

A Addendum zur LCOS-Version 7.7

A.1 Übersicht

- 'Erweiterung des Temperaturbereichs für L-305/310' → Seite 1
- 'Standard-Verschlüsselung mit WPA2' → Seite 2
- 'APSD – Automatic Power Save Delivery' → Seite 2
- 'BFWA – mehr Sendeleistung für mehr Reichweite' → Seite 3
- 'RADIUS-Accounting neu starten' → Seite 4
- 'Voucher für Public-Spot mit Zeitbudget' → Seite 4
- 'Erweiterungen im RADIUS-Server' → Seite 9
- 'IGMP Snooping' → Seite 11
- 'TACACS+' → Seite 20
- 'Versand von Anhängen mit dem mailto-Kommando' → Seite 27
- 'Firmware-Upload für UMTS-Modul im LANCOM 1751 UMTS' → Seite 28
- 'Performance Monitoring im LANmonitor' → Seite 28
- 'Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor' → Seite 29

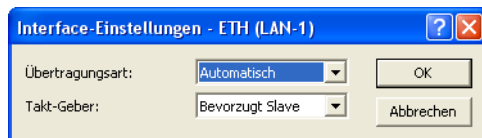
A.2 Erweiterung des Temperaturbereichs für L-305/310

In manchen Anwendungsfällen werden höhere Betriebstemperaturen benötigt als der standardmäßig definierte Temperaturbereich der Access Points LANCOM L-305agn und LANCOM L-310agn zulässt. Diese beiden Modelle können in einem erweiterten Temperaturbereich von bis zu 45° C betrieben werden, wenn die Geschwindigkeit der Gigabit-Ethernet-Schnittstelle auf 100 MBit/s begrenzt wird.

Ab der LCOS-Version 7.70 reduziert die automatische Einstellung der Schnittstellengeschwindigkeit die maximale Übertragungsrate auf 100 MBit/s, solange die standardmäßige Maximaltemperatur von 35° C überschritten wird. Da die erhöhten Temperaturen oft nur temporär (z.B. an besonders warmen Sommertagen) auftreten, resultieren aus der vorübergehenden Begrenzung der Übertragungsrate kaum Einschränkungen für den Betrieb der Geräte.

Die Einstellung der Übertragungsgeschwindigkeit für Ethernet-Ports finden Sie auf folgenden Pfaden:

LANconfig: Schnittstellen ► LAN ► Interface-Einstellungen



WEBconfig: LCOS-Menübaum ► Setup ► Schnittstellen

■ Übertragungsart

Wählen Sie hier aus, welche Übertragungsart Sie für die Verbindung zu Ihrem lokalen Netz verwenden.

Mögliche Werte:

- Automatisch, 10 MBit/s halbduplex, 10 MBit/s voll duplex, 100 MBit/s halbduplex, 100 MBit/s voll duplex, 100 MBit/s automatisch, 1000 MBit/s voll duplex. Das Angebot der möglichen Werte kann modellabhängig variieren.

Besondere Werte:

- In der Einstellung "Automatisch" wird die verwendete Übertragungsart passend zum verwendeten Anschluss automatisch ausgehandelt, dabei wird die maximal mögliche Übertragungsrate der beiden verbundenen Schnittstellen verwendet.
- Die Einstellung "100 MBit/s automatisch" entspricht der Einstellung "Automatisch", allerdings wird eine maximale Geschwindigkeit von 100 MBit/s ausgehandelt. Diese Einstellung ist im Zweifelsfall einer festen Einstellung auf 100 MBit/s vorzuziehen, da so mögliche Duplex-Konflikte verhindert werden können.

Default:

- Automatisch



Durch die manuelle Einstellung auf "100 MBit/s voll duplex" kann bei einigen Modellen mit Gigabit-Schnittstelle und Temperatursensor ein erweiterter Temperaturbereich genutzt werden. Bei diesen Modellen wird die Übertragungsart in der Einstellung "Automatisch" auf maximal 100 MBit/s begrenzt, solange die aktuelle

Temperatur des Gerätes einen gerätespezifischen Wert überschreitet. Sinkt die Temperatur wieder unter den Grenzwert, wird automatisch die höhere Übertragungsrate verwendet. Eine Unterbrechung aufgrund der Aushandlung der Übertragungsrate ist in den WLAN-Netzwerken (SSIDs) der Access Points nicht festzustellen. Weitere Informationen zu den zulässigen Temperaturbereichen finden Sie in den technischen Daten der Geräte.

A.3 Standard-Verschlüsselung mit WPA2

Im werksseitigen Auslieferungszustand bzw. nach einem Reset unterscheiden sich LANCOM Access Points und LANCOM Wireless Router.


- Unkonfigurierte Access Points können im Auslieferungszustand nicht über die WLAN-Schnittstelle in Betrieb genommen werden. Die WLAN-Module sind ausgeschaltet, die Geräte suchen selbstständig im LAN einen LANCOM WLAN Controller, von dem sie automatisch eine Konfiguration beziehen können.
- Unkonfigurierte Wireless Router können auch im Auslieferungszustand über die WLAN-Schnittstelle in Betrieb genommen werden. Dazu wird standardmäßig die hier beschriebene Standard-Verschlüsselung mit WPA-PSK verwendet.

Der Preshared Key für die Standard-WPA-Verschlüsselung setzt sich aus dem Anfangsbuchstaben „L“ gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibweise zusammen. Die LAN-MAC-Adressen der LANCOM-Geräte beginnen immer mit der Zeichenfolge „00A057“. Sie finden die LAN-MAC-Adresse auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie **nur** die als „LAN MAC address“ gekennzeichnete Nummer, die mit „00A057“ beginnt. Bei den anderen ggf. angegebenen Nummern handelt es sich **nicht** um die LAN-MAC-Adresse!



Für ein Gerät mit der LAN-MAC-Adresse „00A05713B178“ lautet der Preshared Key also „L00A05713B178“. Dieser Schlüssel ist in den 'WPA-/Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1/Passphrase' eingetragen.

Um mit einer WLAN-Karte eine Verbindung zu einem LANCOM Wireless Router im Auslieferungszustand herzustellen, muss in der WLAN-Karte die WPA-Verschlüsselung aktiviert und der 13-stellige Preshared Key eingetragen werden.

 Ändern Sie den Preshared Key für WPA nach der ersten Anmeldung, um eine sichere Verbindung zu gewährleisten.

A.4 APSD – Automatic Power Save Delivery

A.4.1 Einleitung

Beim Automatic Power Save Delivery (APSD) handelt es sich um eine Erweiterung des Standards IEEE 802.11e. APSD wird in zwei Varianten angeboten:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

Die beiden Verfahren unterscheiden sich u.a. in der Nutzung der Übertragungskanäle. LANCOM Access Points und Wireless Router unterstützen U-APSD, auf dem auch das von der WiFi als WMM Power Save oder kurz WMMPS zertifizierte Verfahren basiert.

U-APSD ermöglicht für WLAN-Geräte eine deutliche Stromeinsparung. Ein besonders großer Bedarf für diese Funktion entsteht durch die immer stärkere Nutzung von WLAN-fähigen Telefonen (Voice over WLAN – VoWLAN).

Mit der Aktivierung des U-APSD für ein WLAN können die WLAN-Geräte im Gesprächsbetrieb in einen "Schlummermodus" wechseln, während sie auf das nächste Datenpaket warten. Die VoIP-Datenübertragung erfolgt in einem festen zeitlichen Raster – die WLAN-Geräte synchronisieren ihre aktiven Phasen mit diesem Zyklus, so dass sie rechtzeitig vor dem Empfang des nächsten Pakets wieder bereit sind. Der Stromverbrauch wird dadurch deutlich reduziert, die Gesprächszeit der Akkus wird merklich erhöht.

Das genaue Verhalten des Stromsparmmodus wird zwischen Access Point und WLAN-Client ausgehandelt und wird dabei auf die spezifische Anwendung hin optimiert. APSD ist damit deutlich flexibler als das zuvor verwendete Stromsparverfahren, das in diesem Zusammenhang als "Legacy Power Save" bezeichnet wird.

A.4.2 Konfiguration

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Netzwerk

■ APSD

Aktiviert den Stromsparmmodus APSD für dieses logische WLAN-Netzwerk.

Mögliche Werte:

Ein, Aus

Default:

Aus



Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

A.4.3 Statistik

WEBconfig: LCOS-Menübaum ▶ Status ▶ WLAN ▶ Netzwerke

■ APSD

Zeigt an, ob APSD im jeweiligen WLAN (SSID) aktiv ist. APSD wird hier nur als aktiv angezeigt, wenn sowohl APSD in den Einstellungen des logischen WLANs als auch das globale QoS-Modul aktiviert sind.

■ WEBconfig: LCOS-Menübaum ▶ Status ▶ WLAN ▶ Stationstabelle

Zeigt in einer Bitmaske an, für welche Zugriffskategorien der eingebuchte WLAN-Client APSD nutzt:

Voice (höchste Priorität)

Video

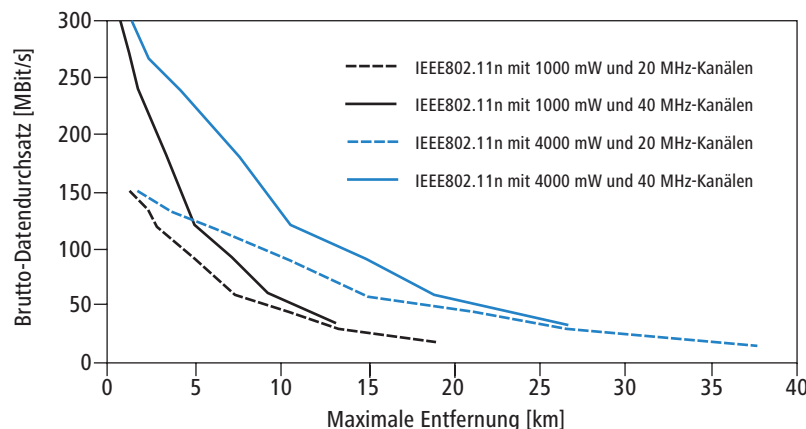
Best effort (einschließlich Datenverkehr von "Legacy Power Save"-Clients)

Background (geringste Priorität).

A.5 BFWA – mehr Sendeleistung für mehr Reichweite

BFWA steht für breitbandige, ortsfeste Funkstrecken, mit denen beispielsweise von einem Netzknoten ausgehend Verbindungen mit dem Internet für die angeschlossenen Teilnehmer zur Verfügung gestellt werden können. Die Frequenzen wurden im Rahmen einer Allgemeinzuteilung von der Bundesnetzagentur bereitgestellt. BFWA funkt im 5,8 GHz-Bereich. Die maximal zulässige Sendeleistung beim Betrieb von BFWA-Funkstrecken liegt bei 4000 mW EIRP (Equivalent Isotropic Radiated Power).

In dieser hohen zulässigen Sendeleistung liegt der Vorteil von BFWA. Denn ohne BFWA ist die zulässige maximale Sendeleistung für Outdoor WLAN-Richtfunkssysteme im 5 GHz-Band auf 1000 mW beschränkt. Durch die Vervierfachung der zulässigen Strahlungsleistung können mit denselben Richtfunkssystemen deutlich größere Distanzen überbrückt werden.



LANCOM Access Points auf Basis von 802.11n sowie alle aktuellen LANCOM 54 Mbit/s Access Points unterstützen BFWA ab der LCOS-Version 7.70. Bei älteren Access Points ist die Unterstützung abhängig vom Chipsatz (AR-5414 Chipsatz). Der LANCOM-Support informiert Sie bei diesen Modellen über eine mögliche Unterstützung von BFWA. Weitere Informationen entnehmen Sie bitte dem Techpaper "Broadband Fixed Wireless Access (BFWA)", erhältlich als Download von www.lancom.de.

