A Addendum to LCOS-Version 7.7

A.1 Overview

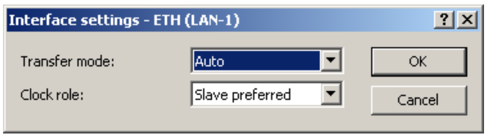
A.2 Extending the temperature range for L-305/310

Some applications require higher operating temperatures than the standard specified temperature range for the access points LANCOM L-305agn and LANCOM L-310agn. The operating temperature range for these two products can be extended to 45° C by limiting the speed of the Gigabit Ethernet interface to 100 Mbps.

As of LCOS version 7.70, the interface speed is automatically reduced to 100 Mbps if the standard maximum operating temperature of 35° C is exceeded. Often, these temperature increases are not long lasting (e.g. during a warm summer's day), so a temporary reduction of transfer rates has little effect on the device's operation.

The settings for the Ethernet port transfer speeds are to be found under the following paths:

LANconfig: Interfaces ▶ LAN ▶ Interface settings



Interface settings - ETH (LAN-1)

Transfer mode: Auto

Clock role: Slave preferred

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces

- **Transfer mode**

  Select the transfer mode for the connection to your local network.

  Possible values:

  □ Automatic, 10 Mbps half-duplex, 10 Mbps full-duplex, 100 Mbps half-duplex, 100 Mbps full-duplex, 100 Mbps automatic, 1000 Mbps full-duplex. The values available for selection here can vary between models.

  Special values:

  □ The setting "Automatic" enables the transfer mode to adapt automatically to the available connection. The maximum available transfer rate common to the two interfaces is taken.

  □ The setting "100 Mbps automatic" corresponds to the setting "Automatic", although the maximum speed that can be negotiated is 100 Mbps. If in doubt, this setting is to be preferred to setting a fixed 100 Mbps, as this avoids potential duplex conflicts.

  Default:

  □ Automatic

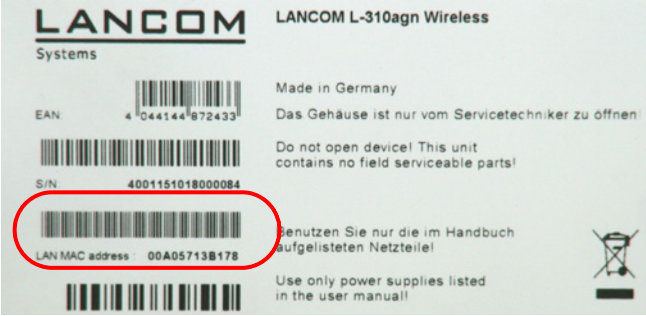
By manually selecting "100 Mbps full-duplex" some models with Gigabit interfaces and temperature sensors can operate within an extended temperature range. With these models, setting transfer mode to "Automatic" limits the speed to 100 Mbps for the time that the temperature inside the device exceeds a device-specific maximum. If the temperature sinks below the threshold, then the higher transfer rate is activated automatically. Interruptions from the re-negotiation of transfer rates is unnoticeable in the WLAN networks. Further information on permissible operating temperatures is to be found in the technical specifications for the device.

A.3 Standard encryption with WPA2

The factory settings (or those after resetting the device) are different in LANCOM access points than in LANCOM wireless routers.

- Unconfigured access points with standard factory settings cannot be commissioned by means of the WLAN interface. The WLAN modules are switched off and the devices search the LAN for a LANCOM WLAN controller which will supply a configuration profile.
- Unconfigured wireless routers with standard factory settings cannot be commissioned by means of the WLAN interface. Furthermore, encryption with WPA-PSK as described here is used as standard.

The preshared key (PSK) for the standard WPA encryption consists of the first letter “L” followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the LANCOM devices always begin with the character string “00A057”. You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as “LAN MAC address” that starts with “00A057”. The other numbers that may be found are **not** the LAN MAC address.


LANCOM
Systems
LANCOM L-310agn Wireless
EAN
4 044144 872433
Made in Germany
Das Gehäuse ist nur vom Servicetechniker zu öffnen!
Do not open device! This unit contains no field serviceable parts!
S/N
4001151018000084
Benutzen Sie nur die im Handbuch aufgelisteten Netzteile!
LAN MAC address : 00A05713B178
Use only power supplies listed in the user manual!

A device with the LAN MAC address “00A05713B178” thus has a preshared key of “L00A05713B178”. This key is entered into the ‘WPA or private WEP settings’ of the device for each logical WLAN network as ‘Key 1/Passphrase’.

To use a WLAN adapter to establish a connection to a LANCOM wireless router that has factory settings, the WPA encryption must be activated for the WLAN adapter and the standard 13-character preshared key.

After registering for the first time, change the WPA preshared key to ensure that you have a secure connection.

A.4 APSD – Automatic Power Save Delivery

A.4.1 Introduction

Automatic Power Save Delivery (APSD) is an extension to the IEEE 802.11e standard. APSD is available in two versions:

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

These two methods differ in the way that they use the transmission channels, among others. LANCOM access points and wireless routers support U-APSD, which forms the basis for the WiFi-certified WMM Power Save (WMMPS).

U-APSD allows WLAN devices to save considerable amounts of energy. This function has come into demand due to the increasing use of WLAN-capable telephones (Voice over WLAN – VoWLAN). Activating U-APSD for a wireless LAN enables WLAN devices making calls to switch into "doze mode" while they wait for the next data packet. Transmission of VoIP data takes place in a fixed time pattern—WLAN devices synchronize their phases of activity with this cycle, so that they are ready in good time to receive the next packet. This significantly reduces power consumption and the batteries provide a considerably longer call time.

The precise behavior of the power-saving mode is negotiated between the access point and WLAN client under consideration of the actual application at hand. This makes APSD much more flexible than former power saving methods, referred to in this context as "legacy power save".

A.4.2 Configuration

WEBconfig: LCOS menu tree ▶ Setup ▶ Interfaces ▶ WLAN ▶ Network

- **APSD**

  Activates APSD power saving for this logical WLAN network.

  Possible values:

  □ On, off

  Default:

  □ Off

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

A.4.3 Statistics

WEBconfig: LCOS menu tree ▶ Status ▶ WLAN ▶ Networks

- **APSD**

  Indicates whether APSD is activated or deactivated for the respective WLAN (SSID). APSD is only indicated as active if it is activated in the settings for the logical WLAN and also if the general QoS module is activated.

- **WEBconfig: LCOS menu tree ▶ Status ▶ WLAN ▶ Station table**

  Displays the access categories for which associated WLAN clients are using APSD:

  □ Voice (highest priority)

  □ Video

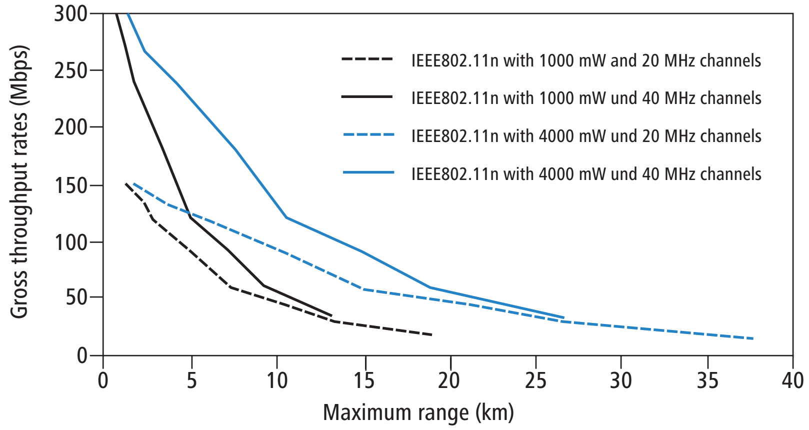
  □ Best effort (including data traffic from legacy power-save clients)

  □ Background (lowest priority).

A.5 BFWA – higher transmission power for longer ranges

BFWA stands for Broadband Fixed Wireless Access. A typical application would be to support a network node that provides Internet to subscribers connected to it. In Germany, the frequencies were provided as part of a general frequency allocation by the German Federal Network Agency. BFWA transmits at a frequency of 5.8 GHz. The maximum permitted transmission power for the operation of BFWA wireless bridges is 4000 mW EIRP (Equivalent Isotropic Radiated Power).

These high transmission powers are the advantage from BFWA. Without BFWA, the maximum permissible transmission power for outdoor WLAN directional radio systems in the 5-GHz band is limited to 1000 mW. This increases the legal transmission power to allow the same directional radio systems to function over significantly longer distances.



LANCOM access points based on 802.11n and all of the current LANCOM 54 Mbps access points support BFWA as of LCOS version 7.70. For older access points, support depends on the chipset (AR-5414 chipset). LANCOM Support can inform you whether these models are able to support BFWA.

For further information see the tech-paper "Broadband Fixed Wireless Access (BFWA)", available for download from www.lancom.eu.

A.6 Restarting RADIUS accounting

The accounting function in the LANCOM can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate a restart.

WEBconfig: LCOS menu tree ▶ Setup ▶ WLAN ▶ RADIUS accounting

- **Restart accounting**

  Terminates all current accounting sessions and opens new accounting sessions on the RADIUS server.

A.7 Voucher for Public Spot with time budget

A.7.1 Introduction

With the Voucher Printing Wizard, setting up time-limited access to a wireless LAN Public Spot takes just a few mouse-clicks. All that is required is to set the access-account time budget; the user name and password are generated automatically and entered into the configuration of the LANCOM device. As a result, a personalized voucher is printed out that contains the information required for a user to register with a wireless LAN Public Spot for a limited period of time.

