der Name einer existierenden DPS-Richtlinie aus *Richtlinien* auf Seite 7.

Interface

Der Name eines Interfaces (z. B. WAN-Gegenstellen, VPN-Tunnel), welches Teil eines Load Balancers ist, der von der Richtlinie bewertet werden soll. Die in der Richtlinie referenzierten Messprofile werden nicht dafür genutzt, um auf dem Interface Messungen zu starten.

Wenn ein Interface Bestandteil mehrerer Load Balancer ist oder wenn mehrere Richtlinien den Load Balancer, der dieses Interface enthält, bewerten sollen, dann muss das Interface für alle in Frage kommenden Richtlinien als Ausnahme eingetragen werden, um die Messungen zu verhindern.

Fester Score

Da es ohne Messungen nicht möglich ist, ein dynamisches Gesamtergebnis zu bestimmen, wird dieser Wert bei allen Entscheidungen zur dynamischen Pfadauswahl als Wert für das Interface verwendet.

2.1.2 Show Kommandos

- `DPS-v4-Policies <Richtlinie> <Gegenstelle>`: Zeigt Informationen über die IPv4-Richtlinien des Dynamic Path Selection für die entsprechende Richtlinie und Gegenstelle.
- `DPS-v4-Score <Richtlinie> <Loadbalancer>`: Zeigt Informationen über den Wert des Dynamic Path Selection bei IPv4 für die entsprechenden Richtlinie und Load-Balancer.
- `DPS-v4-Score-Details <Richtlinie> <Gegenstelle>`: Zeigt Detail-Informationen über den IPv4 Dynamic Path Selection Wert der entsprechenden Richtlinie und Gegenstelle.
- Erweiterung des Ping Kommandos:

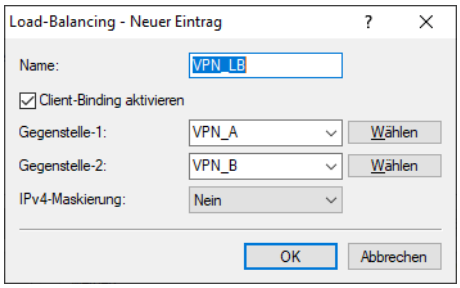
  `ping -l <Richtlinie>`: Verwendet die angegebene Dynamic Path Selection Load-Balancer-Richtlinie, um das abgehende Interface zu bestimmen.

2.1.3 Beispielkonfigurationen

Szenario mit zwei VPN-Tunneln über zwei unterschiedliche Internetverbindungen von der Filiale zur Zentrale

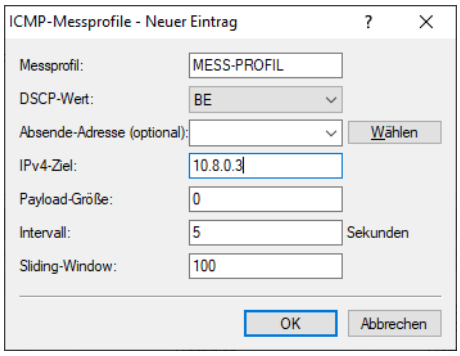
In diesem Beispiel soll Dynamic Path Selection in einem Szenario mit zwei VPN-Tunneln über zwei unterschiedliche Internetverbindungen von der Filiale zur Zentrale für den gesamten Datenverkehr eingerichtet werden. Die IP-Adresse zur Überprüfung der Leitungsqualität per ICMP-Testpaketen ist die private IP-Adresse des zentralseitigen Gateways 10.8.0.3. Ziel ist es, dass immer nur die beste Leitung bzw. VPN-Tunnel basierend auf der Latenz gewählt werden soll.

Dynamic Path Selection wird dabei nur in der Filiale aktiviert. Es wird davon ausgegangen, dass die beiden Internetverbindungen vorhanden sind und die beiden VPN-Tunnel VPN_A und VPN_B bereits zu einem Load Balancer mit Namen VPN_LB eingerichtet wurden:



1. Legen Sie eine neue Tabellenzeile unter **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP-Messprofile** an.

   Im ersten Schritt wird zunächst ein neues Messprofil angelegt. Das IPv4-Ziel ist hierbei die private IP-Adresse des zentralseitigen Gateways 10.8.0.3. In einem Intervall von 5 Sekunden werden Messpakete zur Evaluierung der Pfade über die VPN-Tunnel (SD-WAN-Overlays) gesendet.

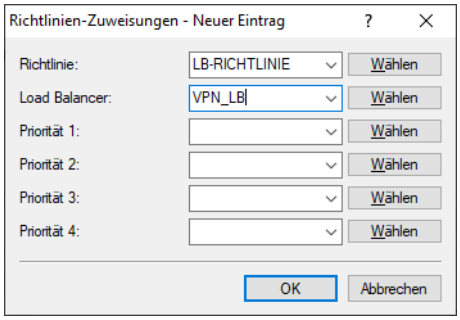


2. Legen Sie eine neue Tabellenzeile unter **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien** an.

   Im nächsten Schritt wird eine neue Richtlinie angelegt, die als SLA-Metrik „Latenz" einen Schwellenwert von 50 ms besitzt. Wenn der entsprechende VPN-Tunnel eine Latenz unter 50 ms besitzt, so erhält der Pfad einen Score von 100 (Punkten). Eine Verbindung, die dieses Kriterium nicht erfüllt, erhält einen Score von 0, d. h. sie wird also schlechter bewertet. Der Pfad mit dem höchsten Score wird bevorzugter Pfad und somit für den Datenverkehr verwendet. Haben beide Pfade einen identischen Score von 100, so wird ein Load-Balancing zwischen beiden VPN-Tunneln durchgeführt.

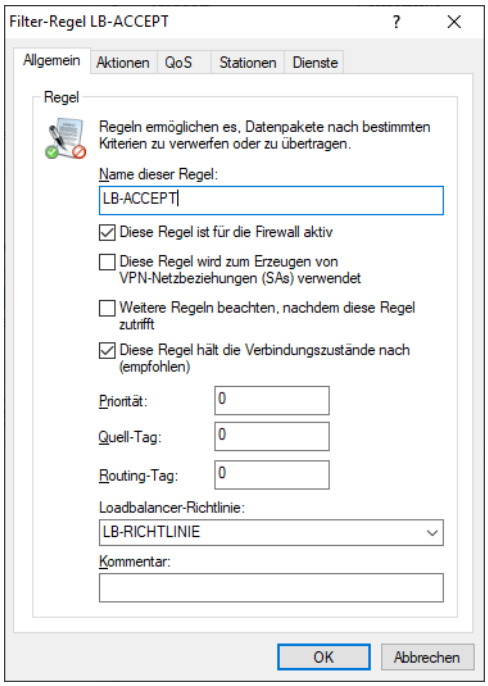
3. Legen Sie eine neue Tabellenzeile unter **IP-Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Richtlinien-Zuweisungen** an.

Im Folgenden wird die eben neu erstellte Richtlinie mit dem VPN-Load-Balancer-Verbund VPN_LB verknüpft. Die Felder für Prioritäten können leer bleiben.



4. Legen Sie eine neue Tabellenzeile unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** an.

   Legen Sie eine neue Firewall-Regel an, die allen Datenverkehr akzeptiert und als Load-Balancer-Richtlinie den Wert „LB-RICHTLINIE“ besitzt.



2.1.4 Ergänzungen im Setup-Menü

Dynamische-Pfadauswahl

Dynamic Path Selection erlaubt die Steuerung von Datenverkehr über die Leitung mit der besten Qualität basierend auf Metriken wie Last, Paketverlust, Latenz oder Jitter um die Anwendungsperformance bei mehreren verfügbaren Leitungen in einem SD-WAN-Szenario zu optimieren.

Dynamic Path Selection wird auf einem Load Balancer aktiviert (siehe *2.8.10.2.16 LB-Policy* auf Seite 22). Ein Load Balancer kann entweder für Internetverbindungen oder SD-WAN-Overlay-Tunnel (VPN) definiert sein. Der Endpunkt für ICMP-Testpakete kann entweder eine beliebige IP-Adresse oder das zentralseitige SD-WAN-Gateway sein.

SNMP-ID:

2.110.4

Pfad Konsole:

Setup > **Firewall**

ICMP-Messprofile

ICMP-Messprofile definieren einen Parametersatz, nach dem Messungen auf Basis von ICMP-Pings durchgeführt werden. Aus den Messungen werden Interface-Metriken abgeleitet, die die Verbindungsqualität quantifizieren sollen. Diese Metriken sind: Mittlere Round Trip Time (RTT, Latenz), Jitter und Paketverlustrate (Packet Loss Rate).

SNMP-ID:

2.110.4.1

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl**

Messprofil

Der Name des Profils. Über diesen Namen wird das Profil in DPS-Richtlinien referenziert.

SNMP-ID:

2.110.4.1.1

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

DSCP-Wert

Definiert den DSCP-Wert, der im IP-Header der Messpakete gesetzt wird. DSCP (Differentiated Services Code Point) wird für QoS (Quality of Service) verwendet.

SNMP-ID:

2.110.4.1.2

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

BE
CS0
CS1
CS2
CS3
CS4
CS5
CS6
CS7
AF11
AF12
AF13
AF21
AF22
AF23
AF31
AF32
AF33
AF41
AF42
AF43
EF

Loopback-Addr.

Referenziert optional eine benamte Loopback-Adresse, die bei den Messpaketen als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus, die zum Absende-Interface passt.

SNMP-ID:

2.110.4.1.3

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

IPv4-Ziel-1

Das erste von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresse oder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

SNMP-ID:

2.110.4.1.4

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

Payload-Groesse

Gibt die Größe der Daten nach dem ICMP-Header (Payload-Größe) der versendeten Pings an.