A.6 RADIUS-Accounting neu starten

Die Accounting-Funktion im LANCOM kann u.a. dazu genutzt werden, das Budget von angeschlossenen WLAN-Clients zu kontrollieren. Wireless Internet Service Provider (WISPs) nutzen diese Möglichkeit teilweise zur Abrechnung ihrer Kunden. Da die Abrechnungsintervalle üblicherweise zum Monatsende wechseln, kann über eine entsprechende Aktion der Neustart aller aktuellen Accounting-Sitzungen ausgelöst werden – die eigentliche WLAN-Verbindung bleibt dabei bestehen. Mit Hilfe eines Cron-Jobs kann dieser Neustart komfortabel automatisiert werden.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN ▶ RADIUS-Accounting

■ Neustart-Accounting


Beendet alle aktuellen Accounting-Sitzungen und eröffnet gegenüber dem RADIUS-Server entsprechende neue Accounting-Sitzungen.


A.7 Voucher für Public-Spot mit Zeitbudget

A.7.1 Einleitung

Mit Hilfe des Voucher Druck-Assistenten richten Sie zeitlich begrenzte Zugänge zu einem Public-Spot-WLAN mit wenigen Mausklicks ein. Dabei wird lediglich die Nutzungsdauer des Zugangs festgelegt, Benutzername und Kennwort werden automatisch vergeben und in die Konfiguration des LANCOM-Gerätes eingetragen. Als Ergebnis wird ein personalisierter Gutschein (Voucher) ausgedruckt, mit dem sich der Anwender im Public-Spot-WLAN für eine begrenzte Zeit anmelden kann.

Damit die Vouchers nicht immer genau in dem Moment ausgedruckt werden müssen, wenn ein Anwender einen Zugang zum Public-Spot-WLAN wünscht, können die Gutscheine auch auf Vorrat ausgedruckt werden. Dabei wird der Zugang so eingestellt, dass die Nutzungsdauer erst ab dem ersten Login mit den zugehörigen Zugangsdaten läuft. Dazu wird eine maximale Gültigkeitsdauer des Zugangs definiert – nach dieser Zeit wird der Zugang automatisch gelöscht, auch wenn die Nutzungsdauer noch nicht genutzt wurde.

 Zeitlich begrenzte Public-Spot-Zugänge können nur eingerichtet werden, wenn das LANCOM über die korrekte Uhrzeit verfügt.

 In den LCOS-Versionen vor 7.70 wurden Public-Spot-Zugänge über den Assistenten in der Benutzer-Liste des Public-Spot-Moduls eingetragen. Ab der LCOS-Version 7.70 speichert der Assistent die Public-Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Um diese Public-Spot-Zugänge nutzen zu können, muss der RADIUS-Server im LANCOM konfiguriert sein. Bitte beachten Sie dazu die Hinweise unter 'RADIUS-Server für Public-Spot-Nutzung konfigurieren' → Seite 5.

A.7.2 Public-Spot-Benutzer einrichten und Voucher drucken

Zum Einrichten des Public-Spot-Zugangs ruft der Mitarbeiter in seinem Browser die IP-Adresse des Wireless Routers oder Access Points auf (z. B. über eine Verknüpfung auf dem Desktop) und meldet sich mit seinem Benutzernamen und Kennwort an. Sofern sein Administrator-Zugang entsprechend eingestellt ist, kann der Mitarbeiter ausschließlich den Assistenten zum Einrichten der Public-Spot-Benutzer ausführen.

- ① Nach dem Starten des Assistenten stellen Sie die Nutzungsdauer für den Zugang ein.
- ② Wählen Sie aus, ob der Zugang sofort aktiviert werden soll oder ob die Nutzungsdauer erst mit dem ersten Login startet.
- ③ Bei einer Nutzungsdauer nach erstem Login geben Sie die Dauer in Tagen ein, nach welcher der Zugang spätestens abläuft (Gültigkeitsdauer).
- ④ Im Kommentarfeld tragen Sie optional einen Text ein, der den Nutzer eindeutig identifiziert (z.B. Name oder Raumnummer des Hotelgastes). Alternativ zum vordefinierten Kommentarfeld können auch bis zu fünf kundenspezifische Kommentarfelder verwendet werden.
- ⑤ Klicken Sie danach auf **Benutzerdaten speichern und drucken**, um die Zugangsdaten im Gerät zu speichern und auszudrucken.

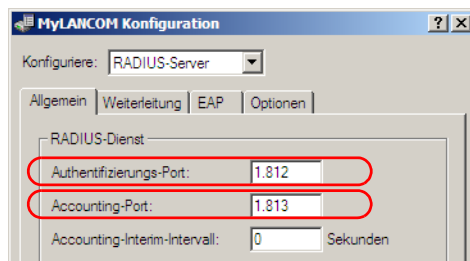


Hinweise zu den Rechten und Pflichten für Betreiber von öffentlichen Public-Spot-Zugängen finden Sie im entsprechenden LANCOM Whitepaper unter www.lancom.de.

A.7.3 RADIUS-Server für Public-Spot- Nutzung konfigurieren

In den LCOS-Versionen vor 7.70 wurden Public-Spot-Zugänge über den Assistenten in der Benutzer-Liste des Public-Spot-Moduls eingetragen. Ab der LCOS-Version 7.70 speichert der Assistent die Public-Spot-Zugänge nicht mehr in dieser Liste, sondern in der Benutzerdatenbank des internen RADIUS-Servers. Um diese Public-Spot-Zugänge nutzen zu können, **muss** der RADIUS-Server konfiguriert und das Public-Spot-Modul auf die Nutzung des RADIUS-Servers eingestellt sein.

- ① Damit die Benutzer-Datenbank im internen RADIUS-Server genutzt werden kann, muss der RADIUS-Server im LANCOM zunächst eingeschaltet werden. Aktivieren Sie den RADIUS-Server durch das Eintragen von Authentifizierungs- und Accounting-Port. Verwenden Sie den Authentifizierungs-Port 1.812 und den Accounting-Port 1.813.



LANconfig: RADIUS ► Allgemein

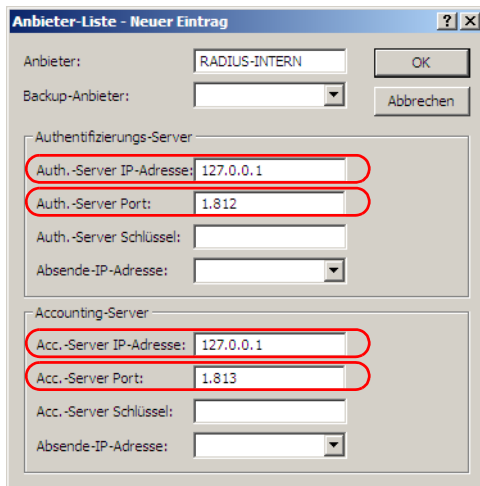
WEBconfig: LCOS-Menübaum ► Setup ► RADIUS ► Server ► Authentifizierungs- und Accounting-Port

- ② Damit die Public-Spot-Zugänge am internen RADIUS-Server des LANCOMs authentifiziert werden können, muss der Public-Spot die Adresse des RADIUS-Servers kennen. Erstellen Sie dazu für den internen RADIUS-Server einen neuen Eintrag als "Anbieter". Tragen Sie die IP-Adresse des LANCOMs, in dem der RADIUS-Server aktiviert wurde, als Authentifizierungs- und Accounting-Server ein.



Wenn der Public-Spot und der RADIUS-Server vom gleichen LANCOM bereitgestellt werden, tragen Sie hier die interne Loopback-Adresse des Geräts (127.0.0.1) ein.

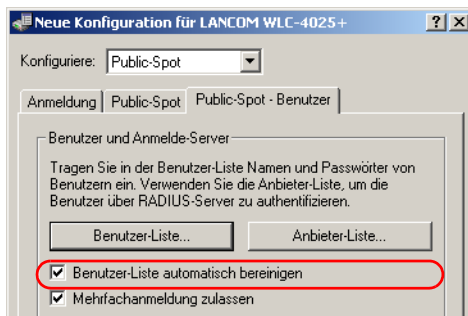
- ③ Übernehmen Sie Authentifizierungs- und Accounting-Port von der Einstellung im RADIUS-Server (1.812 und 1.813).



LANconfig: Public-Spot ▶ Public-Spot-Benutzer ▶ Anbieter-Liste

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Public-Spot-Modul ▶ Anbieter-Tabelle

- ④ Aktivieren Sie im Public-Spot-Modul die Option zum Bereinigen der Benutzer-Liste, damit die nicht mehr benötigten Einträge automatisch gelöscht werden können.



LANconfig: Public-Spot ▶ Public-Spot-Benutzer

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server

- ! Nach einem Update auf LCOS 7.70 sind die mit der vorherigen LCOS-Version angelegten Benutzerkonten in der Benutzer-Liste des Public-Spot-Moduls weiterhin gültig.

A.7.4 Interner und externer RADIUS-Server kombiniert

Für die Authentifizierung der internen WLAN-Benutzer mit IEEE 802.1x wird in manchen Unternehmen ein externer RADIUS-Server eingesetzt. In einer Anwendung mit einem WLAN Controller und mehreren Access Points fungiert zunächst der WLAN Controller als RADIUS-Server für alle Access Points. Im WLAN Controller wird dazu die entsprechende Weiterleitung der RADIUS-Anfragen an den externen RADIUS-Server definiert.

- ! Die im folgenden beschriebenen Einstellungen sind nur dann notwendig, wenn Sie neben dem Public Spot im LANCOM einen externen RADIUS-Server nutzen.

Im Zusammenhang mit einem Public Spot für Gast-Zugänge sind weitere Einstellungen notwendig:

- Die Authentifizierungsanfragen der internen Mitarbeiter sollen an den externen RADIUS-Server weitergeleitet werden.
- Die Authentifizierungsanfragen der Public-Spot-Zugänge sollen vom internen RADIUS-Server geprüft werden.

Realm-Tagging für das RADIUS-Forwarding

Die Authentifizierungsanfragen der beiden Benutzergruppen müssen separat behandelt werden. Damit der WLAN Controller diese beiden Gruppen unterscheiden kann, werden so genannte "Realms" eingesetzt. Realms dienen der Adressierung von Domänen, innerhalb derer Benutzeraccounts gültig sind. Die Realms können mit der Authentifizierungsanfrage an den RADIUS-Server im WLAN Controller übermittelt werden. Alternativ kann der RADIUS-Server nach folgenden Regeln die Realms der Benutzernamen verändern, um das RADIUS-Forwarding zu steuern:

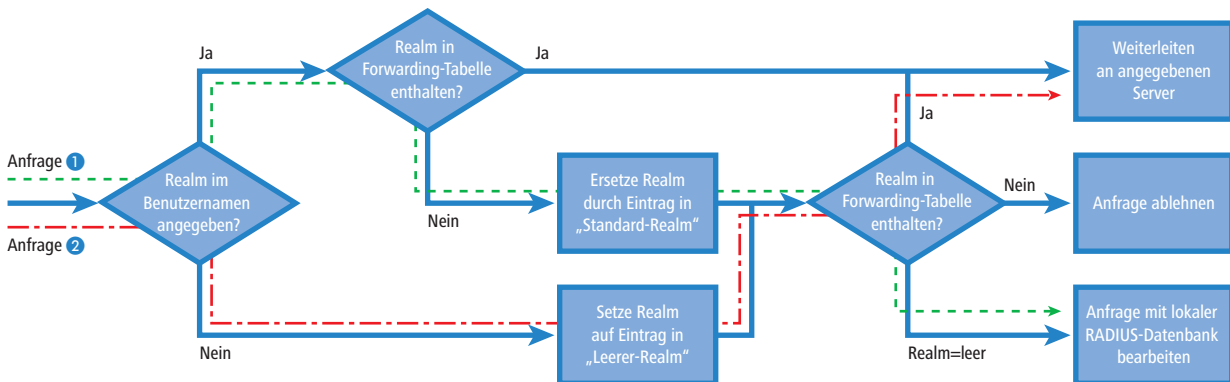
- Der als "Standard-Realm" definierte Wert ersetzt einen vorhandenen Realm einer eingehenden Anfrage, wenn für diesen Realm keine Weiterleitung definiert ist.