Users may not want to access the Public Spot WLAN at the moment when the voucher is printed out. For this situation, vouchers can be printed out in advance. The access is set up so that the time budget only starts running when the user logs in for the first time. A maximum period of validity is also defined, after which the access account is automatically deleted, even if the access time budget has not been used up.

Public Spot access with a time limit can only be set up if the LANCOM is set with the correct time.

In LCOS versions prior to 7.70, Public Spot access accounts were entered into the user list for the Public Spot module with the Wizard. As of LCOS version 7.70, the Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. To be able to use Public Spot access accounts, the RADIUS server has to be configured in the LANCOM. Please observe the notices about this under 'Configuring the RADIUS server to operate a Public Spot' → Page 5.

A.7.2 Setting up Public-Spot users and printing vouchers

To set up a Public-Spot access account, the employee opens a browser and enters the IP address of the wireless router or access point (for example by means of a link on the desktop) and logs in with the appropriate user name and password. If this administrator access account is configured appropriately, the user will only be able add new Public Spot users after starting the Wizard.

① After starting the Wizard, set the time budget for the access.

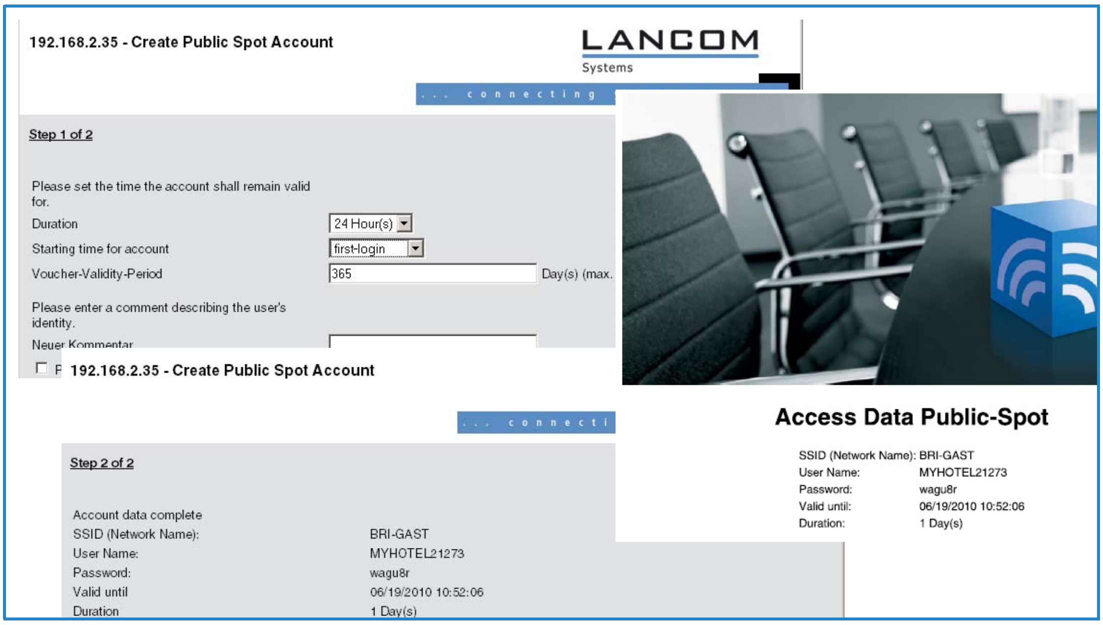
② Select whether the access should be activated immediately or after the first login.

③ If the time budget is only to be consumed after logging in, specify the number of days after which the access account is to expire (validity period).

④ The commentary field gives you the option of entering text to identify the user (e.g. name or room number of the guest). As an alternative to the predefined commentary field, you can use up to five customer-specific commentary fields.

⑤ You then click on **Save and print out user data** to save the access data to the device+ and print it out.

You will find notices on the rights and obligations that apply to operators of Public Spot accesses in the LANCOM White Paper on the subject under www.lancom.eu.



192.168.2.35 - Create Public Spot Account

Step 1 of 2

Please set the time the account shall remain valid for.

Duration	24 Hour(s)
Starting time for account	first-login
Voucher-Validity-Period	365 Day(s) (max.

Please enter a comment describing the user's identity.

Neuer Kommentar

192.168.2.35 - Create Public Spot Account

Step 2 of 2

Account data complete

SSID (Network Name):	BRI-GAST
User Name:	MYHOTEL21273
Password:	wagu8r
Valid until	06/19/2010 10:52:06
Duration	1 Day(s)

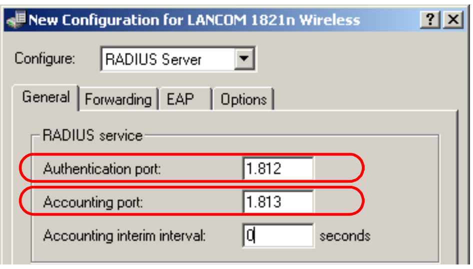
Access Data Public-Spot

SSID (Network Name):	BRI-GAST
User Name:	MYHOTEL21273
Password:	wagu8r
Valid until:	06/19/2010 10:52:06
Duration:	1 Day(s)

A.7.3 Configuring the RADIUS server to operate a Public Spot

In LCOS versions prior to 7.70, Public Spot access accounts were defined by entering users into into the Public Spot module's user list by using the Wizard. As of LCOS version 7.70, the Wizard no longer stores the Public Spot access accounts in this list, but in the user database of the internal RADIUS server instead. In order to use Public Spot access accounts, the RADIUS server **must** be configured and the Public Spot module must be set to use the RADIUS server.

① In order to use the user database in the internal RADIUS server, the RADIUS server in the LANCOM must be activated first. Activate the RADIUS server by entering authentication and accounting ports. Use the authentication port 1,812 and the accounting port 1,813.



New Configuration for LANCOM 1821n Wireless

Configure: RADIUS Server

RADIUS service

Authentication port:	1.812
Accounting port:	1.813
Accounting interim interval:	0 seconds

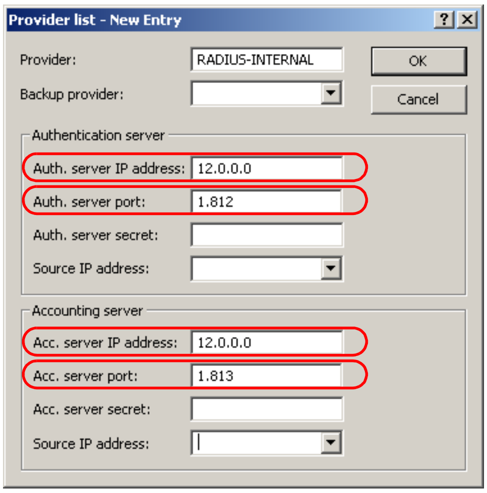
LANconfig: RADIUS ▶ General

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server ▶ Authentication port and Accounting port

② In order for the Public Spot access accounts to be authenticated by the LANCOM's internal RADIUS server, the Public Spot must know the address of the RADIUS server. To ensure that this is the case, create a new entry to define the internal RADIUS server as a "Provider". Enter the IP address for the LANCOM with the activated RADIUS server as the authentication and accounting server.

! If the Public Spot and the RADIUS server are provided by the same LANCOM, enter the device's internal loopback address (127.0.0.1) here.

③ Use the authentication and accounting port settings from the RADIUS server (1,812 and 1,813).



Provider: RADIUS-INTERNAL

Backup provider:

Auth. server IP address: 12.0.0.0

Auth. server port: 1.812

Auth. server secret:

Source IP address:

Acc. server IP address: 12.0.0.0

Acc. server port: 1.813

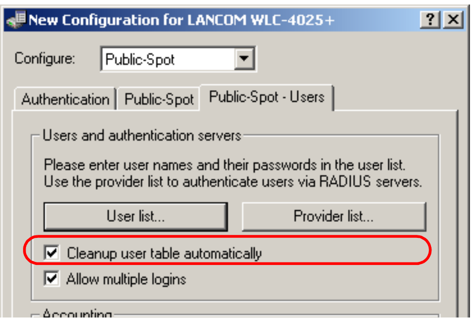
Acc. server secret:

Source IP address:

LANconfig: Public Spot ▶ Public Spot users ▶ Provider list

WEBconfig: LCOS menu tree ▶ Setup ▶ Public Spot module ▶ Port table

④ In the Public Spot module, activate the "Cleanup user table automatically" option to ensure that unwanted entries are automatically deleted.



Configure: Public-Spot

Please enter user names and their passwords in the user list.
Use the provider list to authenticate users via RADIUS servers.

☑ Cleanup user table automatically

☑ Allow multiple logins

LANconfig: Public Spot ▶ Public Spot users

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server

After updating to LCOS 7.70, user accounts created in the Public Spot module's user list with previous versions of LCOS remain valid.

A.7.4 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate internal WLAN users by IEEE 802.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. The WLAN controller then forwards the RADIUS requests to the external RADIUS server.

The settings described below are only necessary if you are operating an external RADIUS server in addition to the Public Spot in the LANCOM.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.