SNMP-ID:

2.110.4.1.6

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

Intervall

Der Abstand in Sekunden zwischen 2 Messungen. Außerdem wird die maximale Round Trip Time vorgegeben. Pakete, die binnen eines Messintervalls nicht beantwortet wurden, zählen als Packet Loss.

SNMP-ID:

2.110.4.1.7

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

Sliding-Window

Maximale Anzahl an Messwerten, die für die Bestimmung der Interface-Metriken benutzt werden. Wird ein Messwert empfangen, obwohl bereits die hier angegebene Anzahl an Messwerten aufgezeichnet wurde, dann wird der älteste Messwert verworfen.

SNMP-ID:

2.110.4.1.8

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

IPv4-Ziel-2

Das zweite von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresse oder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

SNMP-ID:

2.110.4.1.9

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

IPv4-Ziel-3

Das dritte von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresse oder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

SNMP-ID:

2.110.4.1.10

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

IPv4-Ziel-4

Das vierte von bis zu 4 Messzielen als gültige IPv4-Unicast-Adresseoder DNS Hostname. Wird „0.0.0.0" eingetragen, wird das Messziel dynamisch vom VPN festgelegt. Wird das Feld leer gelassen, erfolgt keine Messung für die entsprechende Adressfamilie.

SNMP-ID:

2.110.4.1.11

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **ICMP-Messprofile**

Mögliche Werte:

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

Richtlinien

Um die Verbindungsqualität von Interfaces für die dynamische Pfadauswahl bewerten zu können, können den aus den Messprofilen errechneten Metriken abhängig von Schwellenwerten Punktwerte zugewiesen werden. Diese Punktwerte werden aufsummiert, um das „beste" Interface zu bestimmen. Es ist ebenfalls möglich, einzelne Schwellenwerte als „kritisch" zu bewerten (z. B. ein Jitter <= 30 ms). Die Summe dieser Punkte (Gesamtergebnis) und die überschrittenen kritischen Schwellenwerte stellen die Grundlage für dynamische Load Balancer-Entscheidungen dar. Eine DPS-Richtlinie enthält die Sammlung der Schwellenwerte und Kritikalitätsmarkierungen, die für eine Berechnung der Punktsumme notwendig sind.

SNMP-ID:

2.110.4.16

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl**

Richtlinie

Der Name der DPS-Richtlinie. Über diesen Namen wird die Richtlinie in Firewall-Regeln referenziert. Alle Zeilen in dieser Tabelle, die den selben Richtlinien-Namen tragen, werden zu einer Richtlinie zusammengefasst. Somit ist es möglich, u. a. die selbe Metrik mehrfach mit verschiedenen Schwellenwerten in der selben Richtlinie zu verwenden. So lässt sich eine abgestufte Punktebewertung vornehmen (z. B. 10 Punkte bei Latenz <= 100, weitere 10 Punkte bei Latenz <= 50).

SNMP-ID:

2.110.4.16.1

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien**

Mögliche Werte:

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

Messprofil

Entweder leer oder der Name eines ICMP-Messprofils.

Das Feld muss genau dann leer sein, wenn als SLA-Metrik „Last(%)" ausgewählt wird. In allen anderen Fällen muss ein Messprofil angegeben werden.

SNMP-ID:

2.110.4.16.2

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien**

Mögliche Werte:

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

SLA-Metrik

Die aus den Messungen des eingestellten Messprofils generierte Metrik, deren Wert gegen den Schwellenwert verglichen wird.

Die Metrik „Last(%)" bezeichnet die Auslastung des Interfaces in Prozent der Maximalbandbreite. Dieser Wert wird nicht über gesonderte Messungen ermittelt, daher muss in diesem Fall der Eintrag *2.110.4.16.2 Messprofil* auf Seite 16 leer bleiben.

SNMP-ID:

2.110.4.16.3

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien**

Mögliche Werte:

Latenz(ms)
Jitter(ms)
Paketverlust(%)
Last(%)

Schwellwert

Der Schwellenwert, den die gewählte SLA-Metrik nicht unterschreiten darf.

SNMP-ID:

2.110.4.16.4

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien**

Mögliche Werte:

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

Wert

Wenn eine Metrik den gewählten Schwellenwert unterschreitet, dann wird diese Punktzahl zum Gesamtergebnis der Richtlinie dazuaddiert.

SNMP-ID:

2.110.4.16.5

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien**

Mögliche Werte:

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

Kritisch

Markierung, ob ein Schwellenwert kritisch ist. Wenn ein als „kritisch" markierter Schwellenwert nicht unterschritten wird, ist das Gesamtergebnis nicht definiert.

Ein Interface mit einem undefinierten Gesamtergebnis kann nicht durch eine dynamische Load Balancer-Entscheidung ausgewählt werden.

SNMP-ID:

2.110.4.16.6

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien**

Mögliche Werte:

Nein

Schwellenwert wird nicht als kritisch markiert.

Ja

Schwellenwert wird als kritisch markiert.

Richtlinien-Zuweisungen

Hier legen Sie fest, welche DPS-Richtlinie mit welchem Load Balancer verwendet werden soll, und welche Prioritäten bei Gleichstand des Gesamtergebnisses gelten sollen.

SNMP-ID:

2.110.4.17

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl**

Richtlinie

Der Name einer existierenden DPS-Richtlinie aus *2.110.4.16.1 Richtlinie* auf Seite 16.

SNMP-ID:

2.110.4.17.1

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

Mögliche Werte:

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

Load-Balancer

Name eines Load Balancers, der mit dieser Policy bewertet werden soll. Auf allen Interfaces, die zu diesem Load Balancer gehören, werden automatisch Messungen entsprechend der in der Richtlinie referenzierten Messprofile gestartet.

Es ist möglich, das Starten der Messungen für einzelne Interfaces dieses Load Balancers zu unterdrücken. Siehe hierzu *2.110.4.18 Richtlinien-Zuweisungs-Ausnahmen* auf Seite 21.

SNMP-ID:

2.110.4.17.2

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

Mögliche Werte:

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

Prioritaet-1

Wenn im Rahmen der dynamischen Pfadauswahl mehrere Interfaces das gleiche Policy-Gesamtergebnis erreichen, wird über die Einträge „Priorität" bestimmt, welches Interface ausgewählt wird (1 – höchste Priorität, 4 – geringste Priorität). Wenn die Felder leer gelassen werden, dann wird ein Load Balancing nach der standardmäßigen Load-Balancer-Verteilungsstrategie „Round-Robin" durchgeführt.

SNMP-ID:

2.110.4.17.3

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

Mögliche Werte:

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

Prioritaet-2

Wenn im Rahmen der dynamischen Pfadauswahl mehrere Interfaces das gleiche Policy-Gesamtergebnis erreichen, wird über die Einträge „Priorität" bestimmt, welches Interface ausgewählt wird (1 – höchste Priorität, 4 – geringste Priorität).

Wenn die Felder leer gelassen werden, dann wird ein Load Balancing nach der standardmäßigen Load-Balancer-Verteilungsstrategie „Round-Robin“ durchgeführt.

SNMP-ID:

2.110.4.17.4

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

Mögliche Werte:

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

Prioritaet-3

Wenn im Rahmen der dynamischen Pfadauswahl mehrere Interfaces das gleiche Policy-Gesamtergebnis erreichen, wird über die Einträge „Priorität“ bestimmt, welches Interface ausgewählt wird (1 – höchste Priorität, 4 – geringste Priorität). Wenn die Felder leer gelassen werden, dann wird ein Load Balancing nach der standardmäßigen Load-Balancer-Verteilungsstrategie „Round-Robin“ durchgeführt.

SNMP-ID:

2.110.4.17.5

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

Mögliche Werte:

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

Prioritaet-4

Wenn im Rahmen der dynamischen Pfadauswahl mehrere Interfaces das gleiche Policy-Gesamtergebnis erreichen, wird über die Einträge „Priorität“ bestimmt, welches Interface ausgewählt wird (1 – höchste Priorität, 4 – geringste Priorität). Wenn die Felder leer gelassen werden, dann wird ein Load Balancing nach der standardmäßigen Load-Balancer-Verteilungsstrategie „Round-Robin“ durchgeführt.

SNMP-ID:

2.110.4.17.6

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungen**

Mögliche Werte:

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

Richtlinien-Zuweisungs-Ausnahmen

Es ist möglich, einzelne Messprofile nicht auf bestimmte Interfaces anzuwenden, z. B. wenn diese per Volumentarif bezahlt werden.

SNMP-ID:

2.110.4.18

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl**

Richtlinie

Der Name einer existierenden DPS-Richtlinie aus *2.110.4.16.1 Richtlinie* auf Seite 16.

SNMP-ID:

2.110.4.18.1

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungs-Ausnahmen**

Mögliche Werte:

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

Interface

Der Name eines Interfaces (z. B. WAN-Gegenstellen, VPN-Tunnel), welches Teil eines Load Balancers ist, der von der Richtlinie bewertet werden soll. Die in der Richtlinie referenzierten Messprofile werden nicht dafür genutzt, um auf dem Interface Messungen zu starten.

Wenn ein Interface Bestandteil mehrerer Load Balancer ist oder wenn mehrere Richtlinien den Load Balancer, der dieses Interface enthält, bewerten sollen, dann muss das Interface für alle in Frage kommenden Richtlinien als Ausnahme eingetragen werden, um die Messungen zu verhindern.

SNMP-ID:

2.110.4.18.2

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungs-Ausnahmen**

Mögliche Werte:

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

Wert-Fest

Da es ohne Messungen nicht möglich ist, ein dynamisches Gesamtergebnis zu bestimmen, wird dieser Wert bei allen Entscheidungen zur dynamischen Pfadauswahl als Wert für das Interface verwendet.