- Der unter "Leerer-Realm" definierte Wert wird **nur dann** verwendet, wenn der eingehende Benutzername **noch keinen** Realm enthält.

Über einen Eintrag in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit einem bestimmten Realm an einen RADIUS-Server weitergeleitet werden. Wenn in der Weiterleitungstabelle kein passender Eintrag vorhanden ist, wird die Anfrage abgelehnt.

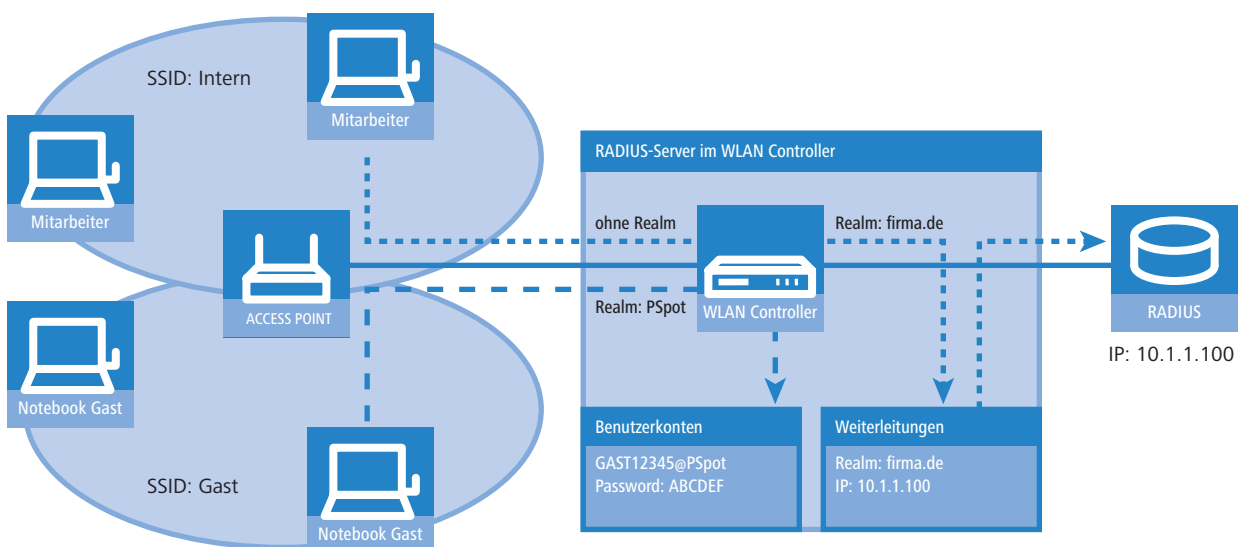
! Wenn nach der Ermittlung eines Realms ein leerer Realm festgestellt wird, so wird die Authentifizierungsanfrage **immer** mit der internen RADIUS-Datenbank des LANCOMs geprüft.

Das folgende Flussdiagramm zeigt schematisch die Arbeitsweise des RADIUS-Server bei der Verarbeitung von Realms:



Durch ein unterschiedliches Realm-Tagging können somit verschiedene RADIUS-Server angesprochen werden. Den Entscheidungsweg im RADIUS-Server des LANCOMs können Sie im Diagramm für die beiden Anfragen verfolgen:

- 1 Da die Benutzernamen für die Gastzugänge automatisch erzeugt werden, wird für diese Benutzernamen der Realm "PSpot" verwendet. Da in der Weiterleitungstabelle kein entsprechender Eintrag vorhanden ist und der Standard-Realm leer ist, werden alle Authentifizierungsanfragen mit diesem Realm an den internen RADIUS-Server weitergeleitet.
- 2 Um den Konfigurationsaufwand zu begrenzen, werden die internen Benutzer weiterhin ohne Realm geführt. Der RADIUS-Server im LANCOM kann einen leeren Realm automatisch durch einen anderen Realm ersetzen, mit dem die internen Benutzer identifiziert werden. In diesem Beispiel wird der leere Realm durch die Domäne der Firma "firma.de" ersetzt. Mit den Angaben in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit diesem Realm an den externen RADIUS-Server weitergeleitet werden.

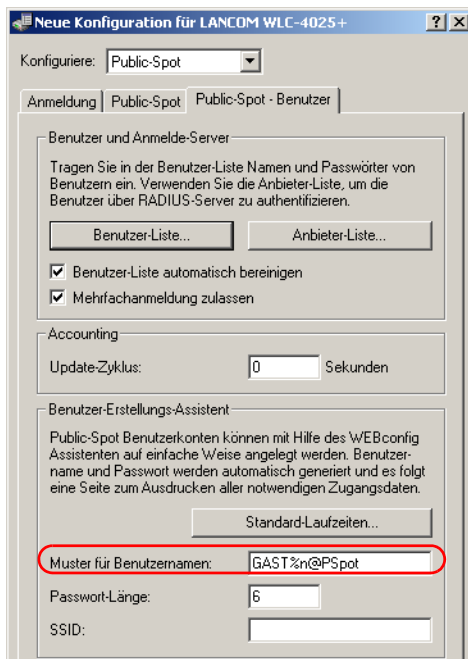


Konfiguration für das RADIUS-Forwarding

Mit den folgenden Konfigurationsschritten können Sie die separate Behandlung der internen Benutzer und der Gastzugänge definieren.

□ Voucher für Public-Spot mit Zeitbudget

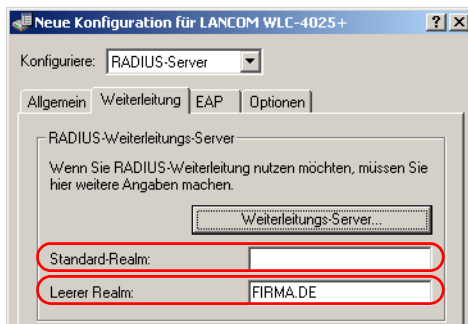
- ① Passen Sie im Public Spot das Muster für die Benutzernamen so an, dass ein eindeutiger Realm verwendet wird. Mit dem Muster "GAST%n@PSpot" werden z. B. Benutzernamen der Form "GAST12345@PSpot" erzeugt.



LANconfig: Public-Spot ▶ Public-Spot-Benutzer

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Public-Spot-Modul

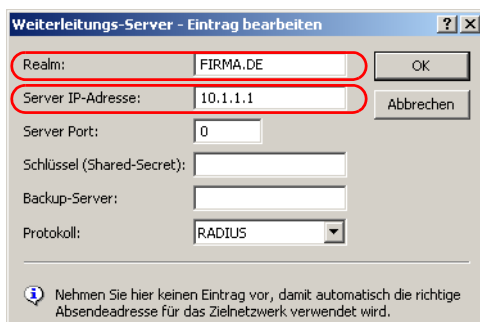
- ② Tragen Sie im RADIUS-Server des WLAN Controllers einen "leeren Realm" ein (z. B. "FIRMA.DE"). Dieser Realm wird für alle Benutzernamen verwendet, die ohne Realm eine Authentifizierungsanfrage bei dem WLAN Controller stellen. Das sind in dieser Anwendung die internen Benutzer, für die kein Realm definiert ist. Damit der RADIUS-Server des WLAN Controllers für diese Benutzernamen auch keinen Realm einsetzt, muss der "Standard-Realm" unbedingt leer bleiben.



LANconfig: RADIUS-Server ▶ Weiterleitung

WEBconfig: LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server

- ③ Damit die Authentifizierungsanfragen der internen Benutzer an den externen RADIUS-Server weitergeleitet werden, legen Sie einen passenden Eintrag bei den Weiterleitungen an. Mit dem Realm "FIRMA.DE" werden alle eingehenden RADIUS-Anfragen an die angegebene IP-Adresse weitergeleitet, die über diesen Realm verfügen.



LANconfig: RADIUS-Server ► Weiterleitung ► Weiterleitungs-Server

WEBconfig: LCOS-Menübaum ► Setup ► RADIUS ► Server ► Weiterleit.-Server

- ④ Die Authentifizierungsanfragen der Public-Spot-Benutzer gehen mit dem Realm "@PSpot" beim WLAN Controller ein. Da für diesen Realm keine Weiterleitung definiert ist, werden die Benutzernamen automatisch in der internen RADIUS-Datenbank geprüft. Da die über den Assistenten angelegten Public-Spot-Zugänge in dieser Datenbank gespeichert werden, können diese Anfragen wie gewünscht authentifiziert werden.

A.8 Erweiterungen im RADIUS-Server

Für die Einrichtung von Public-Spot-Benutzern mit Zeit- und Volumen-Budgets sind zusätzliche Parameter in der Benutzertabelle des RADIUS-Servers erforderlich.

LANconfig: RADIUS ► Allgemein ► Benutzerkonten

WEBconfig: LCOS-Menübaum ► Setup ► RADIUS ► Server ► Benutzer

■ Mehrfach-Logins

Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

Mögliche Werte:

- Ja, Nein

Default:

- Ja



Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

■ Ablauf-Art

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

Mögliche Werte:

- Absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.

- Relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Default:

- Leer: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.



Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.



Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

■ Abs.-Ablauf

Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

Mögliche Werte:

- Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus 0123456789/ : .Pp

Default:

- Leer

Besondere Werte:

- 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

■ Rel.-Ablauf

Wenn der Ablauf-Typ "Relativ" aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Mögliche Werte:

- Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default:

- 0

Besondere Werte:

- 0 schaltet die Überwachung der relativen Ablaufzeit aus.

■ Zeit-Budget

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte:

- Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default:

- 0

Besondere Werte:

- 0 schaltet die Überwachung der Nutzungsdauer aus.

■ Volumen-Budget

Maximales Datenvolumen für diesen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte:

- Volumen-Budget in Bytes. Maximal 10 Zeichen aus 0123456789

Default:

- 0

Besondere Werte:

- 0 schaltet die Überwachung des Datenvolumens aus.

■ Kommentar

Kommentar zu diesem Eintrag.

■ Service-Typ

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt.

Mögliche Werte:

- Umrahmt: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.

- Login: Für Public-Spot-Anmeldungen.
 - Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.
 - Beliebig
- Default:
- Beliebig



Die Anzahl der Einträge mit dem Service-Typ "Beliebig" oder "Login" ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service-Typ "Beliebig" verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

A.9 IGMP Snooping

A.9.1 Einleitung

Alle LANCOM-Geräte mit WLAN-Schnittstellen verfügen über eine "LAN-Bridge", die für die Übertragung der Daten zwischen den Ethernet-Ports und den WLAN-Schnittstellen sorgen. Die LAN-Bridge arbeitet dabei in vielen Aspekten wie ein Switch. Die zentrale Aufgabe eines Switches – im Gegensatz zu einem Hub – besteht darin, Pakete nur an den Port weiterzuleiten, an dem der Empfänger angeschlossen ist. Dazu bildet der Switch automatisch aus den eingehenden Datenpaketen eine Tabelle, in der die Absender-MAC-Adressen den Ports zugeordnet werden.