Realm tagging for RADIUS forwarding

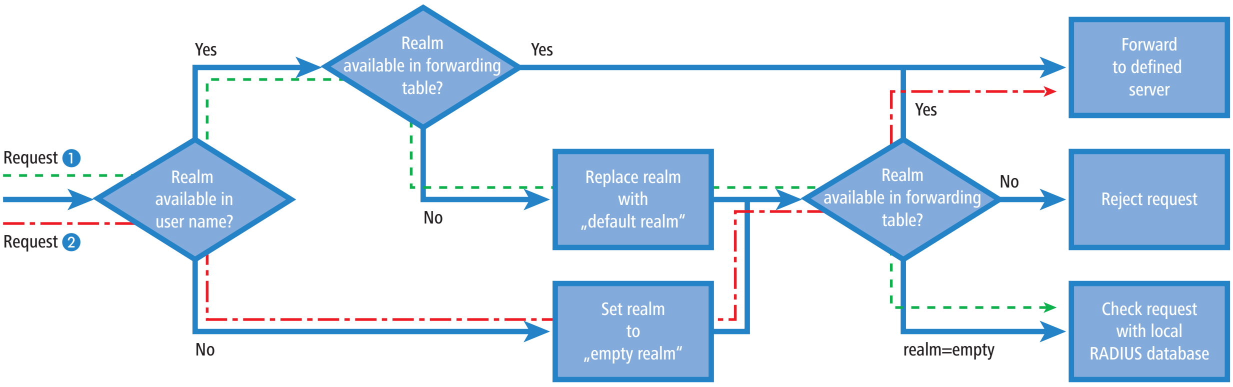
Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. Realms are used for addressing domains, in which user accounts are valid. Realms can be sent with the authentication requests to the WLAN controller's RADIUS server. Alternatively, the RADIUS server can modify the realms in accordance with the following rules for RADIUS forwarding:

- The value defined as the "Default realm" replaces an existing realm of an incoming request, if no forwarding is is defined for this realm.
- The value defined under "empty realm" is used **only if** the incoming user name **does not yet have** a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no corresponding entry can be found in the forwarding table, the request will be rejected.

> If an empty realm is detected, then the authentication request is **always** checked against the LANCOM's internal RADIUS database.

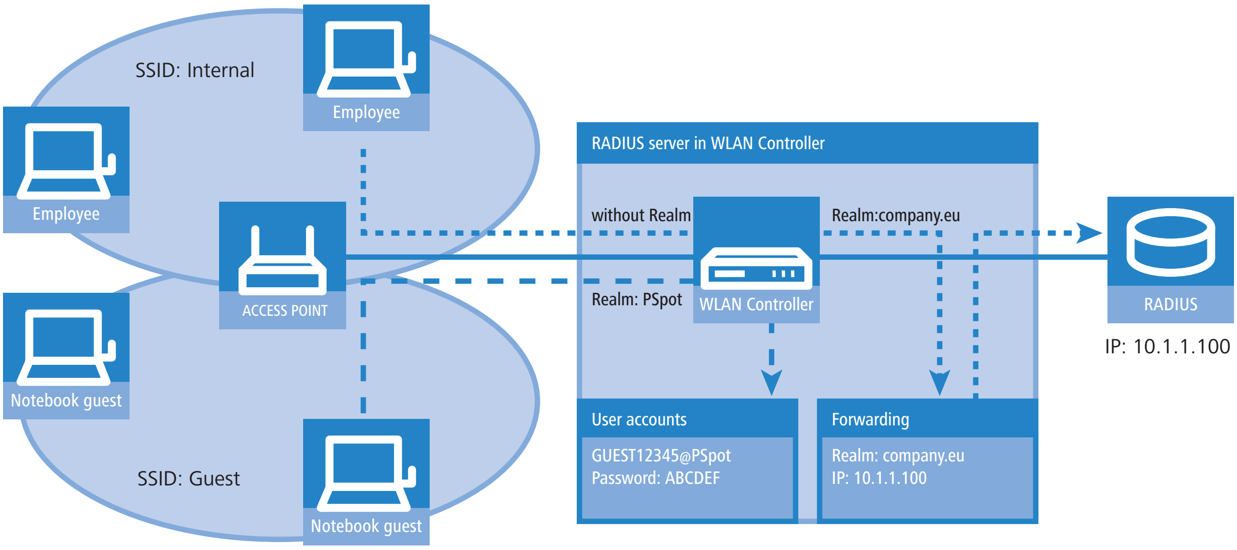
The following flow chart shows the working principle of the RADIUS server when processing realms:


Request 1
Request 2
Realm available in user name?
Yes
No
Realm available in forwarding table?
Yes
No
Replace realm with „default realm"
Set realm to „empty realm"
Realm available in forwarding table?
Yes
No
realm=empty
Forward to defined server
Reject request
Check request with local RADIUS database

Using different realm tags allows different RADIUS servers to be targeted with requests. The decision making process can be tracked in the flow chart.

1. Because the user names for guest access accounts are generated automatically, they can use the realm "PSpot". Because the forwarding table does not contain this entry, all authentication requests with this realm are forwarded to the internal RADIUS server.

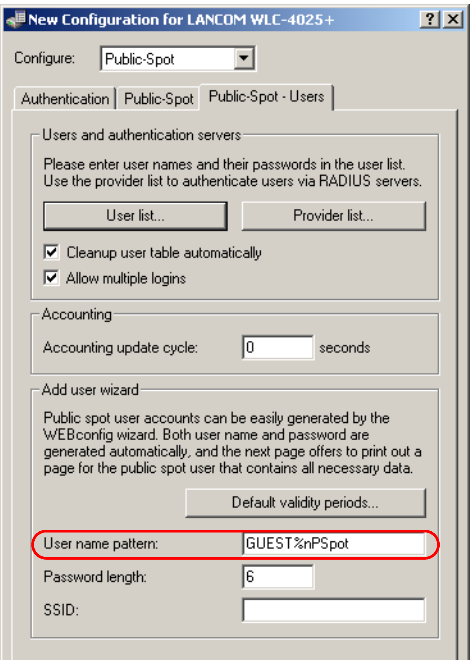
2. To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the LANCOM can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain of the company "company.eu". The information specified in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.



Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

① In the Public Spot, adapt the pattern of user names such that a unique realm can be used. For example, the pattern 'GUEST%n@PSpot" generates user names that appear like "GUEST12345@PSpot".



Configure: Public-Spot

Users and authentication servers

Please enter user names and their passwords in the user list. Use the provider list to authenticate users via RADIUS servers.

☑ Cleanup user table automatically

☑ Allow multiple logins

Accounting

Accounting update cycle: 0 seconds

Add user wizard

Public spot user accounts can be easily generated by the WEBconfig wizard. Both user name and password are generated automatically, and the next page offers to print out a page for the public spot user that contains all necessary data.

User name pattern: GUEST%nPSpot

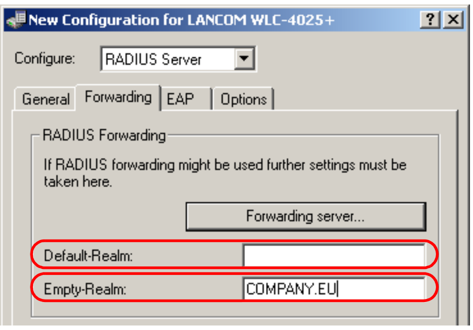
Password length: 6

SSID:

LANconfig: Public Spot ▶ Public Spot users

WEBconfig: LCOS menu tree ▶ Setup ▶ Public Spot module

② In the WLAN controller's RADIUS server, define an "empty realm" (e.g. "COMPANY.EU"). This realm is used for all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controllers RADIUS server from inserting a realm, the "Default realm" field must be left empty.



Configure: RADIUS Server

RADIUS Forwarding

If RADIUS forwarding might be used further settings must be taken here.

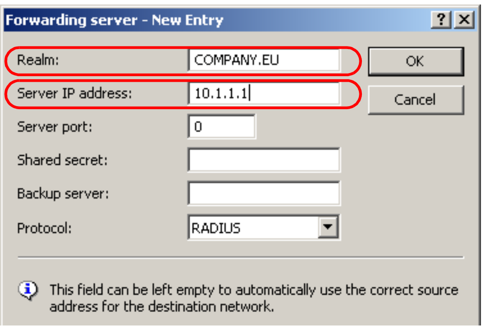
Default-Realm:

Empty-Realm: COMPANY.EU

LANconfig: RADIUS server ▶ Forwarding

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server

③ In order for authentication requests from internal users to be forwarded to the external RADIUS server, suitable entries must be entered into the forwarding settings. The realm "COMPANY.EU" causes all incoming RADIUS requests to be forwarded to the specified IP address.



Realm: COMPANY.EU

Server IP address: 10.1.1.1

Server port: 0

Shared secret:

Backup server:

Protocol: RADIUS

This field can be left empty to automatically use the correct source address for the destination network.

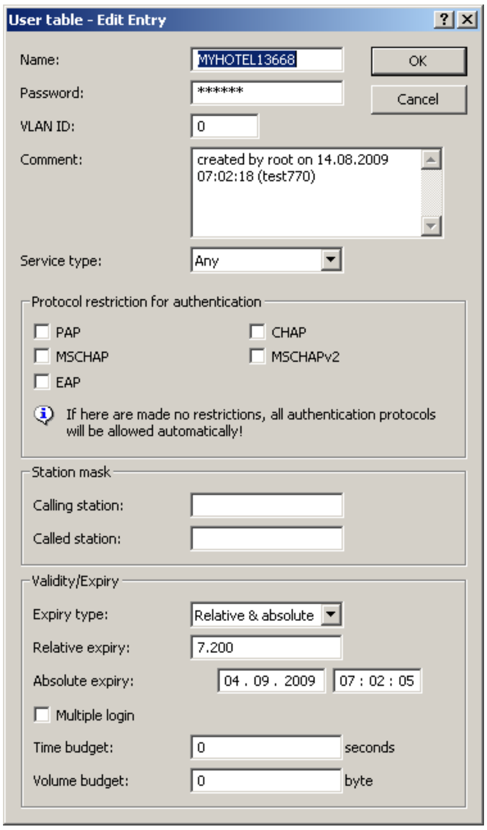
LANconfig: RADIUS server ▶ Forwarding ▶ Forwarding server

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Servers ▶ Forward servers

④ Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

A.8 Extensions to the RADIUS server

To set up Public Spot users with time and volume budgets, additional parameters have to be entered into the RADIUS server user table.