SNMP-ID:

2.110.4.18.3

Pfad Konsole:

Setup > **Firewall** > **Dynamische-Pfadauswahl** > **Richtlinien-Zuweisungs-Ausnahmen**

Mögliche Werte:

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

LB-Policy

Definiert die Dynamic Path Selection Policy, die für diese Firewall Regel verwendet wird.

SNMP-ID:

2.8.10.2.16

Pfad Konsole:

Setup > **IP-Router** > **Firewall** > **Regel-Tabelle**

Mögliche Werte:

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

Default-Wert:

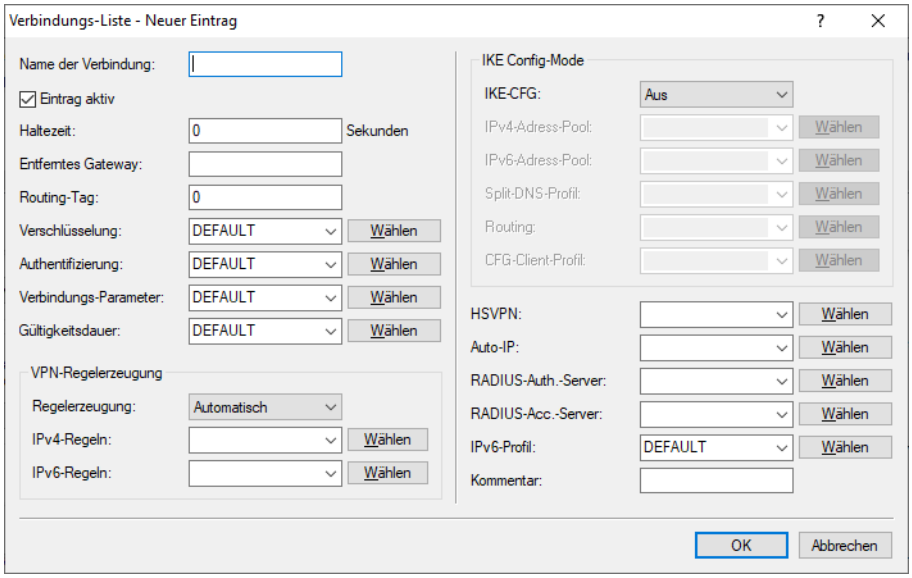
leer

3 Virtual Private Networks – VPN

3.1 IKEv2 Auto-IP

Mittels des Auto-IP-Parameters kann eine VPN-Zentrale einer VPN-Filiale die IP-Adresse für das Messziel der Dynamic Path Selection übermitteln. Dazu wird auf der Zentrale der Parameter Auto-IP konfiguriert. Auf der Filiale sind dann als (IPv4-)Messziel„ 0.0.0.0“ bzw. als IPv6-Messziel „::“ einzutragen, damit die Filiale das Messziel automatisch von der Zentrale übernimmt.

Die Referenz auf das Auto-IP-Profil tragen Sie unter **VPN** > **IKEv2/IPSec** > **Verbindungsliste** ein.

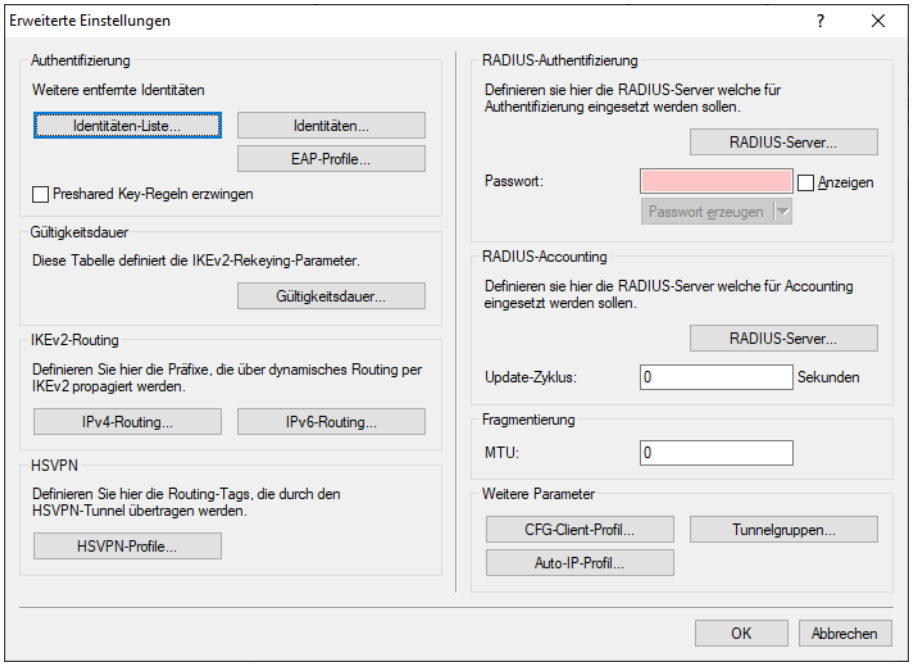


Auto-IP

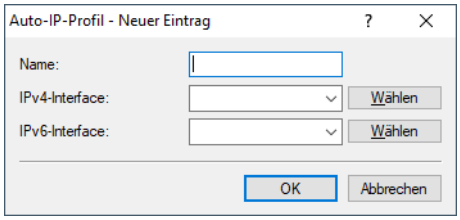
Mittels des Auto-IP-Parameters kann eine VPN-Zentrale einer VPN-Filiale die IP-Adresse für das Messziel der *Dynamic Path Selection* übermitteln. Dazu wird auf der Zentrale der Parameter Auto-IP konfiguriert. Auf der Filiale muss dann als (IPv4-)Messziel 0.0.0.0 bzw. als IPv6-Messziel :: eingetragen werden, damit die Filiale das Messziel automatisch von der Zentrale übernimmt.

Verweist auf das entsprechende Auto-IP-Profil, welches Sie unter *IKEv2-Auto-IP-Profil* auf Seite 24 einrichten.

Wechseln Sie zur Konfiguration des Auto-IP-Profils in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** und konfigurieren Sie im Abschnitt **Weitere Parameter** das **Auto-IP-Profil**.



3.1.1 IKEv2-Auto-IP-Profil



Name

Eindeutiger Name des Auto-IP-Profils.

IPv4-Interface

IPv4-Netzwerkname von dem die IPv4-Adresse an die VPN-Gegenseite für das Dynamic-Path-Selection-Messziel übermittelt werden soll.

Mögliche Werte: IPv4-Netzwerke

IPv6-Interface

IPv6-Interfacename, von dem die IPv6-Adresse an die VPN-Gegenseite für das Dynamic-Path-Selection-Messziel übermittelt werden soll.

Mögliche Werte: IPv6-LAN-Interfaces

3.1.2 Ergänzungen im Setup-Menü

Auto-IP-Profil

Mittels des Auto-IP-Parameters kann eine VPN-Zentrale einer VPN-Filiale die IP-Adresse für das Messziel der Dynamic Path Selection übermitteln. Dazu wird auf der Zentrale der Parameter Auto-IP konfiguriert. Auf der Filiale sind dann als

(IPv4-)Messziel„ 0.0.0.0“ bzw. als IPv6-Messziel „::“ einzutragen, damit die Filiale das Messziel automatisch von der Zentrale übernimmt.

Tragen Sie hier eine Referenz auf ein Auto-IP-Profil (siehe *2.19.36.16 Auto-IP-Profile* auf Seite 25) ein.

SNMP-ID:

2.19.36.1.25

Pfad Konsole:

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

Mögliche Werte:

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

Auto-IP-Profile

In dieser Tabelle werden die Auto-IP-Profile konfiguriert.

SNMP-ID:

2.19.36.16

Pfad Konsole:

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

Name

Vergeben Sie einen Namen für das Auto-IP-Profil. Dieser wird unter *2.19.36.1.25 Auto-IP-Profil* auf Seite 24 referenziert.

SNMP-ID:

2.19.36.16.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auto-IP-Profile**

Mögliche Werte:

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

IPv4-Interface

IPv4-Netzwerkname von dem die IPv4-Adresse an die VPN-Gegenseite für das Dynamic-Path-Selection-Messziel übermittelt werden soll.

Mögliche Werte: IPv4-Netzwerke

SNMP-ID:

2.19.36.16.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auto-IP-Profile**

Mögliche Werte:

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

IPv6-Interface

IPv6-Interfacename, von dem die IPv6-Adresse an die VPN-Gegenseite für das Dynamic-Path-Selection-Messziel übermittelt werden soll.

Mögliche Werte: IPv6-LAN-Interfaces

SNMP-ID:

2.19.36.16.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Auto-IP-Profile**

Mögliche Werte:

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

3.2 IPv6-Adressbereich für die VPN-Verhandlung steuerbar

Ab LCOS 10.42 können Sie den IPv6-Adressbereich für die VPN-Verhandlung über die Kommandozeile steuern.

3.2.1 Ergänzungen im Setup-Menü

Quell-Adressen-Filter

Definiert das IPv6-Präfix, mit dem keine VPN-Verbindungen aufgebaut werden sollen. Wird beispielsweise von einem vorgeschalteten Router nur eine Unique Local Address (ULA) aus dem Präfix „fc00::/7“ an das Gerät vergeben, so kann verhindert werden, dass das Gerät mit einer Absende-Adresse aus diesem Präfix eine VPN-Verbindung zu einer globalen IPv6-Adresse aufbaut. Dies kann mit der alternativen Gateway-Liste kombiniert werden, in der eine IPv4-Adresse als alternatives Gateway steht und dann verwendet wird.

Eingabewert: IPv6 Präfix, z. B. „fc00::/7“.