Wenn eine Ziel-Adresse eines eingehenden Pakets in dieser Tabelle gefunden wird, kann der Switch das Paket gezielt an den richtigen Port weiterleiten. Wird die Ziel-Adresse nicht gefunden, so leitet der Switch das Paket an alle Ports weiter. D.h. ein Switch kann ein Paket nur dann zielgerichtet weiterleiten, wenn die Zieladresse schon einmal als Absenderadresse eines Pakets über einen bestimmten Port bei ihm eingegangen ist. Broadcast- oder Multicast-Pakete können aber niemals als Absenderadresse in einem Paket eingetragen sein, darum werden diese Pakete immer auf alle Ports "geflutet".

Während dieses Verhalten für Broadcasts die richtige Aktion ist (Broadcasts sollen schließlich alle möglichen Empfänger erreichen), ist es für Multicasts nicht ungedingt die gewünschte Lösung. Multicasts richten sich in der Regel an eine bestimmte Gruppe von Empfängern in einem Netzwerk, nicht aber an alle:

- Videostreams werden z.B. häufig als Multicast übertragen, aber nicht alle Stationen im Netzwerk sollen einen bestimmten Stream empfangen.
- Verschiedene Anwendungen im medizinischen Bereich nutzen Multicasts, um Daten an bestimmte Endgeräte zu übertragen, die nicht an allen Stationen eingesehen werden sollen.

Bei einer LAN-Bridge im LANCOM wird es daher auch Ports geben, an denen kein einziger Empfänger des Multicasts angeschlossen ist. Das "überflüssige" Versenden der Multicasts auf Ports ohne Empfänger ist zwar kein Fehler, es führt aber zu Performance-Problemen:

- Viele Stationen können die unerwünschten Multicasts nicht in der Hardware der Netzwerkadapter aussortieren, sondern reichen die Pakete einfach an die höher gelegenen Protokollschichten weiter, was zu einer höheren Belastung der CPU führt.
- Gerade in WLANs kann die unnötige Aussendung der Multicasts zu einer deutlichen Einschränkung der verfügbaren Bandbreite führen, wenn keiner der angemeldeten WLAN-Clients Bedarf für den Multicast hat.

Mit dem Internet Group Management Protocol (IGMP) stellt die TCP/IP-Protokollfamilie ein Protokoll bereit, mit dem die Netzwerkstationen dem Router, an dem sie angeschlossen sind, das Interesse an bestimmten Multicasts mitteilen können. Dazu registrieren sich die Stationen bei den Routern für bestimmte Multicast-Gruppen, von denen Sie die entsprechenden Pakete beziehen wollen (Multicast-Registration). IGMP nutzt dazu spezielle Nachrichten zum Anmelden (Join-Messages) und Abmelden (Leave-Messages).



Die Information, in welchen Multicast-Gruppen sich eine Station registrieren kann oder soll, erhält die Station über andere Protokolle außerhalb von IGMP.

IGMP kann als Layer-3-Protokoll nur IP-Subnetze entsprechend der Anmeldungen an Multicast-Gruppen verwalten. Die in den Netzwerkstrukturen vorhandenen Geräte wie Bridges, Switches oder WLAN Access Points leiten die Pakete aber oft nur auf Layer 2 weiter, so dass IGMP zunächst keine Funktionen bietet, um die Pakete zielgerichtet durch diese Netzwerkstrukturen zu leiten. Die Bridges nutzen daher die Multicast-Registrierung zwischen Stationen und Routern, um zusätzliche Informationen über die zielgerichtete Verteilung der Multicasts zu erhalten. IP-Multicasts müssen nur an die Ports weitergeleitet werden, an denen sich ein Router befindet, der Multicast-Routing beherrscht und die Pakete in bestimmte IP-Subnetzen weiterleiten kann. Dieses Verfahren wird als IGMP Snooping bezeichnet. Die Bridges, die eigentlich die Entscheidung für das Weiterleiten der Pakete anhand der MAC auf Layer 2 treffen, nutzen damit zusätzlich die Layer 3-Informationen der IP-Multicast-Pakete.

□ IGMP Snooping

Für die weitere Beschreibung der Funktionen des IGMP Snooping im LCOS werden zwei wesentliche Begriffe unterschieden:

- Ein Port ist "Mitglied einer Multicast-Gruppe", wenn mindestens eine daran angeschlossene Station Pakete für eine bestimmte Multicast-Adresse empfangen möchte. Diese Multicast-Registrierung kann sowohl dynamisch über IGMP Snooping gelernt wie auch manuell konfiguriert sein.
- Ein Port ist ein "Router-Port", wenn daran ein Router angeschlossen ist, der Multicast-Routing beherrscht und die Pakete in bestimmte IP-Subnetzen weiterleiten kann.
- Eine Multicast-Gruppe ist "nicht registriert", wenn kein Port der Bridge Mitglied dieser Multicast-Gruppe ist.

A.9.2 Ablauf des IGMP Snooping

Beim Empfang eines Pakets unterscheidet die Bridge zunächst, ob es sich um einen Broadcast, Multicast oder Unicast handelt. Broadcasts und Unicasts werden wie üblich weitergeleitet, d.h. entweder auf alle Ports oder nur auf den Port, an den entsprechend des Eintrags in der MAC-Tabelle der Empfänger angeschlossen ist.

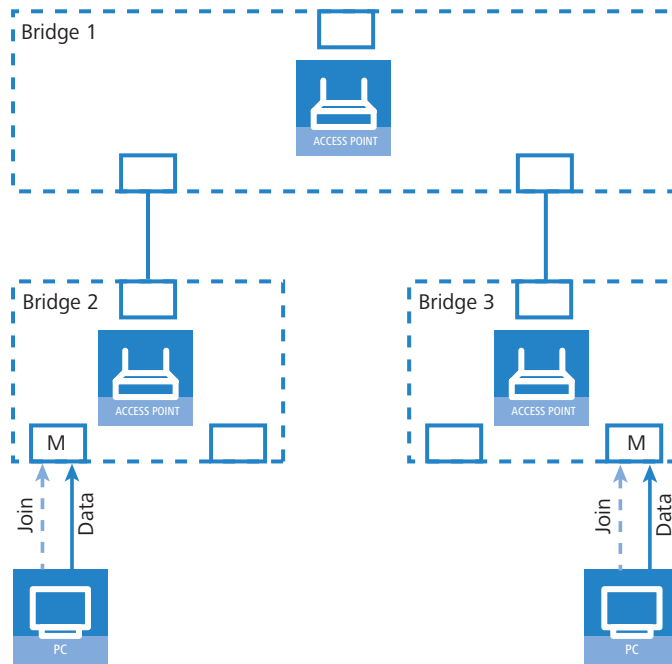
Für die IP-Multicast-Pakete werden zwei Typen unterschieden (abgeschnittene Pakete oder Pakete mit ungültiger Prüfsumme werden dabei verworfen):

- IGMP-Nachrichten werden je nach Inhalt unterschiedlich behandelt:
 - Eine Join-Message führt dazu, dass der Port, über den das Paket eingeht, Mitglied der entsprechenden Multicast-Gruppe wird. Diese Nachricht wird nur an Router-Ports weitergeleitet.
 - Entsprechend führt eine Leave-Message dazu, dass der Port, über den das Paket eingeht, aus der entsprechenden Multicast-Gruppe entfernt wird. Auch diese Nachricht wird nur an Router-Ports weitergeleitet.
 - Eine eingehende IGMP-Anfrage macht den Port zu einem Router-Port. Diese Nachrichten werden an alle Ports weitergeleitet.
 - Alle anderen IGMP-Nachrichten werden an alle Ports weitergeleitet – dabei werden keine der Port-Eigenschaften geändert.
- Wenn es sich bei einem IP-Multicast-Paket nicht um eine IGMP-Nachricht handelt, wird die Ziel-Adresse ausgewertet. Pakete für die Zieladresse "224.0.0.x" werden dabei an alle Ports weitergeleitet, weil dieser "reservierte" Bereich von Protokollen ohne richtige IGMP-Registrierung verwendet wird. Für alle anderen Pakete wird die Zieladresse in der Tabelle der IGMP-Mitgliedschaften ermittelt:
 - Wenn die Adresse gefunden wird, wird das Paket an die entsprechenden Ports weitergeleitet.
 - Wenn die Adresse nicht gefunden wird, wird das Paket je nach Konfiguration entweder verworfen, an alle Ports oder ausschließlich an alle Router-Ports weitergeleitet.

In beiden Fällen werden die Pakete an alle Router-Ports weitergeleitet.

A.9.3 IGMP Snooping über mehrere Bridges hinweg

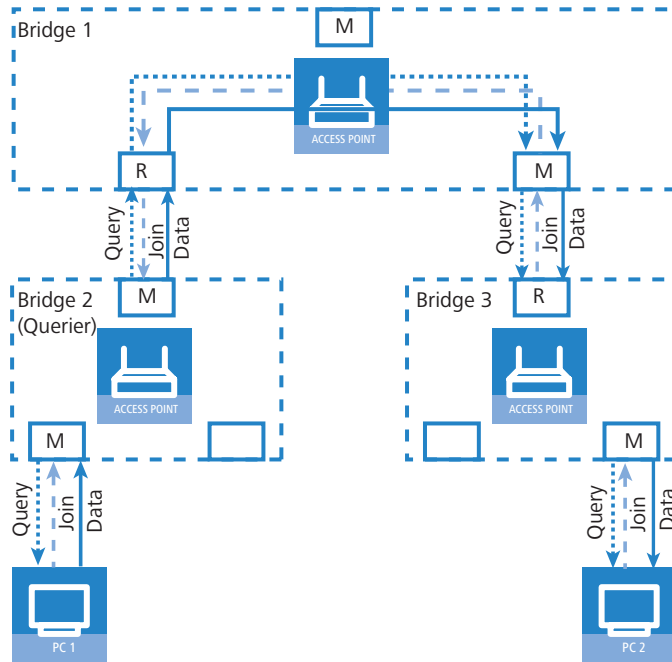
Wie beschrieben leitet IGMP Snooping eingehende Join- oder Leave-Nachrichten nur über Router-Ports weiter. In einer Struktur mehrerer Bridges sind zu Beginn alle Ports weder Router-Port noch Mitglied einer Multicast-Gruppe. Wenn sich die an den Bridges angeschlossenen Stationen für eine Multicast-Gruppe registrieren, wird der verwendete Port automatisch Mitglied dieser Gruppe. In dieser Phase ist allerdings keiner der Ports als Router-Port aktiviert, daher werden die Join-Nachrichten auch nicht an andere Bridges weitergeleitet. Die übergeordneten Bridges erfahren also nichts von der Mitgliedschaft des Ports in der gewünschten Multicast-Gruppe.