Name: MYHOTEL13668

Password: ******

VLAN ID: 0

Comment: created by root on 14.08.2009 07:02:18 (test770)

Service type: Any

Protocol restriction for authentication

□ PAP □ CHAP

□ MSCHAP □ MSCHAPv2

□ EAP

If here are made no restrictions, all authentication protocols will be allowed automatically!

Station mask

Calling station:

Called station:

Validity/Expiry

Expiry type: Relative & absolute

Relative expiry: 7.200

Absolute expiry: 04 . 09 . 2009 07 : 02 : 05

□ Multiple login

Time budget: 0 seconds

Volume budget: 0 byte

LANconfig: RADIUS ▶ General ▶ User accounts

WEBconfig: LCOS menu tree ▶ Setup ▶ RADIUS ▶ Server ▶ Users

- **Multiple logins**

  Allows a single user account to login multiple times simultaneously.

  Possible values:

  □ Yes, No

  Default:

  □ Yes

The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

- **Expiry type**

  This option defines how the validity period is limited for a user account.

  Possible values:

  □ Absolute: The validity of the user account terminates at a set time.

  □ Relative: The validity of the user account terminates a certain period of time after the first user login.

  Default:

  □ Blank: The user account never expires, unless a predefined time or volume budget expires.

The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.

! The device must have a valid time in order for the device to work with user-account time budgets.

- **Abs. expiry**

  If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

  Possible values:

  □ Valid time information (date and time). Max. 20 characters from `0123456789/:.Pp`

  Default:

  □ Blank

  Special values:

  □ 0 switches off the monitoring of the absolute expiry time.

- **Rel. expiry**

  If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.

  Possible values:

  □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  □ 0

  Special values:

  □ 0 switches off the monitoring of the relative expiry time.

- **Time budget**

  The maximum duration of access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

  Possible values:

  □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  □ 0

  Special values:

  □ 0 switches off the monitoring of the time budget.

- **Volume budget**

  The maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

  Possible values:

  □ Time span in seconds. Max. 10 characters from `0123456789`

  Default:

  □ 0

  Special values:

  □ 0 switches off the monitoring of data volume.

- **Comment**

  Comment on this entry.

- **Service type**

  The service type is a special attribute of the RADIUS protocol. The NAS (Network Access Server) sends this with the authentication request. The response to this request is only positive if the requested service type agrees with the user account service type.

  Possible values:

  □ Framed: For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.

  □ Login: For Public-Spot logins.

  □ Auth. only: For RADIUS authentication of dialup peers via PPP.

  □ Any

  Default:

  □ Any

! The number of entries permissible with the service type "any" or "login" is 64 or 256, depending on the model. This means that the table is not completely filled with entries for Public Spot access accounts (using the service type "Any") and it enables the parallel use of logins via 802.1x.

A.9 IGMP snooping

A.9.1 Introduction

All LANCOM devices with wireless LAN interfaces feature a "LAN bridge", a software entity for transferring data between the Ethernet ports and the WLAN interface(s). In many ways the LAN bridge works like a switch. The core task of a switch, as opposed to a hub, is to forward packets precisely to the port which the relevant user is connected to. Based on the incoming data packets, the switch automatically creates a table listing the senders' MAC addresses and their ports.

If the table contains the destination address for an incoming packet, the switch forwards the packet to the corresponding port. If the destination address is not in the table, the switch forwards the packet to all ports. This means that a switch can only deliver a packet precisely if the destination address appeared earlier in a packet arriving at a certain port from the sender's address. However, broadcast or multicast packets can never be entered as a sender address into a packet, and so these packets end up being "flooded" to all ports.

This may be the correct action for broadcasts which are supposed to reach all available receivers, but this may not be the case for multicasts. Multicasts are generally aimed at a certain group of receivers within a network, but not all of them:

- For example, video streams are frequently transmitted as multicasts, but not all of the network stations are intended to receive that stream.
- Various applications in the medical field rely on multicasts to send data to certain terminal devices, but this data should not be available to all stations.

A LAN bridge in the LANCOM will have ports to which no multicast recipients are connected. This "unnecessary" transmission of multicasts to ports without any receivers is not an error, but it can compromise overall performance.

- Many stations are unable to reject the unwanted multicasts in their hardware. Instead, the packets are forwarded to higher protocol layers, which leads to an increase in CPU load.
- WLANs are particularly susceptible to bandwidth restrictions due to multicasts if none of the associated WLAN clients want to receive the multicast.

The TCP/IP protocol suite defines a protocol called IGMP that allows network stations to register their desire to receive certain IP multicasts to their router. Stations carry out a multicast registration with their router to subscribe to certain multicast groups which deliver the relevant packets. IGMP makes use of Join messages and Leave messages to register and de-register respectively.

i Information about which multicast groups a station can or should join are available from other protocols than IGMP.

As a layer-3 protocol, IGMP only performs multicast guiding/routing for whole IP subnets. However, network devices such as bridges, switches or WLAN access points only forward the packets on layer 2, meaning that IGMP itself does not help in any way to further guide multicast traffic through this substructure. For this reason, the bridges use the multicast registrations between stations and routers to receive additional information for targeting the distribution of multicasts. IP multicasts only need to be forwarded to an interface where a router is located that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets. This method is called IGMP snooping. The bridges, which normally use the MAC on layer 2 for packet forwarding, thus additionally use the layer 3 information in the IP multicast packets.

For more detailed description of the functions of IGMP snooping in LCOS, we have to differentiate between two important terms:

- A port is "member" of a multicast group if at least one station connected to it wishes to receive the packets for a certain multicast address. Multicast registration can be dynamic via IGMP snooping or configured manually.
- A port is a "router port" if it is connected to a router that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets.
- A multicast group is "unregistered" if none of the interfaces attached to the bridge is a member of this multicast group.

A.9.2 IGMP snooping operation

Whenever a packet is received, the bridge initially determines whether it is a unicast, broadcast, or multicast packet. For broadcast and unicast packets, the bridge operates in the usual way, i.e. it floods to all ports or sends to a specific port based on the MAC table entry for the receiver.

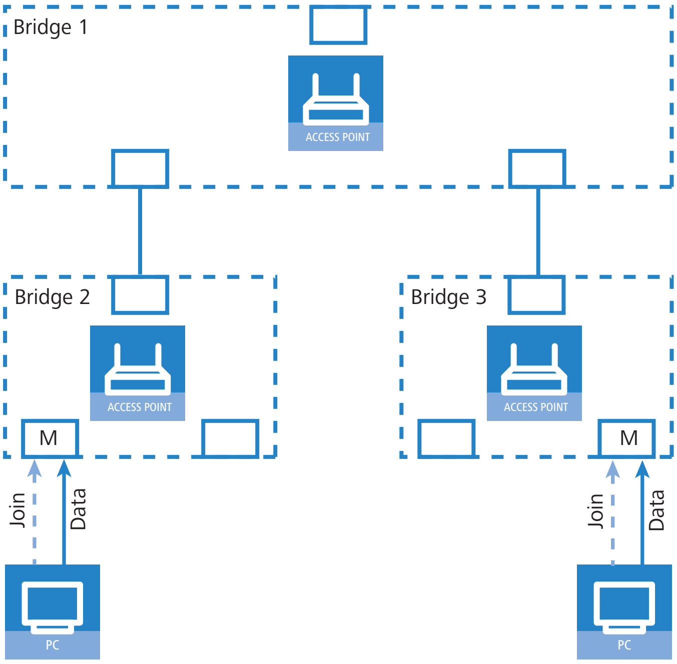
Two types of IP multicast packet are differentiated (whereby packets which are truncated or contain an invalid checksum are discarded entirely):

- IGMP messages are handled in different ways depending on their content:
  - A Join message results in the incoming port becoming member of the respective multicast group. This message is forwarded to router ports only.
  - Similarly, a Leave message results in the incoming port being removed from the multicast group's member list. This message is also forwarded to router ports only.
  - An incoming IGMP query results in the port being marked as a router port. These messages are flooded to all interfaces.
  - All other messages are flooded to all interfaces—no ports experience a change of state.
- If an IP multicast packet does not contain an IGMP message, the IP destination address is examined. Packets for the destination address "224.0.0.x" are flooded to all ports because this is a "reserved" range. For all other packets the destination address is looked up in the IGMP membership table:
  - If the address is found, the packet is forwarded according to the membership stored in the table.
  - If the address is not found, the packet may either be discarded, flooded to all ports, or forwarded exclusively to all router ports (depending on the configuration).

  In either case, packets are forwarded to all router ports.

A.9.3 IGMP snooping through multiple bridges

As described, IGMP snooping only forwards incoming Join or Leave messages via router ports. In a structure with multiple bridges, initially none of the ports are router ports or members of a multicast group. If a station connected to the bridge registers with a multicast group, the port automatically becomes a member of this group. However, none of the ports are router ports at this phase, so the Join messages are not forwarded anywhere. Other bridges thus receive no information about the port's membership with the multicast group.