SNMP-ID:

2.19.36.34

Pfad Konsole:

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

Mögliche Werte:

Max. 253 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

4 Wireless LAN – WLAN

4.1 Entfall der WPA-Standard-Passphrase

Bisher war im LCOS standardmäßig eine WPA-Passphrase bestehend aus „L“ und der LAN-MAC-Adresse voreingestellt. Ab LCOS 10.42 wird diese voreingestellte WLAN-Passphrase entfallen. Es ist nun immer eine sichere, benutzerdefinierte Passphrase zu konfigurieren. Wenn keine Passphrase konfiguriert ist, obwohl für den gewählten Verschlüsselungsmodus eine Passphrase benötigt wird (WEP, WPA2/3-PSK), geht das WLAN nicht in Betrieb. Im Syslog wird auf den Umstand hingewiesen, dass keine Passphrase gesetzt ist, obwohl diese benötigt wird.

4.2 RTLS (Real-Time Location System)

Unter RTLS versteht man die Möglichkeit zur Echtzeit-Lokalisierung eines Geräts. Dieses Gerät ist ein spezieller WLAN-Sender, der speziell kodierte WLAN-Pakete aussendet. Die Access Points in der Umgebung empfangen diese Pakete und leiten sie mit weiteren Daten an das verwendete System zur Echtzeit-Lokalisierung. Dadurch kann der Aufenthaltsort des WLAN-Senders genau bestimmt werden. Implizit erhält man dann den Aufenthaltsort von Gegenständen und Personen, die diesen WLAN-Sender tragen.

Ab LCOS 10.42 wird als RTLS-System neben dem schon länger unterstützten AiRISTA Flow Blink Modus (vormals Ekahau Blink Modus) nun auch das System Stanley AeroScout RTLS unterstützt. Alle aktuellen LANCOM WLAN-Geräte mit LCOS 10.42 außer dem LANCOM IAP-1781VAW können verwendet werden.

4.2.1 Stanley AeroScout RTLS

Das AeroScout RTLS-System ermöglicht u.a. Asset Management, Umgebungsmonitoring und Staff Workflow mittels spezieller via WLAN angebundener Sensoren und „Tags“. Mittels dieses Features ist die Weiterleitung der speziell kodierten WLAN-Pakete der AeroScout-Tags über eine LANCOM WLAN-Infrastruktur an die AeroScout Location Engine möglich.

Folgende Betriebsarten werden unterstützt:

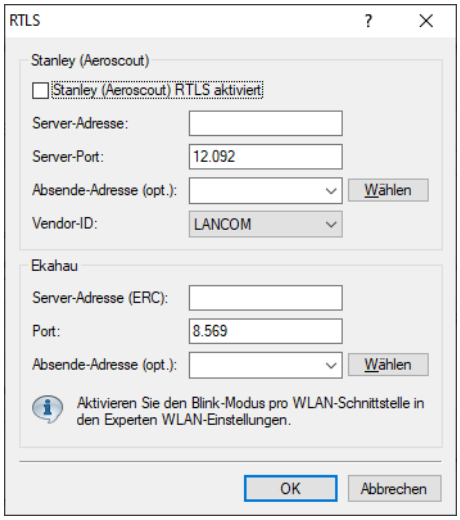
- Weiterleiten von AeroScout Tag Messages

  Es wird der WDS-Modus unterstützt. Achten Sie darauf, dass die Tags im AeroScout-System für den WDS-Modus konfiguriert sind. Der IBSS-Modus wird nicht unterstützt.

- Wi-Fi Client Reports

Stanley AeroScout RTLS konfigurieren

Um den Zugriff auf den Stanley AeroScout RTLS-Server mit LANconfig zu konfigurieren, öffnen Sie die Ansicht **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **RTLS** und konfigurieren Sie im Bereich **Stanley (AeroScout)**.



Stanley (AeroScout) RTLS aktiviert

Aktivieren Sie diese Option, um die Weiterleitung an die Aeroscout Location Engine einzuschalten.

Dieses Feature wird immer für alle WLAN-Module eines Access Points eingeschaltet.

Server-Adresse

Konfigurieren Sie hier die IP-Adresse der Aeroscout Location Engine.

Server-Port

Konfigurieren Sie bei Abweichungen vom Standardwert den Server-Port der Aeroscout Location Engine.

Absende-Adresse (optional)

Konfigurieren Sie optional das Absende-Netzwerk für die Verbindung zur AeroScout Location Engine. Dies ist nur dann erforderlich, wenn mehrere ARF-Netzwerke konfiguriert sind.

Vendor-ID

Konfigurieren Sie hier die Vendor-ID, die der Access Point an die Aeroscout Location Engine meldet. Sollte Ihre Version der AeroScout Location Engine noch nicht die dedizierte LANCOM-Vendor-ID unterstützen, ist hier ein Umschalten auf die Vendor-ID „Motorola“ möglich.

4.2.2 Ergänzungen im Setup-Menü

RTLS

Dieses Menü enthält die Einstellungen zur Kommunikation mit einem RTLS-Server.

SNMP-ID:

2.12.131

Pfad Konsole:

Setup > **WLAN**

Ekahau

Dieses Menü enthält die Einstellungen zum AiRISTA Flow Blink Modus (vormals Ekahau Blink Modus).

SNMP-ID:

2.12.131.4

Pfad Konsole:

Setup > **WLAN** > **RTLS**

Server-Adresse

Enthält die IP-Adresse oder den Hostnamen des RTLS-Servers.

SNMP-ID:

2.12.131.4.1

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **Ekahau**

Mögliche Werte:

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

Default-Wert:

leer

Server-Port

Enthält die UDP-Portnummer des RTLS-Servers.

SNMP-ID:

2.12.131.4.2

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **Ekahau**

Mögliche Werte:

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

Default-Wert:

8569

Loopback-Adresse

Enthält die optionale Absende-Adresse, welche das Gerät anstatt der automatisch für das Ziel gewählten Absende-Adresse verwendet.

SNMP-ID:

2.12.131.4.3

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **Ekahau**

Mögliche Werte:

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

Besondere Werte:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll

"INT"

für die Adresse des ersten Intranets

"DMZ"

für die Adresse der ersten DMZ

LB0 bis LBF

für die 16 Loopback-Adressen

Beliebige gültige IP-Adresse

Default-Wert:

leer

AeroScout

Dieses Menü enthält die Einstellungen des Stanley AeroScout RTLS.

SNMP-ID:

2.12.131.5

Pfad Konsole:

Setup > **WLAN** > **RTLS**

Server-Adresse

Enthält die IP-Adresse oder den Hostnamen des RTLS-Servers.

SNMP-ID:

2.12.131.5.1

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **AeroScout**

Mögliche Werte:

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

Default-Wert:

leer

Server-Port

Enthält den Server-Port der AeroScout Location Engine.

SNMP-ID:

2.12.131.5.2

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **AeroScout**

Mögliche Werte:

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

Default-Wert:

12092

Loopback-Adresse

Enthält die optionale Absende-Adresse, welche das Gerät anstatt der automatisch für das Ziel gewählten Absende-Adresse verwendet.

SNMP-ID:

2.12.131.5.3

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **AeroScout**

Mögliche Werte:

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

Besondere Werte:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll

"INT"

für die Adresse des ersten Intranets

"DMZ"

für die Adresse der ersten DMZ

LB0 bis LBF

für die 16 Loopback-Adressen

Beliebige gültige IP-Adresse

Default-Wert:

leer

Aktiv

Aktivieren Sie hier die Weiterleitung an die Aeroscout Location Engine.

SNMP-ID:

2.12.131.5.4

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **AeroScout**

Mögliche Werte:

Ja

Weiterleitung aktiviert.

Nein

Default-Wert:

Nein

Vendor-ID

Konfigurieren Sie hier die Vendor-ID, die der Access Point an die AeroScout Location Engine meldet. Sollte Ihre Version der Aeroscout Location Engine noch nicht die dedizierte LANCOM-Vendor-ID unterstützen, ist hier ein Umschalten auf die Vendor-ID „Motorola" möglich.

SNMP-ID:

2.12.131.5.5

Pfad Konsole:

Setup > **WLAN** > **RTLS** > **AeroScout**

Mögliche Werte:

Motorola
LANCOM

Default-Wert:

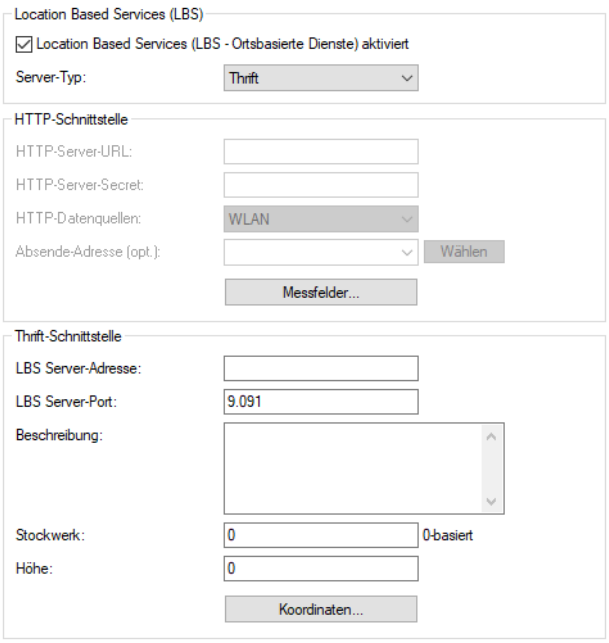
LANCOM

4.3 Location Based Services (LBS)

Die LANCOM Access Points können als LBS-Client mit einem LBS-Server zusammen arbeiten. Dann melden Sie an den LBS-Server alle verbundenen Clients, sodass der LBS-Server entsprechend diesen Clients ortsbasierte Dienste anbieten kann. Unterstützt werden ab LCOS 10.42 eine HTTP-Schnittstelle und eine schon länger unterstützte Thrift-Schnittstelle.