Die Bridges müssen also über Router-Ports verfügen, damit sich die Informationen über die Mitgliedschaften in Multicast-Gruppen verbreiten können. Da die Ports der Bridge nur durch IGMP-Anfragen zu Router-Ports werden können, muss einer der Multicast-fähigen Router im Netzwerk die Aufgabe übernehmen, die benötigten IGMP-Anfragen in Netzwerk zu steuern. Dieser Router wird auch als IGMP-Querier bezeichnet. Für den Fall, dass kein Multicast-Router im Netzwerk vorhanden ist, können die LANCOM Access Points einen Querier simulieren. Um parallele Anfragen von unterschiedlichen Querier-Instanzen zu vermeiden, schaltet sich eine Querier-Instanz ab, wenn ein anderer Querier mit niedrigerer IP-Adresse gefunden wird. Die Verteilung der IGMP-Informationen durch den Querier lässt sich an folgendem Beispiel erklären:

- ① Der Querier (im Beispiel Bridge 2) sendet in regelmäßigen Abständen IGMP-Anfragen über alle verfügbaren Ports aus (gepunktete Linien). Diese Anfragen kennzeichnen in der nächsten Bridge (Bridge 1) den Port, auf dem die Anfrage eingeht, als Router-Port (R). PC 1 antwortet auf diese Anfrage mit einer Join-Nachricht für alle Multicast-Gruppen (helle gestrichelte Linien), in welchen diese Station sich registrieren möchte. Der Port, an dem PC 1 an Bridge 2 angeschlossen ist, wird damit Mitglied der entsprechenden Multicast-Gruppe(n).
- ② Außerdem versendet diese Bridge 1 die Anfragen über alle anderen Ports an angeschlossene Bridges und Stationen weiter unten in der Struktur. In Bridge 3 wird der Port, über den die Anfrage eingeht, dadurch zum Router-Port (R).
- ③ Auch die an Bridge 3 angeschlossene Station (PC 2) antwortet auf diese Anfrage mit einer Join-Nachricht für alle registrierten Multicast-Gruppen. Der Port, an dem PC 2 an Bridge 3 angeschlossen ist, wird damit Mitglied der entsprechenden Multicast-Gruppe(n).
- ④ Bridge 3 leitet diese Join-Nachricht über den Router-Port weiter an Bridge 1. Der empfangende Port von Bridge 1 wird damit auch Mitglied der Multicast-Gruppen, für die sich PC 2 registriert hat.
- ⑤ Im letzten Schritt leitet Bridge 1 die Join-Nachricht von PC 2 über den Router-Port weiter an Bridge 2, wo der empfangende Port ebenfalls Mitglied der Multicast-Gruppen von PC 2 wird.

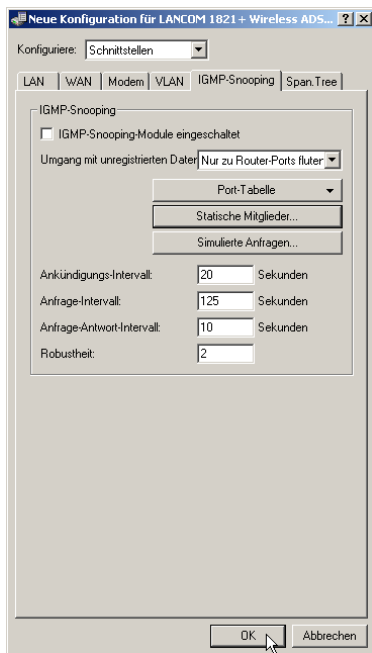
□ IGMP Snooping



Wenn nun PC 1 einen Multicast aussendet für eine der von PC 2 registrierten Multicast-Gruppen, leiten alle Bridges (2, 1 und dann 3) die Pakete jeweils über den Mitglieds-Port weiter bis zu PC 2.

A.9.4 Konfiguration

Allgemeine Einstellungen



LANconfig: Schnittstellen ► IGMP-Snooping

WEBconfig: LCOS-Menübaum ► Setup ► LAN-Bridge ► IGMP-Snooping

■ In-Betrieb

Aktiviert oder deaktiviert IGMP Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicast auf alle Ports weiter.

Mögliche Werte:

Ja, Nein

Default:

Nein



Wenn diese Funktion deaktiviert ist, werden alle IP-Multicast-Pakete auf alle Ports gesendet. Bei einer Änderung des Betriebszustandes wird die IGMP-Snooping-Funktion vollständig zurückgesetzt, d.h. alle dynamische gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften) werden gelöscht.

■ Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP-Anfragen an die Multicast-Adresse 224.0.0.1 schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" und gelöscht werden.

- Ein Querier sendet nach der Anfangsphase IGMP-Anfragen in diesem Intervall.
- Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".
- Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 125



Das Anfrage-Intervall muss größer als das Anfrage-Antwort-Intervall sein.

■ Anfrage-Antwort-Intervall

Intervall in Sekunden, beeinflusst das Timing zwischen den IGMP-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP-Anfragen erwartet. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" und gelöscht werden.

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 10



Das Anfrage-Antwort-Intervall muss kleiner als das Anfrage-Intervall sein.

■ Robustheit

Dieser Wert bestimmt die Robustheit des IGMP-Protokolls. Diese Option toleriert den Paketverlust von IGMP-Anfragen gegenüber den Join-Nachrichten.

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 2

■ Werbe-Intervall

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP Snooping-fähige Geräte schneller lernen, welche ihrer Ports als Router-Ports verwendet werden sollen. Beim Aktivieren von Ports kann ein Switch z.B. eine entsprechende Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP-Anfragen.

Mögliche Werte:

- 4 bis 180 Sekunden

Default:

- 20

□ IGMP Snooping

■ **Unregistrierte-Datenpakete-Behandlung**

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches "224.0.0.x", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Mögliche Werte:

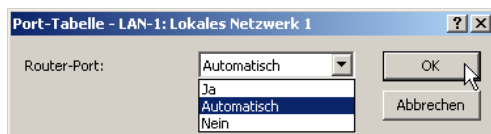
- Nur-Router-Ports: Sendet diese Pakete an alle Router-Ports.
- Fluten: Sendet diese Pakete an alle Ports.
- Verwerfen: Verwirft diese Pakete.

Default:

- Nur-Router-Ports

Port-Einstellungen

In dieser Tabelle werden die Port-bezogenen Einstellungen für IGMP Snooping vorgenommen.



LANconfig: Schnittstellen ▶ IGMP-Snooping ▶ Port-Tabelle

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ IGMP-Snooping ▶ Port-Einstellungen

■ **Port**

Auf diesen Port beziehen sich die Einstellungen.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

Default:

- N/A

■ **Router-Port**

Diese Option definiert das Verhalten des Ports.

Mögliche Werte:

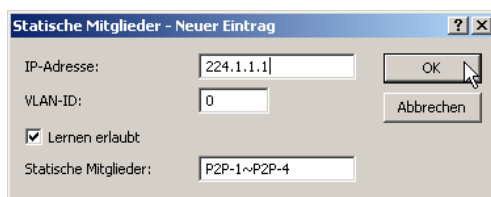
- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- Auto: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn für die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfangen wurden.

Default:

- Auto

Statische-Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z.B. nicht automatisch gelernt werden können oder sollen.



LANconfig: Schnittstellen ▶ IGMP-Snooping ▶ Statische Mitglieder

WEBconfig: LCOS-Menübaum ▶ Setup ▶ LAN-Bridge ▶ IGMP-Snooping ▶ Statische-Mitglieder

■ **Adresse**

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse.

Default:

- Leer

■ VLAN-Id

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

Mögliche Werte:

- 0 bis 4096.

Default:

- 0

Besondere Werte:

- Wenn "0" als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

■ Lernen-erlauben

Mit dieser Option wird das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe aktiviert. Wenn das automatische Lernen deaktiviert ist, werden die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports verschickt.

Mögliche Werte:

- Ja, Nein.

Default:

- Ja

■ Statische-Mitglieder

An diese Ports werden die Pakete mit der entsprechenden IP-Multicast-Adresse immer zugestellt, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

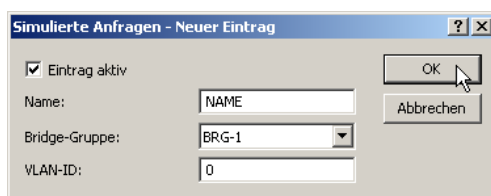
- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen.

Default:

- Leer

Simulierte-Anfrager

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können mehrere unabhängige Querier definiert werden, welche dann die entsprechenden VLAN-IDs nutzen.



LANconfig: Schnittstellen ► IGMP-Snooping ► Simulierte Anfragen

WEBconfig: LCOS-Menübaum ► Setup ► LAN-Bridge ► IGMP-Snooping ► Simulierte-Anfrager

■ Name

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Default:

- Leer

■ In-Betrieb

Aktiviert oder deaktiviert die Querier-Instanz.

□ IGMP Snooping

Mögliche Werte:

- Ja, Nein.

Default:

- Nein

■ **Bridge-Gruppe**

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen, keine.

Default:

- keine

Besondere Werte:

- Wenn "keine" Bridge-Gruppe gewählt wird, werden die IGMP-Anfragen auf allen Bridge-Gruppen ausgegeben.

■ **VLAN-Id**

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096.

Default:

- 0

Besondere Werte:

- Wenn "0" als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

A.9.5 IGMP Status

Allgemeine Statistiken

Die Status-Meldungen zu IGMP Snooping finden Sie auf folgenden Pfaden:

WEBconfig: LCOS-Menübaum ▶ Status ▶ LAN-Bridge-Statistiken ▶ IGMP-Snooping

■ **In-Betrieb**

Zeigt an, ob das IGMP Snooping aktiviert oder deaktiviert ist.

■ **IPv4-Pakete**

Zeigt die gesamte Anzahl der IPv4-Multicast-Pakete, die auf allen Ports empfangen wurden, unabhängig davon, ob es sich um IGMP-Pakete handelt oder nicht.

■ **Daten-Pakete**

Zeigt die gesamte Anzahl der nicht beschädigten IPv4-Multicast-Pakete, die auf allen Ports empfangen wurden, und bei denen es sich nicht um IGMP-Pakete handelt.

■ **Steuer-Pakete**

Zeigt die gesamte Anzahl der nicht beschädigten IGMP-Pakete, die auf allen Ports empfangen wurden.

■ **Defekte-Pakete**

Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP-Pakete, die auf allen Ports empfangen wurden. Mögliche Ursachen für die Beschädigung der Pakete sind IP-Prüfsummenfehler oder abgeschnittene Pakete.



Aus Performance-Gründen werden IP-Prüfsummen nur für IGMP-Pakete ausgewertet, nicht für den Datenteil der Multicast-Pakete. Daher werden Pakete mit einer fehlerhaften Prüfsumme im TCP/UDP- oder IP-Header nicht erkannt. Diese Pakete werden als Datenpakete gezählt.

■ **Werte-loeschen**

Diese Aktion löscht alle Statistik-Einträge.

Port-Status

Diese Tabelle zeigt alle Port-bezogenen Statistiken.

WEBconfig: LCOS-Menübaum ▶ Status ▶ LAN-Bridge-Statistiken ▶ IGMP-Snooping ▶ Port-Status

■ **Router-Port**

Zeigt an, ob der Port derzeit als Router-Port genutzt wird oder nicht, unabhängig davon, ob dieser Zustand statisch konfiguriert oder dynamisch gelernt wurde.

■ **IPv4-Pakete**

Zeigt die gesamte Anzahl der IPv4-Multicast-Pakete, die auf diesem Port empfangen wurden, unabhängig davon, ob es sich um IGMP-Pakete handelt oder nicht.

■ **Daten-Pakete**

Zeigt die gesamte Anzahl der nicht beschädigten IPv4-Multicast-Pakete, die auf diesem Port empfangen wurden und bei denen es sich nicht um IGMP-Pakete handelt.

■ **Steuer-Pakete**

Zeigt die gesamte Anzahl der nicht beschädigten IGMP-Pakete, die auf diesem Port empfangen wurden.

■ **Defekte-Pakete**

Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP-Pakete, die auf diesem Port empfangen wurden. Mögliche Ursachen für die Beschädigung der Pakete sind IP-Prüfsummenfehler oder abgeschnittene Pakete.