Consequently, bridges must have router ports in order for membership information to be propagated. Since the ports of a bridge only become router ports in the case of IGMP queries, one of the multicast-capable routers in the network must take over the task of distributing the necessary IGMP queries throughout the network. This router is referred to as the IGMP querier. If the network does not contain a multicast router, the LANCOM access points are capable of simulating a querier. To avoid parallel queries arriving from various queriers, a querier will deactivate itself if it discovers another querier with a lower IP number. The distribution of IGMP information by the querier can be explained with the following example:

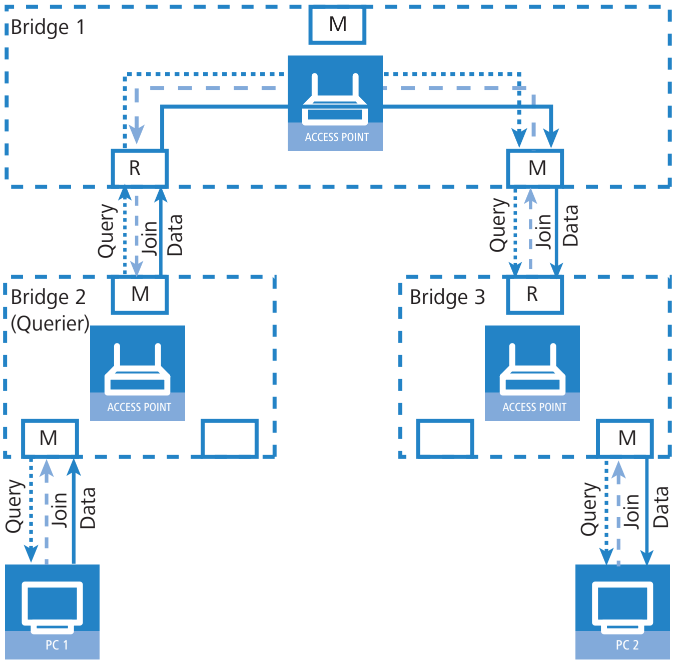
① The querier (Bridge 2 in this example) regularly sends out IGMP queries on all ports of bridge 2 (dotted lines). The next bridge (Bridge 1) receives the query on a port which is then marked as a router port (R). PC 1 responds to this query with a Join message for all multicast groups (light dashed lines) that it wishes to join. The port connecting PC 1 to Bridge 2 then becomes a member of the multicasting group(s).

② In addition to this, Bridge 1 sends the queries on all other ports to the bridges and stations lower down in the structure. In Bridge 3 the port receiving the query becomes a router port (R).

③ The station (PC 2) connected to bridge 3 responds to this query with a Join message for all registered multicast groups. The port connecting PC 2 to Bridge 3 then becomes a member of the multicasting group(s).

④ Bridge 3 forwards this Join message to Bridge 1 over the router port. The receiving port on Bridge 1 thus also takes on membership of the multicast groups that PC 2 has registered for.

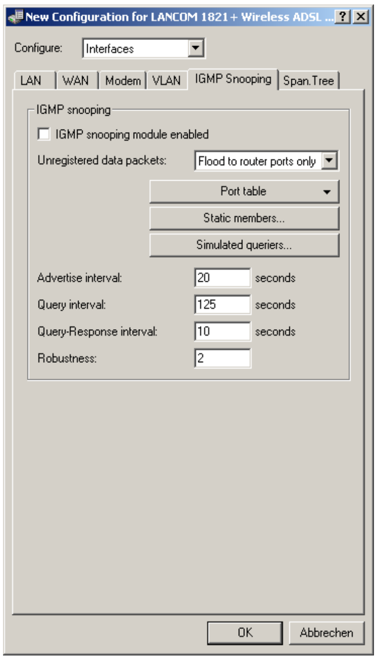
⑤ In the final step, Bridge 1 forwards the Join message from PC 2 via the router port to Bridge 2, where the receiving port also takes on membership of PC 2's multicast groups.



If PC 1 now transmits a multicast for which PC 2 has registered, all of the bridges (2, 1 and then 3) forward the packets to PC 2 via the member port.

A.9.4 Configuration

General settings



Configure: Interfaces

IGMP snooping

☐ IGMP snooping module enabled

Unregistered data packets: Flood to router ports only

Advertise interval: 20 seconds

Query interval: 125 seconds

Query-Response interval: 10 seconds

Robustness: 2

LANconfig: Interfaces ▶ IGMP snooping

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping

- **Operating**

  Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

  Possible values:

  - Yes, No

  Default:

  - No

ⓘ If this function is deactivated, all IP multicast packets are sent on all ports. If the device operating state changes, the IGMP snooping function is completely reset, i.e. all dynamically learned values are lost (membership, router-port states).

- **Query interval**

  Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships age, expire, and are then deleted.

  - After the startup phase, the querier sends IGMP queries in this interval.
  - A querier returns to the querier status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".
  - A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

  Possible values:

  - 10-figure number greater than 0.

  Default:

  - 125

(!) The query interval must be greater than the query response interval.

- **Query response interval**

  Interval in seconds influencing the timing between IGMP queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

Possible values:

- 10-figure number greater than 0.

Default:

- 10

The query response interval must be less than the query interval.

Robustness

This value defined the robustness of the IGMP protocol. This option tolerates packet losses of IGMP queries with respect to Join messages.

Possible values:

- 10-figure number greater than 0.

Default:

- 2

Advertise interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries.

Possible values:

- 4 to 180 seconds.

Default:

- 20

Unregistered data packet handling

This setting defines the handling of multicast data packets with a destination address outside the 224.0.0.x range and for which neither static memberships were defined nor were dynamic memberships learned.

Possible values:

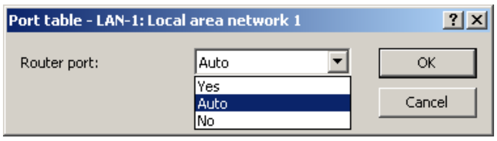
- Router ports only: Sends these packets to all router ports.
- Flood: Sends these packets to all ports.
- Discard: Drops these packets.

Default:

- Router ports only

Port settings

This table defines the port-related settings for IGMP snooping.



Port table - LAN-1: Local area network 1

Router port: Auto

LANconfig: Interfaces ▶ IGMP snooping ▶ Port table

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Port settings

Port

The port for which the settings apply.

Possible values:

- Selects a port from the list of those available in the device.

Default:

- N/A

- **Router port**

  This option defines the port's behavior.

  Possible values:

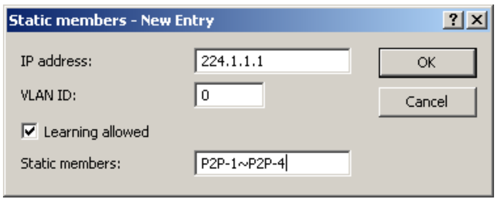
  - □ Yes: This port will always work as a router port, irrespective of IGMP queries or router messages received at this port.
  - □ No: This port will never work as a router port, irrespective of IGMP queries or router messages received at this port.
  - □ Auto: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if no packets are received for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

  Default:

  - □ Auto

Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.



Static members - New Entry

IP address: 224.1.1.1

VLAN ID: 0

☑ Learning allowed

Static members: P2P-1~P2P-4

LANconfig: Interfaces ▶ IGMP snooping ▶ Static members

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Static members

- **Address**

  The IP address of the manually defined multicast group.

  Possible values:

  - □ Valid IP multicast address.

  Default:

  - □ Blank

- **VLAN ID**

  The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

  Possible values:

  - □ 0 to 4096.

  Default:

  - □ 0

  Special values:

  - □ If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

- **Allow learning**

  This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

  Possible values:

  - □ Yes, No.

  Default:

  - □ Yes

- **Static members**

  These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received.

  Possible values:

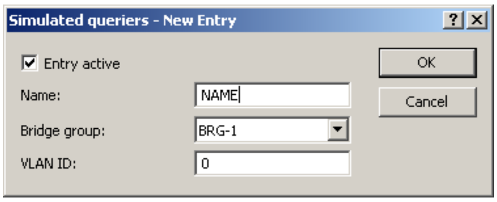
- Comma-separated list of the desired ports, max. 215 alphanumerical characters.

Default:

- Blank

Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.



☑ Entry active
Name: NAME
Bridge group: BRG-1
VLAN ID: 0

LANconfig: Interfaces ▶ IGMP snooping ▶ Simulated queriers

WEBconfig: LCOS menu tree ▶ Setup ▶ LAN bridge ▶ IGMP snooping ▶ Simulated queriers

- **Name**

  Name of the querier instance

  Possible values:

  - 8 alphanumerical characters.

  Default:

  - Blank

- **Operating**

  Activates or deactivates the querier instance

  Possible values:

  - Yes, No.

  Default:

  - No

- **Bridge group**

  Limits the querier instance to a certain bridge group.

  Possible values:

  - Select from the list of available bridge groups.

  Default:

  - none

  Special values:

  - If bridge group is set to "none", the IGMP queries will the sent via all bridge groups.

- **VLAN ID**

  Limits the querier instance to a certain VLAN.

  Possible values:

  - 0 to 4096.

  Default:

  - 0

  Special values:

  - If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

A.9.5 IGMP status

General statistics

Status messages for IGMP snooping are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge statistics ▶ IGMP snooping

- **Operating**

  Indicates whether IGMP snooping is activated or deactivated.

- **IPv4 packets**

  Shows the number of IPv4 multicast packets received at all ports, whether they were IGMP packets or not.

- **Data packets**

  Shows the number of intact IPv4 multicast packets received at all ports and which were not IGMP packets.

- **Control packets**

  Shows the number of intact IGMP packets received at all ports.

- **Bad packets**

  Shows the number of damaged data or IGMP packets received at all ports. Possible causes for damage to packets may be IP checksum errors or truncated packets.

ⓘ For performance reasons, IP checksums are evaluated for IGMP packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

- **Deleted values**

  This action deletes all statistical entries.

Port status

This table shows all port-related statistics.

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge ▶ IGMP snooping ▶ Port status

- **Router port**

  Shows whether the port is currently in use as a router port or not, irrespective of whether this status was configured statically or learned dynamically.

- **IPv4 packets**

  Shows the number of IPv4 multicast packets received at this port, whether they were IGMP packets or not.

- **Data packets**

  Shows the number of intact IPv4 multicast packets received at this port and which were not IGMP packets.

- **Control packets**

  Shows the number of intact IGMP packets received at this port.