Mittels der HTTP-Schnittstelle können Access Points LBS-Daten direkt an einen frei konfigurierbaren HTTP-Endpunkt senden. Da die Daten im JSON-Format vorliegen, wird eine einfache Verarbeitung auf der Empfängerseite sichergestellt.

LANconfig: **Sonstige Dienste** > **Dienste** > **Location Based Services (LBS)**



Location Based Services (LBS – Ortsbasierte Dienste) aktiviert

Aktiviert oder deaktiviert die ortsbasierenden Dienste.

Server-Typ

Konfigurieren Sie hier, ob die HTTP-Schnittstelle oder die Thrift-Schnittstelle verwendet werden soll.

4.3.1 HTTP-Schnittstelle

Mittels der HTTP-API können Access Points LBS-Daten direkt an einen frei konfigurierbaren HTTP-Endpunkt senden. Da die Daten im JSON-Format vorliegen, wird eine einfache Verarbeitung auf der Empfängerseite sichergestellt.

HTTP Server-URL

Konfigurieren Sie hier die URL des HTTP-Endpunkts.

Es werden HTTP und HTTPS unterstützt. Bei der Verwendung von HTTPS kann entweder keine Zertifikatsprüfung, eine Prüfung des Server-Zertifikat oder eine beidseite Prüfung mit Server- und Client-Authentisierung stattfinden. Dazu kann ein PKCS#12-Container mit CA- und Client-Zertifikat auf das Gerät hochgeladen werden, der das CA-Zertifikat oder das CA- und Client-Zertifikat enthält.

Dies kann über LANconfig oder WEBconfig erfolgen.Wird kein PKCS#12-Container hochgeladen, wird bei Verwendung von HTTPS keine Zertifikatsprüfung durchgeführt.

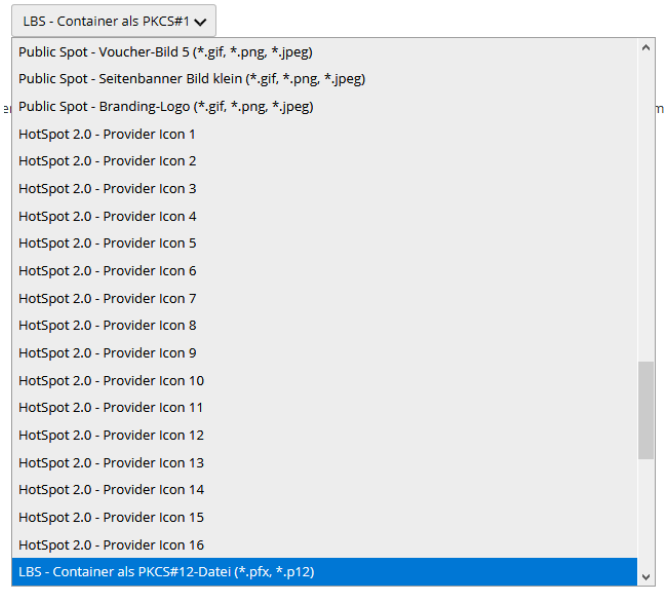


Abbildung 1: Screenshot WEBconfig

HTTP-Server-Secret

Das HTTP-Server-Secret wird in den JSON-Nachrichten des Access Points zum Endpunkt übertragen und kann dazu dienen, die Nachrichten zusätzlich zu authentifizieren.

HTTP-Datenquellen

Konfigurieren Sie hier, ob WLAN-, BLE- oder beide Arten von LBS-Daten gesendet werden sollen.

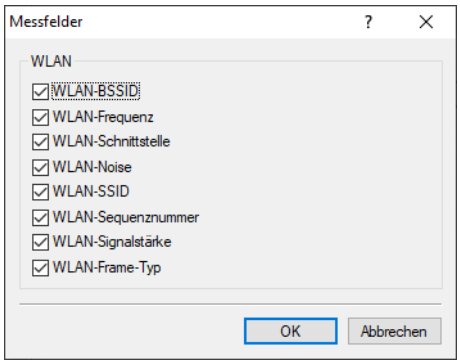
Die Einstellung **BLE** ist nur bei Geräten mit mit verbautem BLE-Modul unterstützt. Dies sind aktuell LN-1700B, LN-1702B, LN-1700UE, OAP-1700B und OAP-1702B.

Absende-Adresse

Konfigurieren Sie hier, welche Absendeadresse für die Kommunikation mit dem HTTP-Endpunkt verwendet werden soll. Dies kann erforderlich sein, wenn auf dem Gerät mehrere IP-Netzwerke konfiguriert sind.

Messfelder

Konfigurieren Sie hier im Detail, welche Messfelder bzw. vom Access Point ermittelten Daten in den Nachrichten an den HTTP-Endpunkt enthalten sein sollen. Es empfiehlt sich, diese auf den tatsächlich benötigten Umfang anzupassen, um das Datenaufkommen gering zu halten.



Datenformat der an den Endpunkt gesendeten Nachrichten

› Für **WLAN**:

```
{
  "version": "1.0",
  "secret": "geheim",
  "type": "WLAN",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "clientMac": "334455667788",
      "seenTime": 1579792598996,
      "frameSeqNum": 1074,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -56,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    },
    {
      "clientMac": "554433aabbcc",
      "seenTime": 1579792601334,
      "frameSeqNum": 2742,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -45,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    }
  ]
}
```

version

Die Version der verwendeten API. Aktuell ist dies immer 1.0.

secret

Das in der Konfiguration des Access Points festgelegte HTTP-Server-Secret.

type

Der Typ der gesendeten Daten. Kann entweder WLAN oder BLE sein.

deviceMac

Die LAN-MAC-Adresse des Access Points.

measurements

Hierin ist mindestens ein Messwert enthalten. Es können aber auch mehrere enthalten sein.

clientMac

Die MAC-Adresse des WLAN-Clients.

seenTime

Der Zeitstempel (in Unix-Zeit), zu dem der WLAN-Frame vom Client am Access Point empfangen wurde.

frameSeqNum

Die Sequenznummer des empfangenen WLAN-Frames.

ssid

Die im WLAN-Frame enthaltene SSID, sofern vorhanden.

module

Beschreibt, von welcher WLAN-Schnittstelle des Access Points der WLAN-Frame empfangen wurde. Typischerweise 0 für die erste WLAN-Schnittstelle oder 2 für die zweite WLAN-Schnittstelle.

bssid

Die im WLAN-Frame enthaltene BSSID.

rssi

Die Signalstärke in dBm des empfangenen WLAN-Frames.

frequency

Die Frequenz in MHz des WLAN-Kanals, auf dem der WLAN-Frame empfangen wurde.

noise

Der Rauschpegel in dBm auf dem Kanal, auf dem der WLAN-Frame empfangen wurde.

frameType

Der Frame-Typ des empfangenen WLAN-Frame. Folgende Typen sind möglich: `PROBE`, `AUTHENTICATION`, `ASSOCIATION`, `DEAUTHENTICATION` oder `DEASSOCIATION`.

› Für **BLE**:

```
{
  "version": "1.0",
  "secret": "geheim",
  "type": "BLE",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "deviceAddress": "001122334455",
      "seenTime": 1579792601269,
      "addressType": "Random",
      "rssi": -77
    },
    {
      "deviceAddress": "ffeeddccbbaa",
      "seenTime": 1579792601273,
      "addressType": "Random",
      "rssi": -61
      "name": "test",
      "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
      "scanResponseData": "050974657374"
    }
  ]
}
```

version

Die Version der verwendeten API. Aktuell ist dies immer 1.0.

secret

Das in der Konfiguration des AP festgelegte HTTP-Server-Secret.

type

Der Typ der gesendeten Daten. Kann entweder WLAN oder BLE sein.

deviceMac

Die LAN-MAC-Adresse des AP.

measurements

Hierin ist mindestens ein Messwert enthalten. Es können aber auch mehrere enthalten sein.

deviceAddress

Die Adresse des BLE-Gerätes bzw. -Clients.

seenTime

Der Zeitstempel (in Unix-Zeit), zu dem der BLE-Frame vom Client am AP empfangen wurde.

addressType

Der BLE-Adresstyp. Folgende Adresstypen sind möglich: `Public` oder `Random`.

rssi

Die Signalstärke in dBm des empfangenen BLE-Frames.

name

Der vom BLE-Gerät übermittelte Name. Kann nur übermittelt werden, wenn der aktive BLE-Scan in den BLE-Betriebseinstellungen aktiviert ist.

advertisingData

Das komplette vom BLE-Gerät übermittelte Advertisement.

scanResponseData

Die komplette vom BLE-Gerät übermittelte Scan-Response. Kann nur übermittelt werden, wenn der aktive BLE-Scan in den BLE-Betriebseinstellungen aktiviert ist.

4.3.2 Ergänzungen im Setup-Menü

LBS-Server-Typ

Konfigurieren Sie hier, ob die HTTP-API mit Datenpaketen im JSON-Format oder die Thrift-API verwendet werden soll.

SNMP-ID:

2.100.17

Pfad Konsole:

Setup > LBS

Mögliche Werte:

Apache-Thrift
HTTP-JSON

HTTP-Server

Hier bestimmen Sie die Einstellungen des HTTP-Servers bei Verwendung der HTTP-API.

SNMP-ID:

2.100.18

Pfad Konsole:

Setup > **LBS**

URL

Konfigurieren Sie hier die URL des HTTP-Endpunkts.

Es werden HTTP und HTTPS unterstützt. Bei der Verwendung von HTTPS muss zusätzlich ein PKCS#12-Container mit CA- und Client-Zertifikat auf das Gerät hochgeladen werden. Dies kann über LANconfig oder WEBconfig erfolgen.

SNMP-ID:

2.100.18.1

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

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

Loopback-Adresse

Konfigurieren Sie hier, welche Absendeadresse für die Kommunikation mit dem HTTP-Endpunkt verwendet werden soll. Dies kann erforderlich sein, wenn auf dem Gerät mehrere IP-Netzwerke konfiguriert sind.