Aus Performance-Gründen werden IP-Prüfsummen nur für IGMP-Pakete ausgewertet, nicht für den Datenteil der Multicast-Pakete. Daher werden Pakete mit einer fehlerhaften Prüfsumme im TCP/UDP- oder IP-Header nicht erkannt. Diese Pakete werden als Datenpakete gezählt.

Gruppen

Diese Tabelle zeigt alle dem Gerät bekannten Mitgliedschaften von Multicast-Gruppen, unabhängig davon, ob sie statisch konfiguriert oder dynamisch gelernt wurden. Wenn für eine Multicast-Gruppe sowohl statische als auch dynamische Mitgliedschaften existieren, werden diese in separaten Einträgen angezeigt.

WEBconfig: LCOS-Menübaum ▶ Status ▶ LAN-Bridge-Statistiken ▶ IGMP-Snooping ▶ Gruppen

■ **Adresse**

Zeigt die IP-Multicast-Adresse der Gruppe.

■ **VLAN-Id**

Zeigt die VLAN-ID, für welche dieser Eintrag gültig ist.

■ **Lernen-erlauben**

Zeigt an, ob für die Gruppe neue Mitgliedschaften dynamisch gelernt werden dürfen oder nicht.

■ **Statische-Mitglieder**

Zeigt die Liste der statisch für die Gruppe definierten Mitglieder.

■ **Dynamische-Mitglieder**

Zeigt die Liste der dynamisch für die Gruppe gelernten Mitglieder.

Simulierte-Anfrager

Die Tabelle zeigt den Status aller definierten und aktiven IGMP-Querier-Instanzen.

■ **Name**

Zeigt den Namen der Multicast-Gruppe.

■ **Bridge-Gruppe**

Zeigt die Bridge-Gruppe, für welche dieser Eintrag gültig ist.

■ **VLAN-Id**

Zeigt das VLAN, für welches dieser Eintrag gültig ist.

■ **Status**


Zeigt den Status des Eintrags.

- Initial: Die Querier-Instanz wurde gerade gestartet und sendet IGMP-Anfragen in kurzen Intervallen (vielleicht schneller als das definierte Anfrage-Intervall).
- Querier: Die Querier-Instanz betrachtet sich selbst als den aktiven Querier und sendet IGMP-Anfragen in den als Anfrage-Intervall definierten Abständen.
- Non-Querier: Eine andere Querier-Instanz mit einer niedrigeren IP-Adresse wurde erkannt, die hier aufgeführte Instanz sendet keine IGMP-Anfragen.

A.10 TACACS+

A.10.1 Einleitung

TACACS+ (Terminal Access Control Access Control Server) ist ein Protokoll für Authentifizierung, Authorisierung und Accounting (AAA), es stellt also den Zugang zu Netzwerkkomponenten nur für bestimmte Nutzer sicher, regelt die Berechtigungen der Benutzer und überträgt Daten für die Protokollierung der Netzwerknutzung. TACACS+ ist also eine Alternative zu anderen AAA-Protokollen wie RADIUS.


 Der Einsatz von TACACS+ ist eine Voraussetzung für die Einhaltung der PCI-Compliance (Payment Card Industry).

Die Regelung der Zugriffsmöglichkeiten für die Anwender stellt in modernen Netzwerken mit zahlreichen Diensten und Netzwerkkomponenten eine große Herausforderung dar. Gerade in größeren Szenarien ist es kaum noch möglich, die Zugangsdaten der Benutzer auf jedem Gerät bzw. in jedem Dienst einzutragen und auf Dauer konsistent zu halten. Aus diesem Grund bietet sich die zentrale Bereitstellung der Benutzerdaten auf einem entsprechenden Server an.

In einem einfachen Anwendungsbeispiel möchte sich ein Anwender auf einem Router anmelden und übermittelt dazu seine Zugangsdaten (User-ID) an den Router. Der Router fungiert in diesem Fall als Network Access Server (NAS): er überprüft die Zugangsdaten nicht selbst, sondern leitet diese an den zentralen AAA-Server weiter, der die Daten nach der Prüfung mit einer positiven Bestätigung (Accept) oder einer Ablehnung (Reject) beantwortet.




Zu den erweiterten Funktionen von TACACS+ gehört u.a. die Möglichkeit, den Benutzer zum Wechseln des Kennworts aufzufordern (z.B. beim ersten Login oder nach Ablauf einer bestimmten Frist). Die entsprechenden Meldungen werden vom NAS an den Benutzer weitergereicht.

 Bitte beachten Sie, dass LANconfig nicht alle Meldungen des erweiterten Login-Dialogs auswerten kann. Falls LANconfig die Anmeldung an einem LANCOM trotz korrekter Eingabe der Benutzerdaten ablehnt, melden Sie sich bitte über einen alternativen Konfigurationsweg an (WEBconfig oder Telnet).

Neben den weit verbreiteten RADIUS-Servern bietet sich als AAA-Server auch TACACS+ an. Die Tabelle zeigt einige wesentliche Unterschiede zwischen RADIUS und TACACS+:

TACACS+	RADIUS
Verbindungsorientierte Datenübertragung über TCP	Verbindungslose Datenübertragung über UDP
Gesamte Datenübertragung wird verschlüsselt	Nur Kennwort wird verschlüsselt, Inhalte bleiben unverschlüsselt
Vollständige Trennung von Authentifizierung, Authorisierung und Accounting möglich	Authentifizierung, Authorisierung sind kombiniert

- Die Übertragung über TCP macht TACACS+ zuverlässiger als RADIUS, da die Kommunikation zwischen NAS und AAA-Server bestätigt wird und der NAS somit informiert wird, wenn der AAA-Server nicht erreichbar ist.
- TACACS+ verschlüsselt neben dem Kennwort die gesamten Nutzdaten (bis auf den TACACS+-Header). Dadurch können auch Informationen wie der Benutzername oder die erlaubten Dienste nicht abgehört werden. TACACS+ benutzt zur Verschlüsselung ein One-Time-Pad, welches auf MD5-Hashes basiert.
- Die Trennung der drei AAA-Funktionen erlaubt unter TACACS+ schließlich die Nutzung anderer Server. Während bei RADIUS Authentifizierung und Authorisierung immer zusammen gehören, kann TACACS+ Authentifizierung und Authorisierung getrennt verwenden. So kann z.B. der TACACS+-Server nur für die Authentifizierung eingesetzt werden, dabei müssen auch nur die Benutzer, nicht aber die erlaubten Kommandos gepflegt werden.

 Bitte beachten Sie: Auch wenn TACACS+ gezielt dazu genutzt wird, die Benutzerkonten nicht auf den einzelnen Geräten, sondern zentral auf einem AAA-Server abzulegen, sollten Sie auf jeden Fall für die LANCOM-Geräte ein sicheres Kennwort für den Root-Zugang definieren. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

A.10.2 Konfiguration der TACACS+-Parameter

Die Parameter für die Konfiguration von TACACS+ finden Sie auf folgenden Pfaden:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TACACS+

■ Accounting

Aktiviert das Accounting über einen TACACS+-Server. Wenn das TACACS+-Accounting aktiviert ist, werden alle Accounting-Daten über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

aktiviert, deaktiviert

Default

deaktiviert



Das TACACS+-Accounting wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.

■ Authentifizierung

Aktiviert die Authentifizierung über einen TACACS+-Server. Wenn die TACACS+-Authentifizierung aktiviert ist, werden alle Authentifizierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

aktiviert, deaktiviert

Default

deaktiviert



Die TACACS+-Authentifizierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Der Rückgriff auf lokale Benutzer kann dabei nur genutzt werden, wenn für das LANCOM ein Root-Kennwort gesetzt ist. Bei Geräten ohne Root-Kennwort muss der Rückgriff auf lokale Benutzer deaktiviert werden, da sonst bei Ausfall der Netzwerkverbindung (TACACS+-Server nicht erreichbar) ein Zugriff ohne Kennwort auf das LANCOM möglich wäre.

■ Authorisierung

Aktiviert die Authorisierung über einen TACACS+-Server. Wenn die TACACS+-Authorisierung aktiviert ist, werden alle Authorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte:

aktiviert, deaktiviert

Default

deaktiviert



Die TACACS+-Authorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Wenn die TACACS+-Authorisierung aktiviert ist, wird für jedes Kommando beim TACACS+-Server eine Anfrage gestellt, ob der Benutzer diese Aktion ausführen darf. Dementsprechend erhöht sich der Datenverkehr bei der Konfiguration, außerdem müssen die Rechte für die Benutzer im TACACS+-Server definiert sein.

■ Rückgriff_auf_lokale_Benutzer

Für den Fall, dass die definierten TACACS+-Server nicht erreichbar sind, kann ein Rückgriff auf die lokalen Benutzerkonten im LANCOM erlaubt werden. So ist der Zugriff auf die Geräte auch bei Ausfall der TACACS+-Verbindung möglich, z.B. um die TACACS+-Nutzung zu deaktivieren oder die Konfiguration zu korrigieren.

Mögliche Werte:

erlaubt, verboten

Default

erlaubt



Der Rückgriff auf lokale Benutzerkonten stellt ein Sicherheitsrisiko dar, wenn kein Root-Kennwort im LANCOM gesetzt ist. Daher kann die TACACS+-Authentifizierung mit Rückgriff auf lokale Benutzerkonten nur aktiviert werden, wenn ein Root-Kennwort definiert ist. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

□ TACACS+

■ **Shared-Secret**

Das Kennwort für die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte:

- 31 alphanumerische Zeichen

Default

- Leer



Das Kennwort muss im LANCOM und im TACACS+-Server übereinstimmend eingetragen werden. Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen.

■ **SNMP-GET-Anfragen-Accounting**

Zahlreiche Netzwerkmanagementtools nutzen SNMP, um Informationen aus den Netzwerkgeräten abzufragen. Auch der LANmonitor greift über SNMP auf die LANCOM-Geräte zu, um Informationen über aktuelle Verbindungen etc. darzustellen oder Aktionen wie das Trennen einer Verbindung auszuführen. Da über SNMP ein Gerät auch konfiguriert werden kann, wertet TACACS+ diese Zugriffe als Vorgänge, die eine Authorisierung voraussetzen. Da LANmonitor diese Werte regelmäßig abfragt, würde so eine große Zahl von eigentlich unnötigen TACACS+-Verbindungen aufgebaut. Wenn Authentifizierung, Authorisierung und Accounting für TACACS+ aktiviert sind, werden für jede Anfrage drei Sitzungen auf dem TACACS+-Server gestartet.

Mit diesem Parameter kann das Verhalten der LANCOM-Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für das Accounting zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.



Mit dem Eintrag einer Read-Only-Community unter LCOS-Menübaum ► Setup ► SNMP kann auch die Authentifizierung über TACACS+ für den LANmonitor deaktiviert werden. Die dort definierte Read-Only-Community wird dazu im LANmonitor als Benutzername eingetragen.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS ein Accounting über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe ein Accounting über den TACACS+-Server durchgeführt. Werden z.B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe kein Accounting über den TACACS+-Server erforderlich.

Default:

- nur_für_SETUP_Baum

■ **SNMP-GET-Anfragen-Authorisierung**

Mit diesem Parameter kann das Verhalten der LANCOM-Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für die Authorisierung zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS eine Authorisierung über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe eine Authorisierung über den TACACS+-Server durchgeführt. Werden z.B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe keine Authorisierung über den TACACS+-Server erforderlich.

Default:

- nur_für_SETUP_Baum

■ **Verschlüsselung**

Aktiviert oder deaktiviert die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte:

- aktiviert, deaktiviert

Default

- aktiviert



Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen. Wenn die Verschlüsselung hier aktiviert wird, muss außerdem das Kennwort für die Verschlüsselung passend zum Kennwort auf dem TACACS+-Server eingetragen werden.