- **Bad packets**

  Shows the number of damaged data or IGMP packets received at this port. Possible causes for damage to packets may be IP checksum errors or truncated packets.

ⓘ For performance reasons, IP checksums are evaluated for IGMP packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

Groups

This table displays all the the multicast group memberships known to the device, irrespective of whether they were configured statically or learned dynamically. If both static and dynamic memberships exist for a multicast group, these are shown in separate entries.

WEBconfig: LCOS menu tree ▶ Status ▶ LAN bridge ▶ IGMP snooping ▶ Groups

- **Address**

  Shows the group's IP multicast address.

- **VLAN ID**

  Shows the VLAN ID that this entry applies to.

- **Allow learning**

  Shows whether new memberships for this group can be learned dynamically or not.

- **Static members**

  Shows the list of statically defined members for this group.

- **Dynamic members**

  Shows the list of dynamically learned members for this group.

Simulated queriers

This table shows the status of all defined and active IGMP querier instances.

- **Name**

  Shows the name of the multicast group.
- **Bridge group**

  Shows the bridge group that this entry applies to.
- **VLAN ID**

  Shows the VLAN that this entry applies to.
- **Status**

  Shows the current status of the entry.
  - □ Initial: The querier instance has just started and is sending IGMP queries in short intervals (four-times faster than the query interval defined).
  - □ Querier: The querier instance considers itself to be the active querier and is sending IGMP queries in the defined query interval.
  - □ Non-Querier: Another querier instance with a lower IP address has been detected, and the instance listed here is not sending any IGMP queries.

A.10 TACACS+

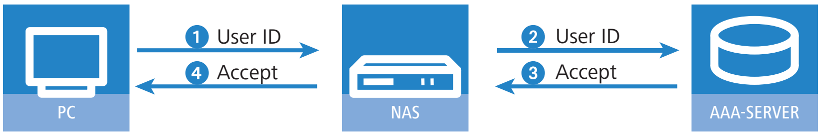
A.10.1 Introduction

Tacacs+ (Terminal Access Controller Access-Control System) is a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for certain authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

TACACS+ must be used in order to meet with PCI compliance (Payment Card Industry).

Modern networks with their numerous types of service and network components present a massive challenge in terms of controlling access rights for the user. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a Network Access Server (NAS): It does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an accept or a reject.



The advanced TACACS+ functions include, among others, the option of requesting user to change their passwords after logging in for the first time, or if the password has expired. The corresponding messages are sent from the NAS to the user.

Please note that LANconfig cannot process all of the messages in the extended login dialog. Should LANconfig reject a login attempt at a LANCOM even if the correct data is entered, please use an alternative method of configuration (such as WEBconfig or telnet).

TACACS+ is an alternative AAA server to the widespread RADIUS servers. The following table shows some of the major differences between RADIUS and TACACS+:

TACACS+	RADIUS
Connection-orientated data transfer via TCP	Connectionless data transfer via UDP
Fully encrypted data transfer	Password only encrypted, other content remains unencrypted
Complete separation of authentication, authorization and accounting possible	Authentication and authorization combined

- TCP-based communication with TACACS+ is more reliable than RADIUS. Communications between the NAS and AAA server are confirmed, so the NAS is always informed if the AAA server is unavailable.
- TACACS+ encrypts not only the password like RADIUS but the entire payload data (except for the TACACS+ header). This assures the confidentiality of information such as user names or the permitted services. TACACS+ encryption works with a one-time pad based on MD5 hashes.
- The separation of the three AAA functions enables TACACS+ to operate with multiple servers. Whereas RADIUS always combines authentication and authorization, TACACS+ allows these to be separated. In this way, for example, TACACS+ servers can be employed for authentication only, in that only the users are managed but not the permissible commands.

Please note: Even though TACACS+ is used to centrally manage user accounts on an AAA server, you should ensure that you set a secure password for root access to the LANCOM. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

A.10.2 Configuring the TACACS+ parameters

The parameters for configuring TACACS+ are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+

- **Accounting**

  Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ accounting will only activate if the defined TACACS+ server is available.

- **Authentication**

  Activates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ authentication will only activate if the defined TACACS+ server is available. Fallback to local users is only possible if a root password has been set for the LANCOM. The fallback to local users must be deactivated for devices without a root password. Otherwise a failure of the network connection (TACACS+ server unavailable) would make the LANCOM accessible without a password.

- **Authorization**

  Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

  Possible values:

  □ Activated, deactivated

  Default

  □ Deactivated

TACACS+ authorization will only activate if the defined TACACS+ server is available.
If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.

- **Fallback to local users**

  Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the LANCOM. This allows for access to the device even if the TACACS+ connection should fail, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.

  Possible values:

  □ Allowed, prohibited

  Default

  □ Allowed

  The fallback to local user accounts presents a security risk if no root password is set for the LANCOM. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

- **Shared secret**

  The password for encrypting the communications between NAS and TACACS+ servers.

  Possible values:

  □ 31 alphanumerical characters

  Default

  □ Blank

  The password must be entered identically into the LANCOM and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

- **SNMP-GET requests accounting**

  Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the LANCOM devices to display information about current connections, etc., or to execute actions such as disconnecting a connection. SNMP can be used to configure devices. For this reason TACACS+ requires authentication for SNMP access requests. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request would initiate three sessions with the TACACS+ server.

  This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

  Entering a read-only community under LCOS menu tree ▶ Setup ▶ SNMP enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

  Possible values:

  □ only_for_SETUP_tree: With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

  □ All: With this setting, accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.

  □ None: With this setting, accounting by TACACS+ server will not be carried out for SNMP accesses.

  Default:

  □ only_for_SETUP_tree

- **SNMP-GET requests authorization**

  This parameter allows the regulation of the behavior of LANCOM devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

  Possible values:

  □ only_for_SETUP_tree: With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

- □ All: With this setting, authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- □ None: With this setting, authorization by TACACS+ server will not be carried out for SNMP accesses.

Default:

- □ only_for_SETUP_tree

- ■ **Encryption**

  Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

  Possible values:

  - □ Activated, deactivated

  Default

  - □ Activated

We recommend that you do not operate TACACS+ without encryption. If encryption is activated here, the password for encryption entered here must match with the password on the TACACS+ server.

A.10.3 Configuring the TACACS+ server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

The parameters for configuring the TACACS+ server are to be found under the following paths:

WEBconfig: LCOS menu tree ▶ Setup ▶ TACACS+ ▶ Server

- ■ **Server address**

  Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

  Possible values:

  - □ Valid DNS resolvable name or valid IP address.

  Default

  - □ Blank

- ■ **Loopback address**

  Optionally you can configure a loopback address here.

  Possible values:

  - □ Name of the IP networks whose addresses are to be used
  - □ "INT" for the address of the first intranet.
  - □ "DMZ" for the address of the first DMZ.
  - □ LB0 to LBF for the 16 loopback addresses
  - □ Any valid IP address

  Default

  - □ Blank

- ■ **Compatibility mode**

  TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers.

  Possible values:

  - □ Activated, deactivated

  Default

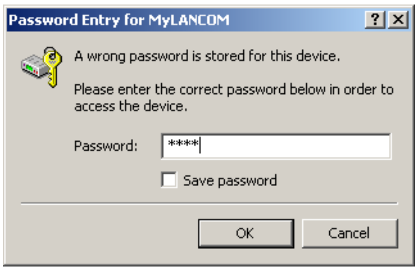
  - □ Deactivated

A.10.4 Login to the TACACS+ server

Once TACACS+ has been activated for authentication and/or authorization, all logins to the device are redirected to the TACACS+ server. The remaining login procedure differs according to the access method.

TACACS+ login via LANconfig

Using LANconfig to login to a device with activated TACACS+ authentication is only possible with the user named "root". Correspondingly, the user "root" must be configured on the TACACS+ server. To login via LANconfig, enter the password as configured for the user "root" on the TACACS+ server.



Password Entry for MyLANCOM

A wrong password is stored for this device.

Please enter the correct password below in order to access the device.

Password: ****

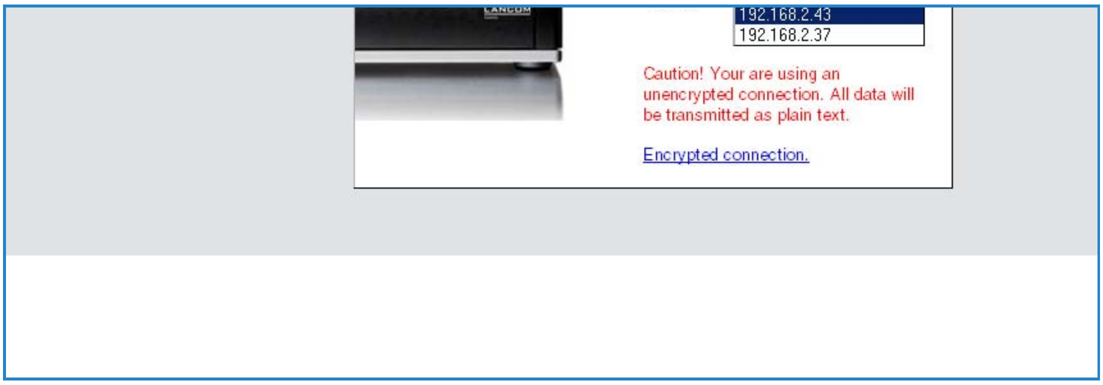
□ Save password

Once authenticated by TACACS+, "root" is the only user automatically assigned with full supervisor rights, and thus able to edit the configuration without having to change privilege level. When authorization is in use, the TACACS+ server decides whether this is allowed or not.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the commands "readconfig" and "writeconfig" for the user "root" in order for the user to read the configuration from the device and to upload any changes ('Assigning rights under TACACS+' → Page 24).