SNMP-ID:

2.100.18.2

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

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

Secret

Das HTTP-Server-Secret wird in den JSON-Nachrichten des Access Points zum Endpunkt übertragen und kann dazu dienen, die Nachrichten zusätzlich zu authentifizieren.

SNMP-ID:

2.100.18.3

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

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

Datenquellen

Konfigurieren Sie hier, ob WLAN-, BLE- oder beide Arten von LBS-Daten gesendet werden sollen.

Die Einstellung **BLE** ist nur bei Geräten mit verbautem BLE-Modul unterstützt.

SNMP-ID:

2.100.18.4

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

WLAN
BLE

5 WLAN-Management

5.1 Konfiguration von Passpoint® Release 2 über den WLAN-Controller

Ab LCOS 10.42 können Sie das mit LCOS 10.32 RU4 eingeführte Passpoint® Release 2 auch über den WLAN-Controller konfigurieren.

Die Einstellungen hierzu finden Sie in LANconfig unter **WLAN-Controller** > **802.11u** > **Hotspot 2.0 Profile** bzw. unter **WLAN-Controller** > **802.11u** > **OSU-Anbieter**.

Die Konfiguration entspricht der unter **Wireless-LAN** > **802.11u** > **Hotspot 2.0** bereits beschriebenen Funktionalität.

Die Verteilung der Dateiem wie z. B. der Icons für die OSU-Provider erfolgt noch nicht automatisiert. Diese müssen auf jedem Access Point einzeln zur Verfügung gestellt werden.

5.1.1 Ergänzungen im Setup-Menü

Hotspot2.0-Release

Stellen Sie das in diesem Profil unterstützte Release von Hotspot 2.0 ein.

Ein Client muss das entsprechende Release beherrschen, um sich verbinden zu können.

SNMP-ID:

2.37.1.17.3.5

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot-2.0-Profile**

Mögliche Werte:

Release-1
Release-2

Domain-Id

Die Domain-ID gibt an, welcher ANQP-Server verwendet wird. Alle Access Points bzw. SSIDs mit gleicher Nummer / Domain-ID (16-Bit Wert) verwenden den gleichen ANQP-Server.

Ein Client würde somit auf eine ANQP-Anfrage auf Access Points / SSIDs mit identischer Domain-ID immer die gleiche Antwort erhalten. Um unterschiedliche Antworten zu erhalten, müsste der Client nach unterschiedlichen Domain-IDs Ausschau halten.

SNMP-ID:

2.37.1.17.3.6

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot-2.0-Profile**

Mögliche Werte:

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

Default-Wert:

0

OSU-Netzwerkname

Name der SSID, die Zugang zum OSU-Server bietet.

SNMP-ID:

2.37.1.17.3.7

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot-2.0-Profile**

Mögliche Werte:

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

Default-Wert:

leer

OSU-Providers

Liste der OSU-Providernamen aus *2.37.1.17.12 OSU-Providers* auf Seite 42, die im Profil unterstützt werden.

SNMP-ID:

2.37.1.17.3.8

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot-2.0-Profile**

Mögliche Werte:

max. 250 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

OSU-Providers

In dieser Tabelle konfigurieren Sie die OSU-Provider für Online Sign-Up bei Passpoint® Release 2.

SNMP-ID:

2.37.1.17.12

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

Name

Geben Sie diesem OSU-Provider einen Namen, über den Sie ihn später referenzieren können. Wenn der gleiche Name erneut verwendet wird, dann kann dieser Provider z. B. für mehrere Spachen verwendet werden.

SNMP-ID:

2.37.1.17.12.1

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

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

Sprache

Stellen Sie die von diesem OSU-Provider unterstützte Sprache ein.

SNMP-ID:

2.37.1.17.12.2

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

Keine
Englisch
Deutsch
Chinesisch
Spanisch
Franzoesisch
Italienisch
Russisch
Niederlaendisch
Tuerkisch
Portugiesisch
Polnisch
Tschechisch
Arabisch
Koreanisch

Friendly-Name

Geben Sie diesem OSU-Provider einen sprechenden Namen.

SNMP-ID:

2.37.1.17.12.3

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

max. 250 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

OSU-Methoden

Stellen Sie hier die von diesem OSU-Provider verwendeten OSU-Methoden ein. Siehe auch *2.71.7.11 OSU-Methoden*. Möglich sind „OMA-DM“ oder „SOAP-XML-SPP“.

SNMP-ID:

2.37.1.17.12.4

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

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

URI

Geben Sie eine URI ein, unter der ein Client den OSU-Server erreicht.

SNMP-ID:

2.37.1.17.12.5

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

NAI

Geben Sie den Network Access Identifier (NAI) für diesen OSU-Provider ein.

SNMP-ID:

2.37.1.17.12.6

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

max. 65 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Dienst-Beschreibung

Geben Sie hier einen Beschreibungstext für diesen Dienst ein.

SNMP-ID:

2.37.1.17.12.7

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

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

Icon-Dateiname

Wählen Sie ein Icon für diesen OSU-Provider aus. Die Icons können über die WEBconfig im Bereich **Dateimanagement** als Datei hochgeladen werden. Als Dateiformat empfehlen wir PNG.

SNMP-ID:

2.37.1.17.12.8

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

Mögliche Werte:

keines
OSU-Prov-Img-1
OSU-Prov-Img-2
OSU-Prov-Img-3
OSU-Prov-Img-4
OSU-Prov-Img-5
OSU-Prov-Img-6
OSU-Prov-Img-7
OSU-Prov-Img-8
OSU-Prov-Img-9
OSU-Prov-Img-10
OSU-Prov-Img-11
OSU-Prov-Img-12
OSU-Prov-Img-13
OSU-Prov-Img-14
OSU-Prov-Img-15
OSU-Prov-Img-16

Icon-Language

Stellen Sie hier die Sprache des ausgewählten Icons ein.

SNMP-ID:

2.37.1.17.12.9

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **OSU-Providers**

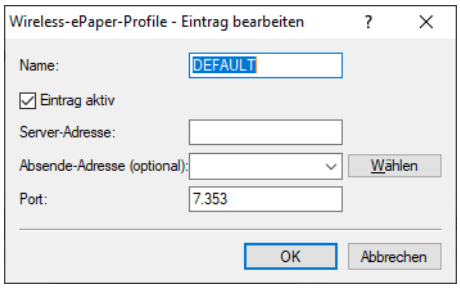
Mögliche Werte:

Keine
Englisch
Deutsch
Chinesisch
Spanisch
Franzoesisch
Italienisch
Russisch
Niederlaendisch
Tuerkisch
Portugiesisch
Polnisch
Tschechisch
Arabisch
Koreanisch

5.2 Erweiterung der Wireless ePaper-Profile

Ab LCOS 10.42 können Sie die mit LCOS 10.40 eingeführte Erweiterung des TCP-Protokolls, welches den Verbindungsaufbau (Wireless ePaper Access Point bzw. Router mit USB-Schnittstelle und Wireless ePaper USB-Stick) zum Wireless ePaper Server zulässt und die Verbindung mittels TLS verschlüsselt, auch über einen WLAN-Controller einstellen.

Die Einstellungen hierzu finden Sie in LANconfig unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** > **Wireless-ePaper-Profile**



5.2.1 Ergänzungen im Setup-Menü

Outbound-Server

IP-Adresse des Wireless ePaper Servers.

SNMP-ID:

2.37.1.23.4

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-ePaper-Profile**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9].-:%`

Loopback-Adresse

Geben Sie hier die Loopback-Adresse an.

SNMP-ID:

2.37.1.23.5

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-ePaper-Profile**

Mögliche Werte:

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

Default-Wert:

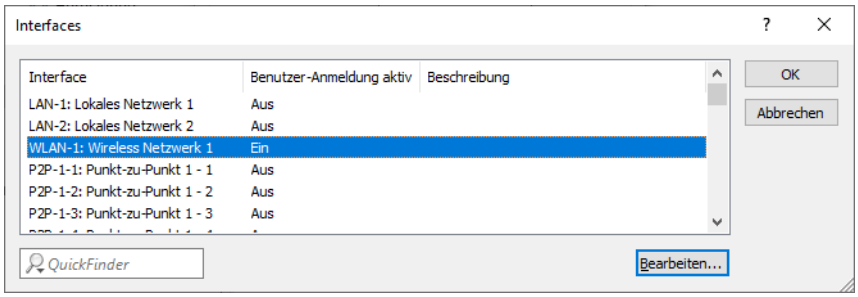
leer

6 Public Spot

6.1 Erweiterung der Public-Spot Port-Tabelle für die LANCOM Management Cloud

Ab LCOS 10.42 gibt es ein neues Feld **Beschreibung** in der Port-Tabelle, welches entweder für eine individuelle Beschreibung genutzt werden kann oder durch die LANCOM Management Cloud für das Cloud-managed Hotspot-Feature verwendet wird.

Die Port-Tabelle finden Sie in LANconfig unter **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**



6.1.1 Ergänzungen im Setup-Menü

Beschreibung

Feld für eine Beschreibung des Ports. Dieses Feld wird ebenfalls für das Cloud-managed Hotspot-Feature der LANCOM Management Cloud als eindeutiger Bezeichner des benutzen Hotspots verwendet. In diesem Fall wird durch die LANCOM Management Cloud hier eine UUID hinterlegt.