A.10.3 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.

Die Parameter für die Konfiguration der TACSACS-Server finden Sie auf folgenden Pfaden:

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TACACS+ ▶ Server

■ Server-Adresse

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

Mögliche Werte:

- Gültiger DNS-auflösbarer Name oder gültige IP-Adresse.

Default

- Leer

■ Loopback-Adresse

Hier können Sie optional eine Loopback-Adresse konfigurieren.

Mögliche Werte:

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

Default

- Leer

■ Kompatibilitätsmodus

TACACS+-Server werden in einer freien und in einer kommerziellen Version angeboten, die jeweils unterschiedliche Nachrichten verwenden. Der Kompatibilitätsmodus ermöglicht die Verarbeitung der Nachrichten von den freien TACACS+-Servern.

Mögliche Werte:

- aktiviert, deaktiviert

Default

- deaktiviert

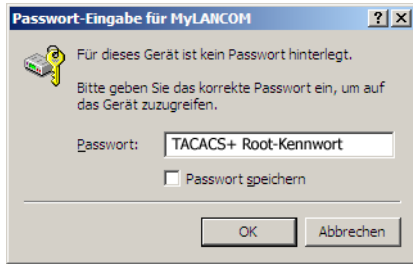
A.10.4 Anmelden am TACACS+-Server

Sobald die Verwendung von TACACS+ für die Authentifizierung und ggf. Authorisierung aktiviert ist, werden alle Logins auf dem Gerät an den TACACS+-Server weitergeleitet. Der weitere Ablauf des Logins unterscheidet sich je nach Zugangsart.

TACACS+-Anmeldung über LANconfig

Die Anmeldung über LANconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt ausschließlich über den Benutzer mit dem Namen "root". Der Benutzer "root" muss entsprechend im TACACS+-Server konfiguriert sein. Geben Sie beim Login über LANconfig das Kennwort ein, das im TACACS+-Server für den Benutzer "root" konfiguriert ist.

□ TACACS+



i Der Benutzer "root" ist der einzige Benutzer, der nach Authentifizierung über TACACS+ automatisch die vollen Rechte eines Supervisors verfügt und somit die Konfiguration ohne Wechsel des Rechteniveaus bearbeiten darf. Wenn die Authorisierung benutzt wird entscheidet dies der TACACS+-Server.

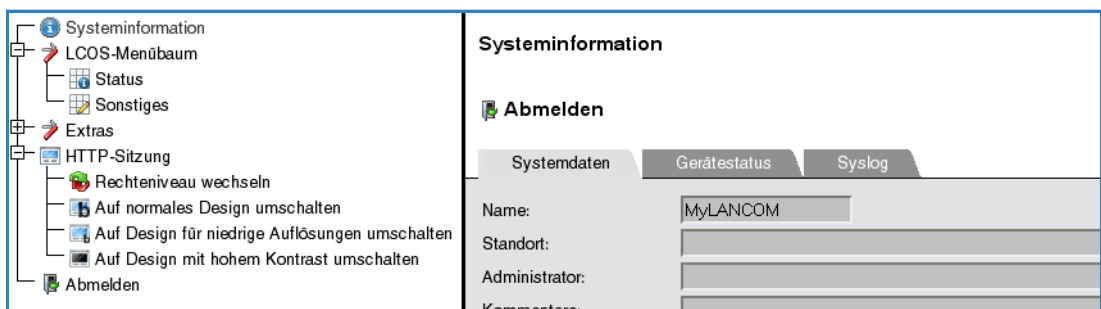
! Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für den Benutzer "root" die Befehle "readconfig" und "writeconfig" erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät auslesen und nach Änderung wieder einspielen kann ('Rechtezuweisung unter TACACS+' → Seite 25).

TACACS+-Anmeldung über WEBconfig

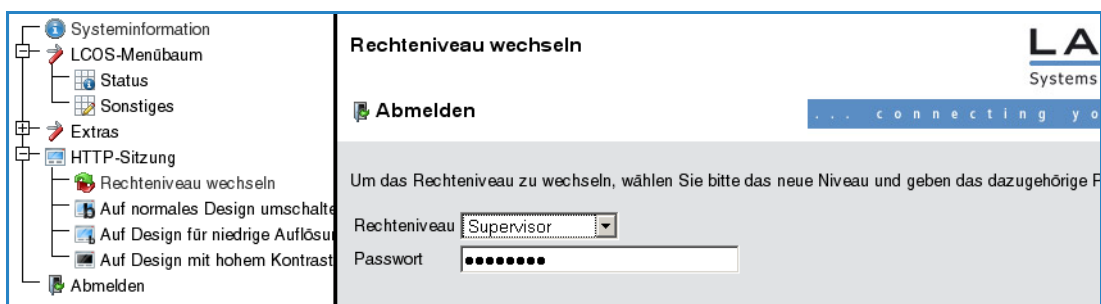
Die Anmeldung über WEBconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind. Geben Sie beim Login über WEBconfig den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung vorgenommen werden soll.



Das zugehörige Kennwort wird im nächsten Dialog abgefragt. Nach dem Login sieht der Benutzer zunächst nur eine eingeschränkte WEBconfig-Oberfläche. Wenn die Autorisierung nicht genutzt wird, haben alle Benutzer (außer der Benutzer "root") unter WEBconfig zunächst nur Leserechte.



Um weitere Rechte zu erhalten, klicken Sie im linken Bildschirmbereich den Link **Rechteniveau wechseln**.



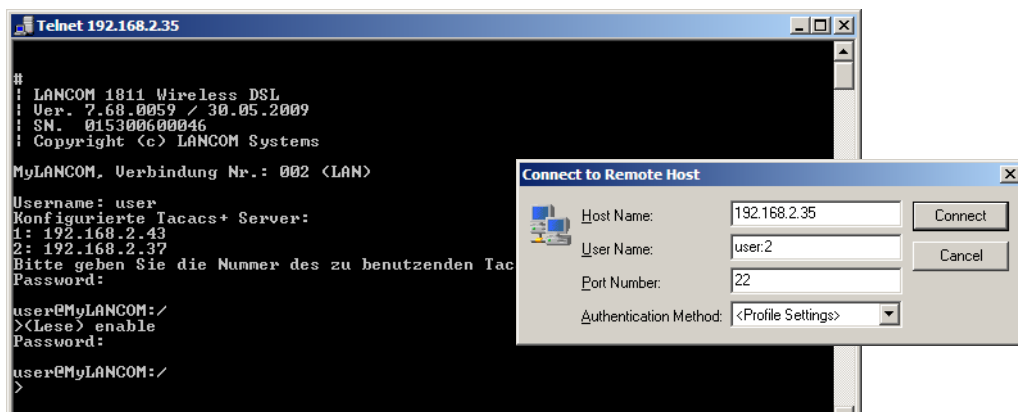
In diesem Dialog wählen Sie gewünschten Benutzerrechte und geben das passende Kennwort ein.

- ! Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als "enable"-Kennwörter konfiguriert.
- ! Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für die jeweiligen Benutzer die gewünschten Befehle erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät einsehen und bearbeiten kann ('Rechtezuweisung unter TACACS+' → Seite 25).

TACACS+-Anmeldung über Telnet oder SSH

Die Anmeldung über Telnet oder SSH an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind.

Geben Sie beim Login über Telnet den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung vorgenommen werden soll. Beim Login über SSH geben Sie den gewünschten Server mit einem Doppelpunkt getrennt nach dem Benutzernamen ein, also entweder "user:1" oder "user:2".



Nach dem Login haben alle Benutzer (außer dem Benutzer "root") zunächst nur Leserechte.

Um weitere Rechte zu erhalten, geben Sie den Befehl enable ein und geben das Kennwort ein. Die Rechte werden dann entsprechend dem konfigurierten Kennwort zugewiesen. Das enable-Kommando nimmt als Parameter die Zahlen 1-15. 1 ist das niedrigste, 15 das höchste Niveau. Ohne Parameter wird automatisch 15 angenommen.

- ! Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als "enable"-Kennwörter konfiguriert.
- ! Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für die jeweiligen Benutzer die gewünschten Befehle erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät einsehen und bearbeiten kann ('Rechtezuweisung unter TACACS+' → Seite 25).

A.10.5 Rechtezuweisung unter TACACS+

Die Rechte unter TACACS+ werden in bestimmten Leveln angegeben. Zur lokalen Authorisierung der Benutzer über das "enable"-Kommando unter Telnet/SSH bzw. das Rechteniveau unter WEBconfig werden die verschiedenen Administratorenrechte von LCOS auf die TACACS+-Level abgebildet:

TACACS+- Level	LCOS-Administratorenrechte
0	No rights
1	Read-Only
3	Read-Write
5	Read-Only-Limited Admin
7	Read-Write-Limited Admin
9	Read-Only Admin
11	Read-Write Admin
15	Supervisor (Root)

A.10.6 Authorisierung von Funktionen


Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen für die Konfiguration die entsprechenden Funktionen für den Benutzer im TACACS+-Server erlaubt sein. Tragen Sie die benötigten Werte in die Benutzerkonfiguration des TACACS+-Servers ein.

LANconfig

Befehl	Argumente	Bemerkung
readconfig	keine	Komplette Konfiguration auslesen
writeconfig	keine	Komplette Konfiguration schreiben


WEBconfig

Befehl	Argumente	Bemerkung
delRow	SNMP-ID der Tabelle	Zeile löschen
addRow	SNMP-ID der Tabelle	Zeile hinzufügen
editRow	SNMP-ID der Tabelle	Zeile bearbeiten
modifyItem	SNMP-ID des Menüeintrags	Bearbeiten eines Menüeintrags
viewTable	SNMP-ID der Tabelle	Tabelle anzeigen
viewRow	SNMP-ID der Zeile	Zeile anzeigen
setValue	SNMP-ID des Menüeintrags	Wert eines Menüeintrags setzen
listmenu	SNMP-ID des Menüs	Untermenü anzeigen
action	SNMP-ID der Aktion	Ausführen einer Aktion
reboot	keine	Gerät neu starten
\$URL	keine	Anzeige eines bestimmten URL

 Für den Zugriff über WEBconfig müssen alle URLs freigeschaltet werden, die während der Konfiguration an den TACACS+-Server übertragen werden. Mit der URL "config2" erlauben Sie z.B. grundsätzlich den Zugriff auf den Konfigurationszweig von LCOS über WEBconfig. Zusätzlich müssen die einzelnen Parameter freigeschaltet werden, die der Benutzer bearbeiten darf. Welche URLs WEBconfig an den TACACS+-Server übermittelt, können Sie z.B. mit dem entsprechenden Trace "trace+ tacacs" einsehen.