TACACS+ login via WEBconfig

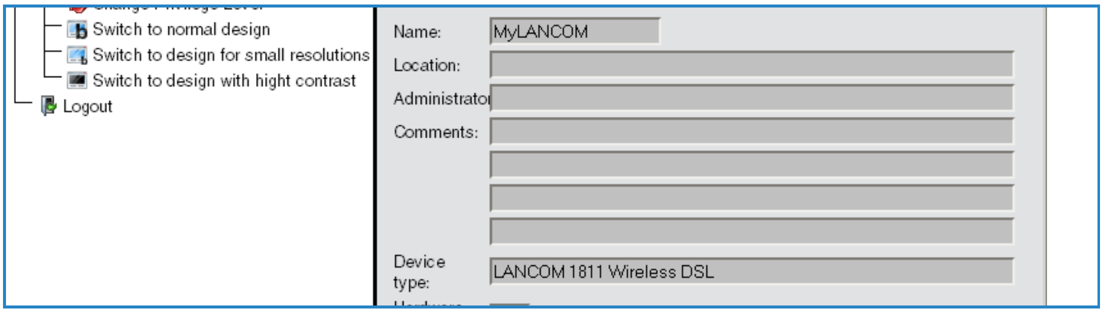
Using WEBconfig to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with WEBconfig, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication.



192.168.2.43
192.168.2.37

Caution! Your are using an unencrypted connection. All data will be transmitted as plain text.

The corresponding password is requested in the following dialog. After logging in, the user initially sees a reduced WEBconfig user interface. If authorization is not being used, all WEBconfig users (except for the user "root") initially have read rights only.



Switch to normal design
Switch to design for small resolutions
Switch to design with hight contrast
Logout

Name: MyLANCOM

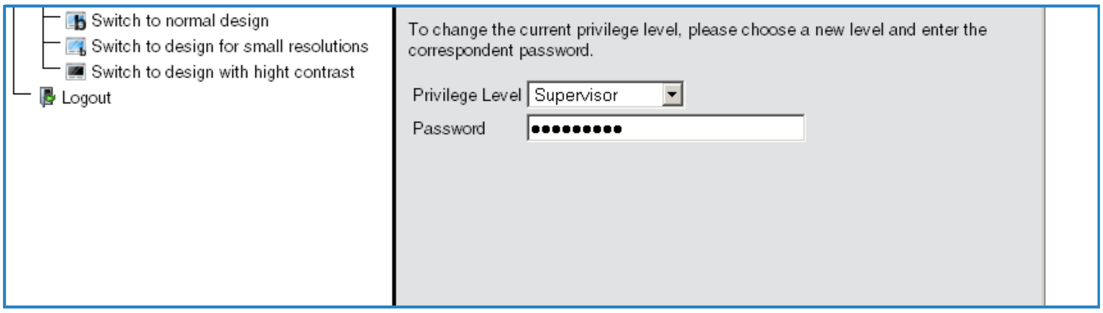
Location:

Administrator:

Comments:

Device type: LANCOM 1811 Wireless DSL

To gain further rights, click on the link **Change privilege level** on the left of the screen.



Switch to normal design
Switch to design for small resolutions
Switch to design with hight contrast
Logout

To change the current privilege level, please choose a new level and enter the correspondent password.

Privilege Level: Supervisor

Password: ●●●●●●●●●●

In this dialog you select the required user rights and enter the corresponding password.

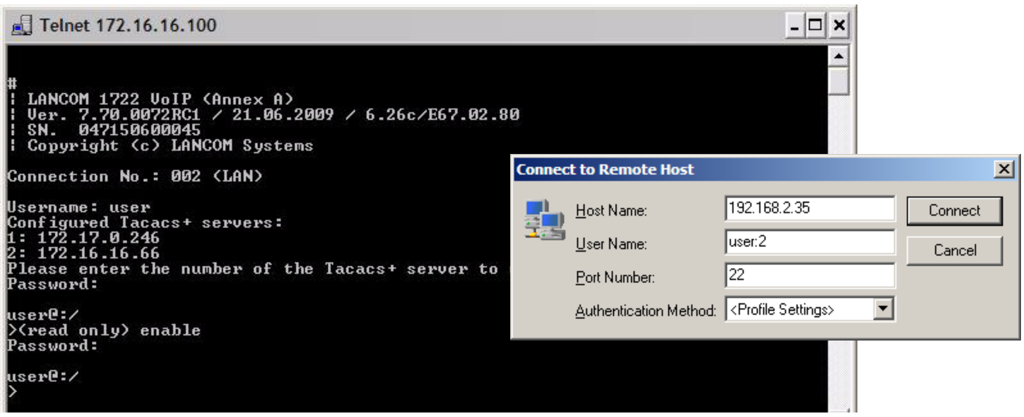
The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration ('Assigning rights under TACACS+' → Page 24).

TACACS+ login with telnet or SSH

Using tenet or SSH to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server.

When logging in with telnet, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication. When logging in with SSH, enter the user name followed by a colon and then the server name, i.e. "user:1" or "user:2".



Telnet 172.16.16.100

```
#
| LANCOM 1722 VoIP (Annex A)
| Ver. 7.70.0072RC1 / 21.06.2009 / 6.26c/E67.02.80
| SN.  047150600045
| Copyright (c) LANCOM Systems

Connection No.: 002 (LAN)

Username: user
Configured Tacacs+ servers:
1: 172.17.0.246
2: 172.16.16.66
Please enter the number of the Tacacs+ server to
Password:

user@:/
>(read only) enable
Password:

user@:/
>
```

Connect to Remote Host

Host Name: 192.168.2.35

User Name: user:2

Port Number: 22

Authentication Method: <Profile Settings>

After login, all users initially have read-rights only (except for the user "root").

To gain further rights, enter the command `enable` and enter the password. Rights will be assigned according to configuration for that password. The parameters for the enable command are the numbers 1-15. 1 is the lowest level, 15 the highest. If no parameter is entered, 15 is taken automatically.

The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration ('Assigning rights under TACACS+' → Page 24).

A.10.5 Assigning rights under TACACS+

TACACS+ uses privilege levels to separate users into different groups. For the local authorization of users via the "enable" command under telnet/SSH or via privilege levels under WEBconfig, the various administrator rights of LCOS are mapped to the TACACS+ privilege levels:

TACACS+ level	LCOS administrator rights
0	No rights
1	Read only
3	Read-write
5	Read-only limited admin

TACACS+ level	LCOS administrator rights
7	Read-write limited admin
9	Read-only admin
11	Read-write admin
15	Supervisor (root)

A.10.6 Authorizing functions

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the corresponding functions for the user. Enter the required values into the user configuration on the TACACS+ server.

LANconfig

Command	Arguments	Remark
readconfig	none	Read out the entire configuration
writeconfig	none	Write the entire configuration

WEBconfig

Command	Arguments	Remark
delRow	SNMP-ID of the table	Delete row
addRow	SNMP-ID of the table	Add row
editRow	SNMP-ID of the table	Edit row
modifyItem	SNMP-ID of the menu item	Edit a menu item
viewTable	SNMP-ID of the table	View table
viewRow	SNMP-ID of the row	View row
setValue	SNMP-ID of the menu item	Set value of a menu item
listmenu	SNMP-ID of the menu	List sub menu
action	SNMP-ID of the action	Execute an action
reboot	none	Restart device
$URL	none	Display a certain URL

When working with WEBconfig, all URLs sent to the TACACS+ server during configuration must be enabled. For example, the URL "config2" under WEBconfig provides access to the configuration branch of the LCOS menu tree. Additionally, the individual parameters which the user may edit must also be enabled. You can view the URLs sent by WEBconfig to the TACACS+ server with the trace "trace+ tacacs".

Telnet/SSH

Command	Arguments	Remark
dir	SNMP-ID of the directory	View directory content
list	SNMP-ID of the directory	View directory content
ls	SNMP-ID of the directory	View directory content
llong	SNMP-ID of the directory	View directory content
del	SNMP-ID of the table	Delete row
delete	SNMP-ID of the table	Delete row
rm	SNMP-ID of the table	Delete row
cd	SNMP-ID of the target directory	Change directory
add	SNMP-ID of the table	Add row
tab	SNMP-ID of the table	Changes the order of the columns for adding values
do	SNMP-ID of the action	Execute action
show	Parameter name	View information
trace	Parameter name	Execute trace
time	Parameter name	Time
feature	Parameter name	Add function
repeat	Parameter name	Repeat the command
readmib	none	Read-out SNMP-MIB
readconfig	none	Read out the entire configuration
readstatus	none	Read-out status menu
writefiash	none	Update firmware
activateimage	Parameter name	Activate another firmware image
ping	Parameter name	Start ping
wakeup	Parameter name	Sends wakeup packet
linktest	Parameter name	WLAN link test
writeconfig	none	Write the entire configuration
ll2mdetect	none	Start LL2M detection
ll2mexec	Parameter name	Execute LL2M command
scp	Parameter name	Secure copy
rcp	Parameter name	Secure copy
readscript	Parameter name	Read-out script
beginscript	none	Start script
endscript	none	Stop script
flash	Parameter name	Activate/deactivate flash mode

For telnet access, all of the parameters that the user may edit must be enabled. You can view the values sent by telnet to the TACACS+ server with the trace "trace+ tacacs".

SNMP

Command	Arguments	Remark
get	SNMP-ID of the menu item	Read-out value
set	SNMP-ID of the menu item	Set value

A.11 Sending attachments with the mailto command

E-mails with information on device status can be sent automatically if certain events occur. To do this, just include the mailto command into entries in the action table or cron table.