SNMP-ID:

2.24.15.4

Pfad Konsole:

Setup > **Public-Spot-Modul** > **Port-Tabelle**

Mögliche Werte:

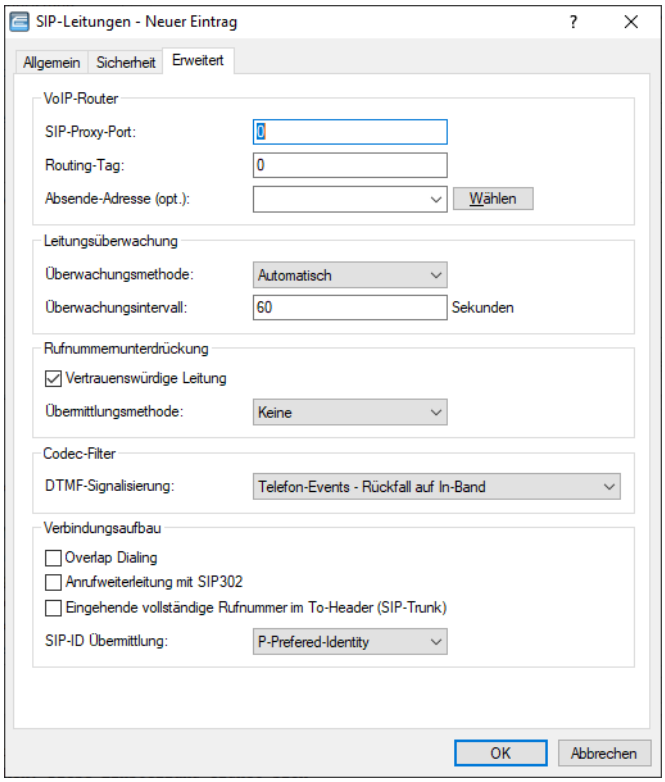
max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

7 Voice over IP – VoIP

7.1 Absende-Adresse für SIP- und SIP-PBX-Leitungen

Ab LCOS 10.42 kann die optionale Absendeadresse, die für jede angelegte SIP-Leitung das Interface spezifiziert, auch über LANconfig eingestellt werden. Dadurch wird die Bedienung und für den Support die Fehleranalyse vereinfacht.

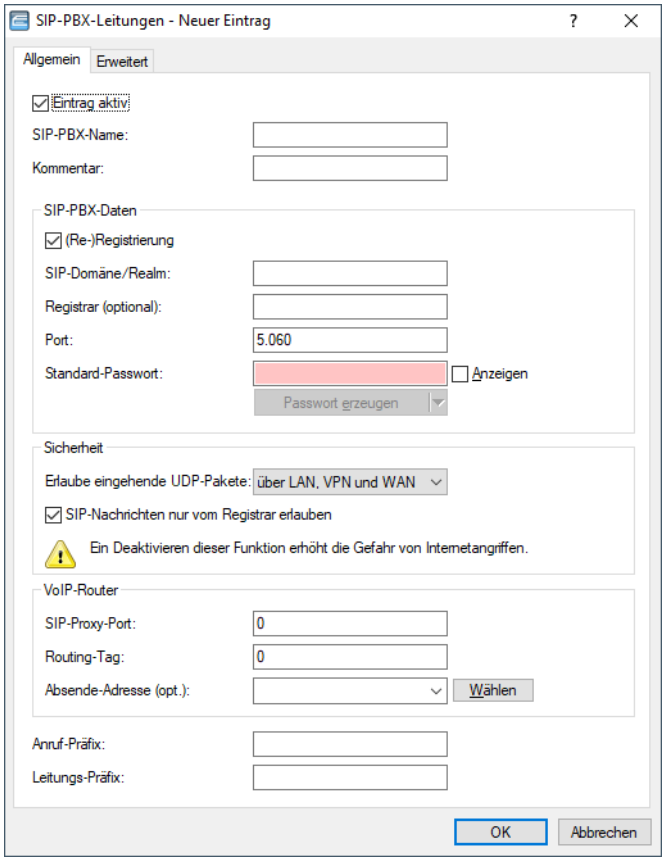
Sie finden die Option für SIP-Leitungen unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen** > **Erweitert**.



Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Sie finden die Option für SIP-PBX-Leitungen unter **Voice Call Manager** > **Leitungen** > **SIP-PBX-Leitungen** > **Allgemein**.



Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

7.2 SIP-ID-Übermittlung

Ab LCOS 10.42 gibt es weitere Möglichkeiten für die **SIP-ID-Übermittlung** unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen** > **Erweitert**.

SIP-ID Übermittlung

In diesem Feld kann eingestellt werden, wie die SIP-ID bei einem ausgehenden Telefonat bei Verwendung eines SIP-Trunks übertragen wird. Je nach Provider kann es erforderlich sein die SIP-ID über ein anderes Feld zu übertragen, da der Anruf ansonsten vom Provider abgelehnt wird.

Es können folgende Werte ausgewählt werden:

- P-Asserted-Identity (Standard-Wert)
- FROM
- Keine
- P-Prefered-Identity ohne DDI
- P-Prefered-Identity
- Keine – P-Prefered-Identity

› Keine – P-Asserted-Identity

Bei Auswahl der Option **P-Asserted-Identity** (PAI) wird die SIP-ID inklusive DDI über die PAI übertragen. Die Quellrufnummer wird über das FROM-Feld übertragen.

Bei Auswahl der Option **P-Prefered-Identity** (PPI) wird die SIP-ID inklusive DDI über die PPI übertragen. Die Quellrufnummer wird über das FROM-Feld übertragen.

Bei Auswahl der Option **FROM** wird die SIP-ID über das FROM-Feld übertragen. Die Quellrufnummer wird über die PPI / PAI übertragen.

Mit der Einstellung **Keine** wird die SIP-ID nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PPI / PAI übertragen.

Mit der Einstellung **P-Prefered-Identity ohne DDI** wird im Gegensatz zur P-Prefered-Identity eine eventuell vorhandene Durchwahl (DDI) nicht in der SIP-ID über die PPI übertragen.

Mit der Einstellung **Keine – P-Prefered-Identity** wird die SIP-ID nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PPI übertragen.

Mit der Einstellung **Keine – P-Asserted-Identity** wird die SIP-ID nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PAI übertragen.

Bei einem Einzel-Account wird die SIP-ID bei einem ausgehenden Anruf immer über das **FROM**-Feld signalisiert.

7.2.1 Ergänzungen im Setup-Menü

User-Id-Feld

Bestimmt das Feld, in dem die SIP-ID übertragen wird.

Bei einem Einzel-Account wird die SIP-ID bei einem ausgehenden Anruf immer über das FROM-Feld signalisiert.

SNMP-ID:

2.33.4.1.1.39

Pfad Konsole:

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

Mögliche Werte:

PPI

Die SIP-ID wird inklusive DDI über die PAI übertragen. Die Quellrufnummer wird über das FROM-Feld übertragen.

From

Die SIP-ID wird über das FROM-Feld übertragen. Die Quellrufnummer wird über die PPI / PAI übertragen.

Keine

Die SIP-ID wird nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PPI / PAI übertragen.

PPI-ohneDDI

Hier wird im Gegensatz zur P-Prefered-Identity eine eventuell vorhandene Durchwahl (DDI) nicht in der SIP-ID über die PPI übertragen.

PPI-PPI

Die SIP-ID wird inklusive DDI über die PPI übertragen. Die Quellrufnummer wird über das FROM-Feld übertragen.

Keine-PPI

Die SIP-ID wird nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PPI übertragen.

Keine-PAI

Die SIP-ID wird nicht übermittelt. Die erste Calling Number wird im FROM, die Zweite im PAI übertragen.

Default-Wert:

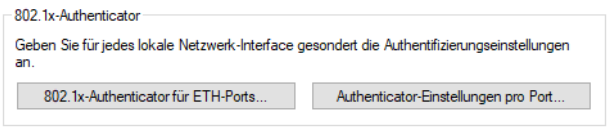
PPI

8 Weitere Dienste

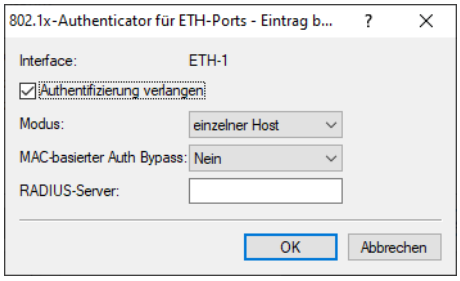
8.1 802.1X-Authenticator für Ethernet-Ports

Mittels des 802.1X-Authenticators können die an die Ethernet-Ports eines LANCOM Gerätes angeschlossenen Geräte mittels 802.1X authentifiziert werden. Dies kann dazu dienen, die Sicherheit vor ungefugtem Zugriff auf das Netzwerk auch im kabelgebundenen Bereich zu erhöhen.

In LANconfig konfigurieren Sie den 802.1X-Authenticator für Ethernet-Ports unter **Schnittstellen** > **LAN** im Abschnitt **802.1x-Authenticator**.



Die Konfiguration nehmen sie in der Tabelle **802.1x-Authenticator für ETH-Ports** vor. Das Interface wird hier jeweils vorgegeben und gibt die vorhandenen Ethernet-Ports an.



Authentifizierung verlangen

Mittels dieses Schalters legen Sie fest, ob für diesen Port eine 802.1X-Authentifizierung gefordert ist.

Modus

Mögliche Werte:

einzelner Host

Es kann an diesem Port nur ein Client die Authentifizierung durchlaufen und anschließend verwendet werden. Wenn an diesem Port ein weiterer Client mit einer eigenen MAC-Adresse erkannt wird, wird der Port in den unauthentifizierten Zustand zurück versetzt.

mehrere Hosts

Es können an diesem Port mehrere Clients (mit unterschiedlichen MAC-Adressen) verwendet werden. Die Authentifizierung muss nur einmalig durchgeführt werden. Dieser Modus bietet sich z. B. an, wenn an einem so konfigurierten Port ein WLAN Access Point betrieben wird und die Nutzdaten nicht zu einem zentralen Controller getunnelt werden. In diesem Fall würden ebenfalls Datenpakete der WLAN-Clients mit deren eigenen MAC-Adressen an dem so konfigurierten Ethernet-Port gesehen werden.

mehrere Authentifizierungen

An diesem Port können mehrere Clients eine jeweils eigene 802.1X-Authentifizierung durchlaufen.