Telnet/SSH

Befehl	Argumente	Bemerkung
dir	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
list	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
ls	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
llong	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
del	SNMP-ID der Tabelle	Zeile löschen
delete	SNMP-ID der Tabelle	Zeile löschen
rm	SNMP-ID der Tabelle	Zeile löschen
cd	SNMP-ID des Zielverzeichnisses	Verzeichnis wechseln
add	SNMP-ID der Tabelle	Zeile hinzufügen
tab	SNMP-ID der Tabelle	Ändert die Reihenfolge der Spalten für das Hinzufügen von Werten
do	SNMP-ID der Aktion	Aktion ausführen
show	Name des Parameters	Information anzeigen
trace	Name des Parameters	Trace ausführen
time	Name des Parameters	Zeit einstellen
feature	Name des Parameters	Funktion hinzufügen
repeat	Name des Parameters	Befehl wiederholen
readmib	keine	SNMP-MIB auslesen
readconfig	keine	Komplette Konfiguration auslesen
readstatus	keine	Status- Menü auslesen
writeflash	keine	Firmware aktualisieren
activateimage	Name des Parameters	Anderes Firmware-Image aktivieren
ping	Name des Parameters	Starte Ping
wakeup	Name des Parameters	Sende Paket zum Aufwecken
linktest	Name des Parameters	WLAN- Linktest
writeconfig	keine	Komplette Konfiguration schreiben
ll2mdetect	keine	Starte LL2M-Erkennung
ll2mexec	Name des Parameters	LL2M-Befehl ausführen
scp	Name des Parameters	Sichere Kopie
rcp	Name des Parameters	Sichere Kopie
readscript	Name des Parameters	Skript auslesen
beginscript	keine	Start Skript
endscript	keine	Stop Skript
flash	Name des Parameters	Flash-Modus ein/ausschalten

 Für den Zugriff über Telnet müssen alle Parameter freigeschaltet werden, die der Benutzer bearbeiten darf. Welche Werte Telnet an den TACACS+-Server übermittelt, können Sie z.B. mit dem entsprechenden Trace "trace+ tacacs" einsehen.

SNMP

Befehl	Argumente	Bemerkung
get	SNMP-ID des Menüeintrags	Wert auslesen
set	SNMP-ID des Menüeintrags	Wert setzen

A.11 Versand von Anhängen mit dem mailto-Kommando

Mit dem mailto-Kommando in den Einträgen der Aktionstabelle oder Cron-Tabelle können bei bestimmten Ereignissen automatisch E-Mails mit Informationen über den Zustand der Geräte verschickt werden.

Mit der Erweiterung um Anhänge in den E-Mails können vor dem Versand der Mail beliebige Konsolen-Befehle auf dem Gerät ausgeführt werden, deren Ergebnis dann als Anhang mit der Mail verschickt werden. So lassen sich auch Inhalte von Tabellen oder Menüs (z.B. umfangreiche Statusmeldungen) per Mail versenden.

■ **Aktion (Aktionstabelle) oder Befehl (Cron-Tabelle) (max. 250 Zeichen)**

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung bzw. beim Erreichen der definierten Zeit ausgeführt werden soll. In jedem Eintrag darf nur eine Aktion ausgeführt werden.

Mögliche Werte für die Aktionen (maximal 250 Zeichen):

- `mailto:` – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus.

Mögliche Variablen zur Erweiterung der Aktionen:

- `attach='Konsolen-Befehl'`

Als Konsolen-Befehl können beliebige Befehle auf der Konsole genutzt werden, die zu einer sinnvollen Ausgabe von Informationen führen. Der Konsolen-Befehl wird in Backquotes (auch bekannt als Backticks) eingefasst. Dieses Zeichen wird mit Hilfe der Taste für den "Accent Grave" erzeugt.

Die Ausgabe des Konsolenbefehls wird in eine Text-Datei geschrieben und an die Mail angehängt. Vor die Ausgaben wird in den angehängten Text automatisch das Kommando und ein Zeit/Datumsstempel eingesetzt.

Default:

- leer

Beispiele:

Mit der folgenden Aktion können Sie den ADSL-Status per E-Mail versenden:

`mailto:admin@mycompany.de?subject=ADSL-Status?attach='dir /status/adsl'`.

Mit einer Aktion können auch durchaus mehrere Konsolenbefehle verschickt werden:

`mailto:admin@mycompany.de?subject=Statusmeldungen?attach='dir /status/adsl'?attach='dir /status/config'`

Die angehängten Texte werden als 'cmd1.txt', 'cmd2.txt' usw. bezeichnet.

A.12 Firmware-Upload für UMTS-Modul im LANCOM 1751 UMTS

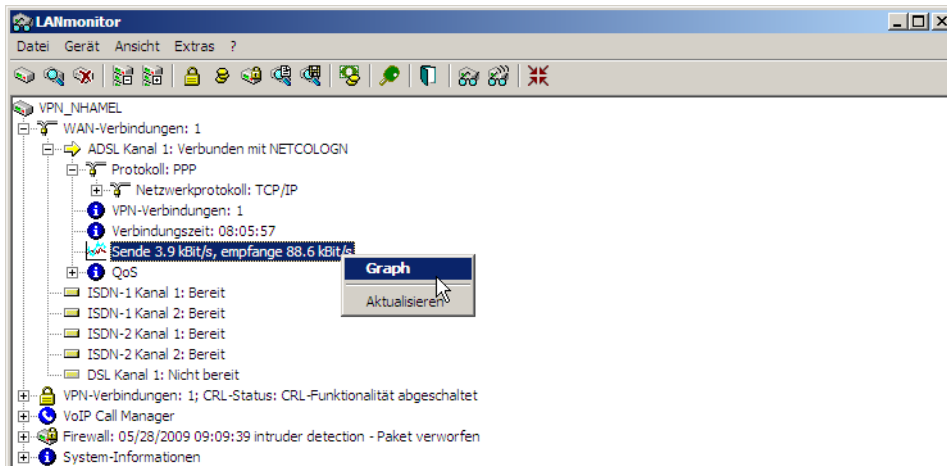
Für LANCOM 1751 UMTS mit einer Firmware ab der LCOS-Version 7.70 kann auch die Firmware für das UMTS-Modul komfortabel aktualisiert werden. Eine Firmware für das UMTS-Modul im UPX-Format kann auf allen Wegen in das LANCOM 1751 UMTS geladen werden, die auch für den Upload der LANCOM-Firmware bereitstehen.

A.13 Performance Monitoring im LANmonitor

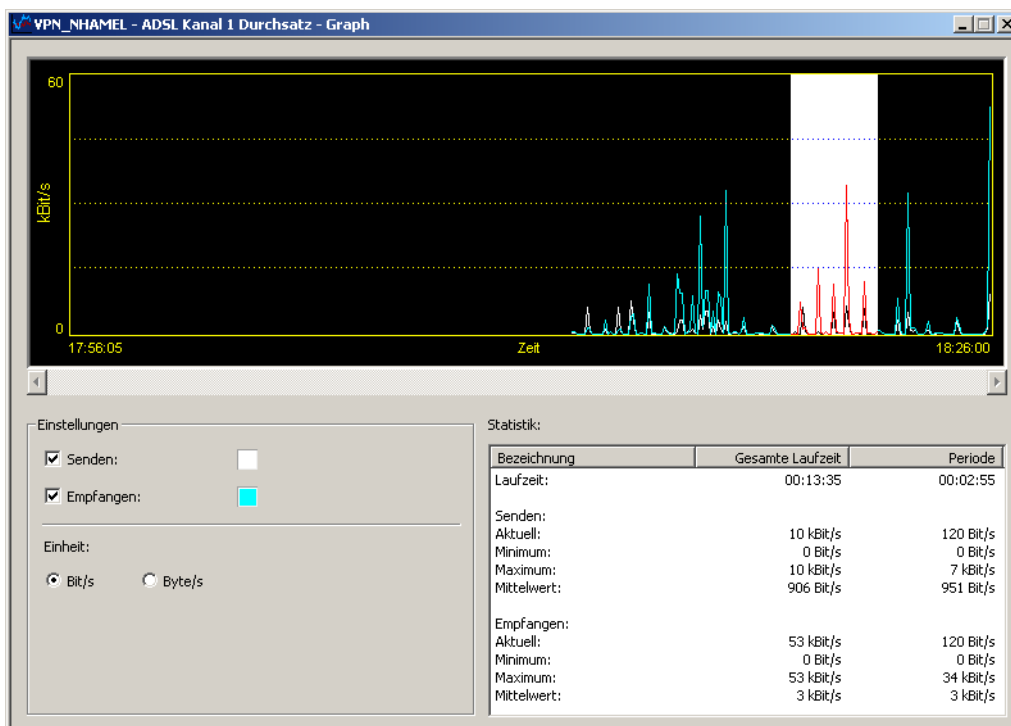
Der LANmonitor zeichnet verschiedene Kenngrößen der Geräte auf und stellt diese grafisch dar:

- Sende- und Empfangsrate für WAN-Verbindungen
- Sende- und Empfangsrate für Point-to-Point-Verbindungen
- Empfangssignalstärke für Point-to-Point-Verbindungen
- Linksignalstärke für Point-to-Point-Verbindungen
- Durchsatz für Point-to-Point-Verbindungen
- CPU-Last
- Freier Speicher
- Temperatur (nicht für alle Modelle verfügbar)

Die aktuellen Werte werden im LANmonitor direkt in der entsprechenden Gruppe angezeigt.



Mit einem Klick auf den Eintrag **Graph** im Kontextmenü öffnen Sie ein weiteres Fenster, in dem der zeitliche Verlauf der Kennwerte dargestellt wird.



Mit der linken Maustaste können Sie im aktuellen Graph eine Periode markieren, deren Werte in der Statistik separat angezeigt werden.

In diesem Dialog werden die aufgezeichneten Werte der letzten 24 Stunden dargestellt.

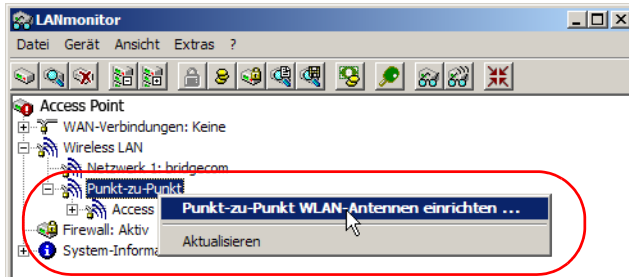
 Bitte beachten Sie, dass die angezeigte Werte gelöscht werden, sobald der Dialog geschlossen wird. Für eine längere Überwachung lassen Sie das Fenster dauerhaft geöffnet.

A.14 Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor

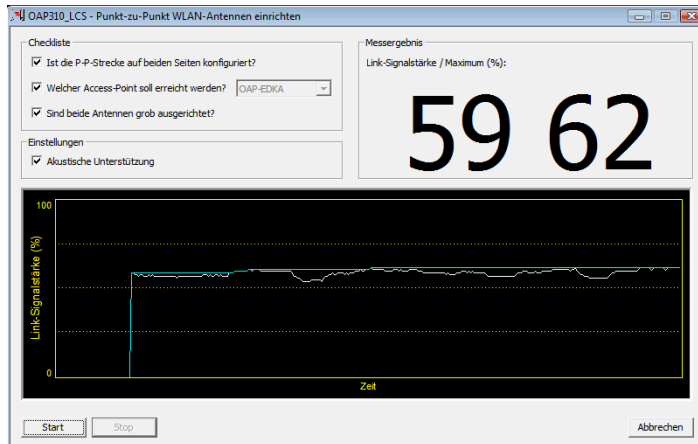
Um die Antennen für Punkt-zu-Punkt-Verbindungen möglichst gut ausrichten zu können, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden. Der LANmonitor bietet dabei neben der optischen Anzeige der Link-Signalstärke auch eine akustische Unterstützung.

Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontext-Menü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf 'Punkt-zu-Punkt WLAN-Antennen einrichten ...'

□ Einrichten von Punkt- zu- Punkt- Verbindungen mit dem LANmonitor



Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

Zur genaueren Ausrichtung kann eine akustische Unterstützung aktiviert werden. Mit dieser Option wird abhängig von der aktuellen Link-Signalstärke ein Ton über den PC ausgegeben. Die maximale Link-Signalstärke wird mit einem Dauerton signalisiert. Fällt die Link-Signalstärke unter das Maximum, wird der Abstand zum bisher erreichten Maximum durch Tonintervalle angezeigt. Je kürzer die Intervalle, um so näher liegt die Link-Signalstärke am Maximum.