Attachments can be sent with the e-mails. This allows the results of console commands executed on the device before sending the mail to be sent as an attachment. In this way, the content of tables or menus (e.g. detailed status messages) can be sent by e-mail.

- **Action (action table) or command (cron table) (max. 250 characters)**

  Here you describe the action that is be executed at a certain time or when a change in the status of the WAN connection occurs. Only one action can be triggered per entry.

  Possible values for the actions (max. 250 characters):

  - mailto: – This prefix causes an e-mail to be sent.

  Optional variables for the actions:

  - attach=`console command`

  Any console command can be entered which outputs useful information. The console command is enclosed in "backquotes" also known as backticks. This character is produced with the aid of the "accent grave" key.

  The output of the console command is written to a text file for attachment to the mail. This text file is headed by the command and a time/date stamp, followed by the output.

  Default:

  - Blank

  Examples:

  The following action enables you to sent the ADSL status by e-mail:
  mailto:admin@mycompany.com?subject=ADSL_status?attach=`dir /status/adsl`.

  An action can be used to send mutliple console commands:
  mailto:admin@mycompany.com?subject=Status_reports?attach=`dir /status/adsl`?attach=`dir /status/config`
  The attached files are named 'cmd1.txt', 'cmd2.txt', etc.

A.12 Firmware upload for the UMTS module in the LANCOM 1751 UMTS

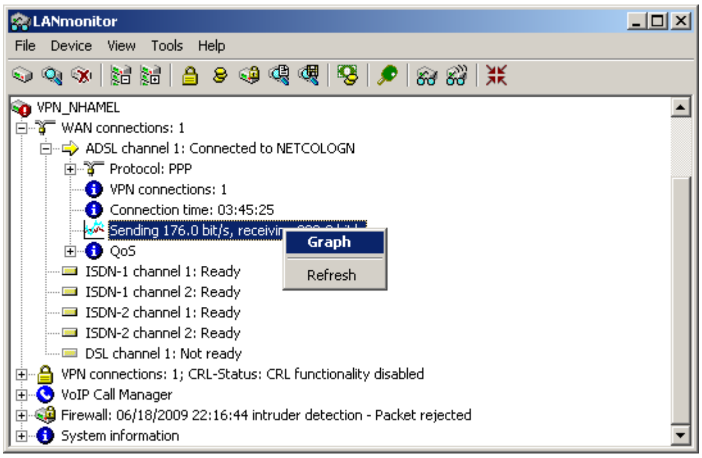
The firmware of the UMTS module in the LANCOM 1751 UMTS can be updated easily as of LCOS version 7.70. Firmware for the UMTS module is available in UPX format and can be uploaded to the LANCOM 1751 UMTS in the same manner as the LANCOM firmware.

A.13 Performance monitoring with LANmonitor

LANmonitor logs various parameters in the devices and displays these graphically:

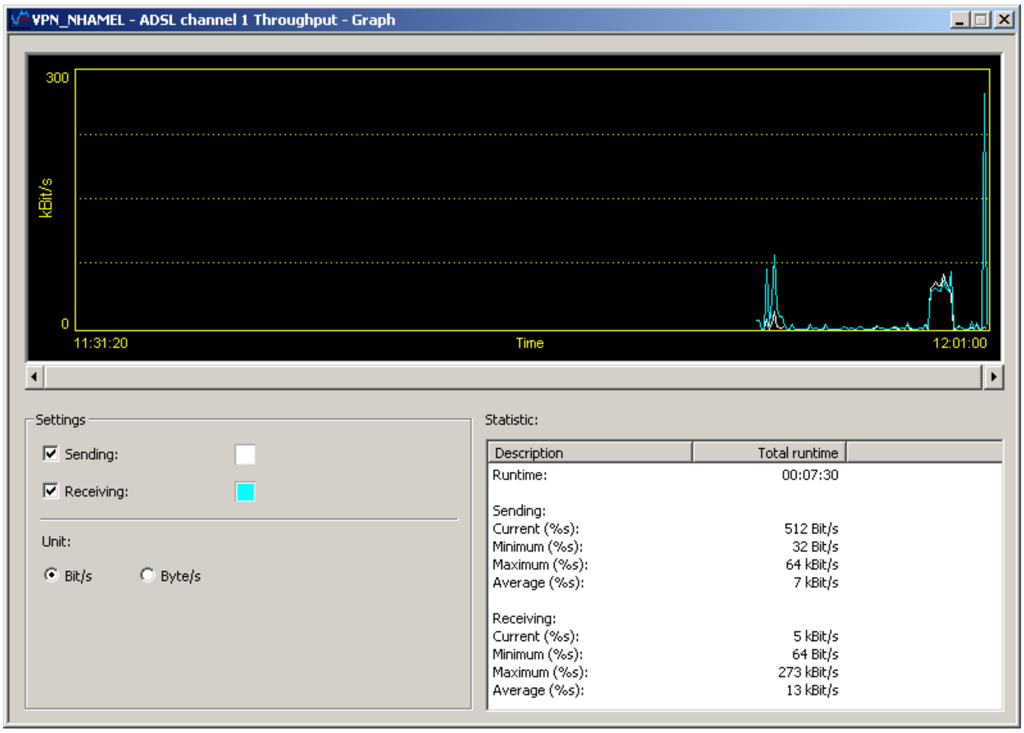
- Transmit and receive rates for WAN connections
- Transmit and receive rates for point-to-point connections
- Signal reception strength for point-to-point connections
- Link signal strength for point-to-point connections
- Throughput for point-to-point connections
- CPU load
- Free memory
- Temperature (not available on all models)

LANmonitor displays the current values directly in the corresponding groups.



```
VPN_NHAMEL
  WAN connections: 1
    ADSL channel 1: Connected to NETCOLOGN
      Protocol: PPP
      VPN connections: 1
      Connection time: 03:45:25
      Sending 176.0 bit/s, receivi
      QoS
    ISDN-1 channel 1: Ready
    ISDN-1 channel 2: Ready
    ISDN-2 channel 1: Ready
    ISDN-2 channel 2: Ready
    DSL channel 1: Not ready
  VPN connections: 1; CRL-Status: CRL functionality disabled
  VoIP Call Manager
  Firewall: 06/18/2009 22:16:44 intruder detection - Packet rejected
  System information
```

A click on the **Graph** item in the context menu opens a new window which displays these parameters over time.



Settings

☑ Sending:

☑ Receiving:

Unit:

● Bit/s ○ Byte/s

Statistic:

Description	Total runtime
Runtime:	00:07:30
Sending:	
Current (%s):	512 Bit/s
Minimum (%s):	32 Bit/s
Maximum (%s):	64 kBit/s
Average (%s):	7 kBit/s
Receiving:	
Current (%s):	5 kBit/s
Minimum (%s):	64 Bit/s
Maximum (%s):	273 kBit/s
Average (%s):	13 kBit/s

You can use the left-hand mouse key to mark any period in the graph, and these statistical values will be displayed separately.

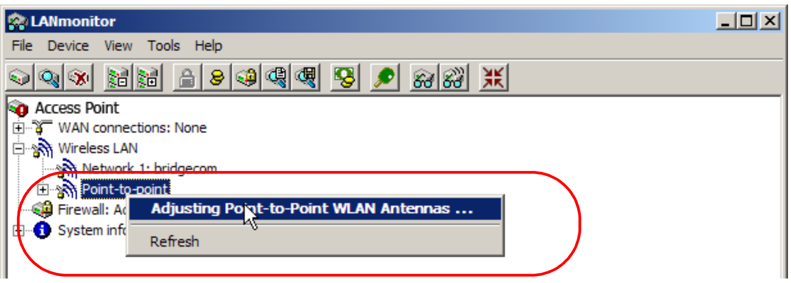
This dialog displays the values collected over the last 24 hours.

Please note that the values on display are deleted when the dialog is closed. For monitoring over a longer period, leave the window open.

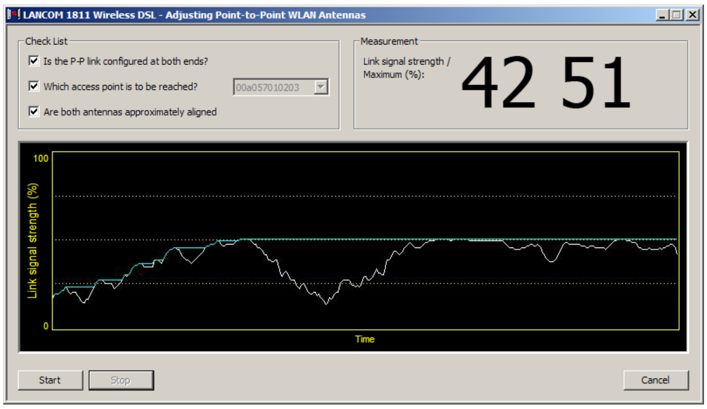
A.14 Setting up point-to-point connections with LANmonitor

To find the best possible alignment for point-to-point connection antennas, the current signal quality over a P2P connection can be displayed on the device's LEDs or in LANmonitor. LANmonitor provides not only an optical display of link strength, but an acoustic signal as well.

In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...'



Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram, too.



LANCOM 1811 Wireless DSL - Adjusting Point-to-Point WLAN Antennas

Check List

☑ Is the P-P link configured at both ends?

☑ Which access point is to be reached? 00a057010203

☑ Are both antennas approximately aligned

Measurement

Link signal strength / Maximum (%): 42 51

Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

An acoustic signal can be activated to help align the antennas precisely. With this option, the PC can emit a tone which varies according to signal strength. Maximum signal strength over the link is signaled by a constant tone. If the signal strength drops below the maximum, tones are emitted at intervals indicating the difference from the former maximum. The shorter the interval, the closer the current link signal strength is to the maximum.