MAC-basierter Auth-Bypass

Legt fest, ob nach dem erfolglosen Versuch, eine 802.1X-Verhandlung zu starten, die MAC-Adresse des Clients via RADIUS geprüft werden und anschließend der Port freigeschaltet werden soll. Die MAC-Adresse wird hierbei als RADIUS-Benutzername und -Passwort im Format „aabbccddeeff" übermittelt und muss auch so im RADIUS-Server hinterlegt werden.

Die MAC-Adresse ist leicht zu fälschen und bietet keinen Schutz vor böswilligen Angriffen.

In der Standardkonfiguration wird der 802.1X-Authenticator zuvor für 90 Sekunden versuchen, eine 802.1X-Verhandlung zu starten, bevor der Rückfall auf die MAC-Adress-Prüfung erfolgt. Dieser Zeitraum kann je Port durch das Ändern der Kommandozeilenparameter **Setup** > **IEEE802.1X** > **Ports** > **Max-Req** (Standard: 3 Versuche) sowie **Setup** > **IEEE802.1X** > **Ports** > **Supp-Timeout** (Standard: 30 Sekunden) angepasst werden. Alternativ kann für **MAC-basierter Auth-Bypass** der Modus „Unverzüglich" gesetzt werden. In diesem Modus wird sofort eine MAC-Adress-Prüfung gestartet, ohne einen Timeout abwarten zu müssen.

Mögliche Werte:

Nein

Die Authentifizierung über die MAC-Adresse ist nicht möglich.

Ja

Die Authentifizierung über die MAC-Adresse ist möglich.

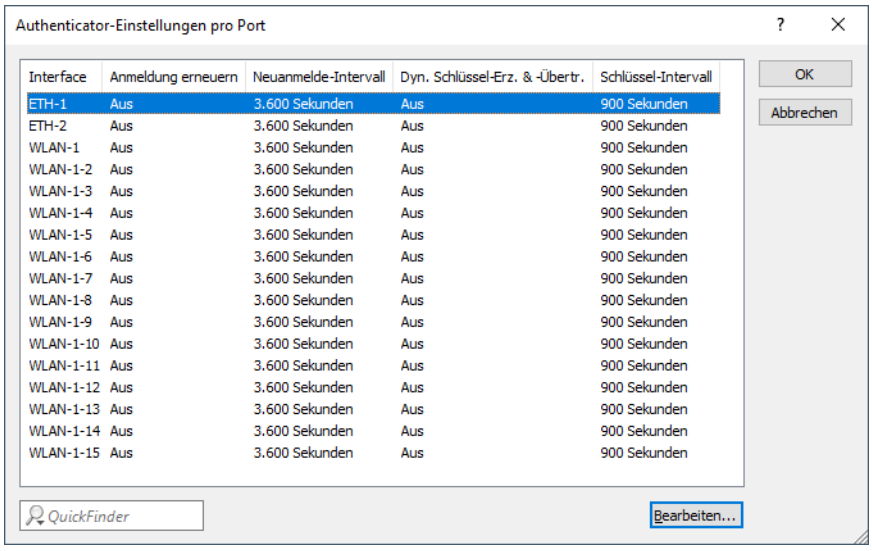
Unverzüglich

Die Authentifizierung wird sofort über die MAC-Adresse durchgeführt.

RADIUS-Server

Legt fest, welcher RADIUS-Server sowohl für 802.1X als auch für eine eventuelle MAC-Adress-Prüfung verwendet wird. Referenzieren Sie dazu einen der Einträge unter **Wireless-LAN** > **802.1X** > **Radius-Server** oder legen dort ggfs. einen neuen Eintrag an.

In der Tabelle **Authenticator-Einstellungen pro Port** stellen Sie die Anmeldeinformationen für die lokalen Netzwerkinterfaces ein.



Interface

Das Interface wird hier jeweils vorgegeben und gibt die vorhandenen Ethernet- und WLAN-Zugänge an.

Anmeldung erneuern

Hier aktivieren Sie die regelmäßige Neuanmeldung. Wird eine Neuanmeldung gestartet, so bleibt der Benutzer während der Verhandlung weiterhin angemeldet.

Neuanmelde-Intervall

Standardwert für das Neuanmelde-Intervall bei regelmäßiger Neuanmeldung ist 3.600 Sekunden.

Dyn. Schlüssel erzeugen und übertragen

Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

Schlüssel-Intervall

Standardwert für das Schlüssel-Intervall ist 900 Sekunden.

8.1.1 Ergänzungen im Setup-Menü

Authenticator-Ifc-Setup

Über dieses Menü nehmen Sie die Einstellung für die RADIUS-Authentifizierung (802.1X-Authentifizierung) von Clients vor, die sich über die LAN-Schnittstellen mit dem Gerät verbinden.

SNMP-ID:

2.4.10.3

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X**

Ifc

Name des Ports.

SNMP-ID:

2.4.10.3.1

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

In-Betrieb

Über diesen Parameter legen Sie fest, ob für diesen Port eine 802.1X-Authentifizierung gefordert ist.

SNMP-ID:

2.4.10.3.2

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Modus

Bestimmen Sie hier, ob sich ein oder mehrere Clients an dieser Schnittstelle über IEEE 802.1X anmelden dürfen.

SNMP-ID:

2.4.10.3.3

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Mögliche Werte:

Einzelner-Host

Es kann an diesem Port nur ein Client die Authentifizierung durchlaufen und anschließend verwendet werden. Wenn an diesem Port ein weiterer Client mit einer eigenen MAC-Adresse erkannt wird, wird der Port in den unauthentifizierten Zustand zurück versetzt.

Mehrfacher-Host

Es können an diesem Port mehrere Clients (mit unterschiedlichen MAC-Adressen) verwendet werden. Die Authentifizierung muss nur einmalig durchgeführt werden. Dieser Modus bietet sich z. B. an, wenn an einem so konfigurierten Port ein WLAN Access Point betrieben wird und die Nutzdaten nicht zu einem zentralen Controller getunnelt werden. In diesem Fall würden ebenfalls Datenpakete der WLAN-Clients mit deren eigenen MAC-Adressen an dem so konfigurierten Ethernet-Port gesehen werden.

Mehrfache-Auth.

An diesem Port können mehrere Clients eine jeweils eigene 802.1X-Authentifizierung durchlaufen.

Default-Wert:

Einzelner-Host

RADIUS-Server

Legt fest, welcher RADIUS-Server sowohl für 802.1X als auch für eine eventuelle MAC-Adress-Prüfung verwendet wird. Referenzieren Sie dazu einen der Einträge unter *2.30.3 Radius-Server* oder legen dort ggfs. einen neuen Eintrag an. Das Format der übermittelten MAC-Adresse können Sie unter *2.4.10.4 Benutzername-Attribut-Format* auf Seite 58 anpassen.

SNMP-ID:

2.4.10.3.4

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Mögliche Werte:

Name aus **Setup** > **IEEE802.1X** > **RADIUS-Server**

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

MAC-Auth.-Umgehung

Legt fest, ob nach dem erfolglosen Versuch, eine 802.1X-Verhandlung zu starten, die MAC-Adresse des Clients via RADIUS geprüft werden und anschließend der Port freigeschaltet werden soll. Die MAC-Adresse wird hierbei als RADIUS-Benutzername und -Passwort im Format „aabbccddeeff" übermittelt und muss auch so im RADIUS-Server hinterlegt werden.

Die MAC-Adresse ist leicht zu fälschen und bietet keinen Schutz vor böswilligen Angriffen.

In der Standardkonfiguration wird der 802.1X-Authenticator zuvor für 90 Sekunden versuchen, eine 802.1X-Verhandlung zu starten, bevor der Rückfall auf die MAC-Adress-Prüfung erfolgt. Dieser Zeitraum kann je Port durch das Ändern der Parameter *2.30.4.5 Max-Req* (Standard: 3 Versuche) sowie *2.30.4.7 Supp-Timeout* (Standard: 30 Sekunden) angepasst werden. Alternativ kann für MAC-Auth-Bypass der Modus „Sofort" gesetzt werden. In diesem Modus wird sofort eine MAC-Adress-Prüfung gestartet, ohne einen Timeout abwarten zu müssen.

SNMP-ID:

2.4.10.3.5

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Mögliche Werte:

nein

Die Authentifizierung über die MAC-Adresse ist nicht möglich.

ja

Die Authentifizierung über die MAC-Adresse ist möglich.

sofort

Die Authentifizierung wird sofort über die MAC-Adresse durchgeführt.

Default-Wert:

nein

Benutzername-Attribut-Format

Das Format der MAC-Adresse, die im Rahmen der MAC-Authentisierung an den RADIUS-Server übermittelt wird, ist hier konfigurierbar.

Die einzelnen Bytes der MAC-Adresse sind hier als Variablen %a bis %f repräsentiert. In der hier angegebenen Standardeinstellung werden die Bytes der MAC-Adresse nacheinander ausgegeben. Zusätzlich zu diesen Variablen können

beliebige vom LCOS unterstützte Zeichen hinzugefügt werden. Ein häufig verwendetes, weiteres Format für die MAC-Adresse „aabbcc-ddeeff" (mit „-" als Trennzeichen) ließe sich dementsprechend wie folgt konfigurieren: „%a%b%c-%d%e%f"

SNMP-ID:

2.4.10.4

Pfad Konsole:

Setup > **LAN** > **IEEE802.1X**

Mögliche Werte:

max. 30 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

%a%b%c%d%e%f