

## A Addendum to LCOS Version 7.8

### A.1 Overview

- 'DHCP cluster' → Page 1
- 'Deactivating Ethernet interfaces' → Page 2
- 'ARF network for IAPP' → Page 2
- 'Routing of local services/ARP handling switchable' → Page 3
- 'XAUTH with external RADIUS servers' → Page 3
- 'Enhanced certificate support' → Page 4
- 'Wildcard matching of certificates' → Page 5
- 'Multiple WLAN profiles in client mode' → Page 5
- 'Averaging of CPU-load display' → Page 6
- 'Bypassing TACACS+' → Page 7
- 'Serial COM-port enhancements' → Page 7
- '32 additional gateways for PPTP connections' → Page 9
- 'Additional commentary fields for describing the devices' → Page 10
- 'DHCP options with LANconfig' → Page 11
- 'Setting the routing tag for local routes' → Page 12
- 'Global settings, DiffServ for SIP & RTP' → Page 12
- 'Increased DoS threshold value for central devices' → Page 13

### A.2 DHCP cluster

#### A.2.1 Introduction

If multiple DHCP servers are active in a network, the stations "divide" themselves equally between them. However, the DNS server in LANCOM devices can only properly resolve the name of the station which was assigned the address information by the DHCP server. In order for the DNS server to be able to resolve the names of other DHCP servers, these can be operated in a cluster. In this operating mode, the DHCP server monitors all DHCP negotiations in the network. It additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster.

#### A.2.2 Configuration

A DHCP server's operation in the cluster can be activated or deactivated for each individual ARF network with the associated DHCP settings.

WEBconfig: LCOS menu tree ► Setup ► DHCP ► Network list

##### ■ Cluster

This setting defines whether the DHCP server for this ARF network is to be operated separately or in the cluster.

Possible values:

- Yes: With cluster mode activated, the DHCP server monitors all of the ongoing DHCP negotiations in the network, and it additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster. These stations are flagged as "cache" in the DHCP table.
- No: The DHCP server manages information only for the stations connected to it.

Default:

- No



If the lease time for the information supplied by DHCP expires, the station requests a renewal from the DHCP server which supplied the original information.

If the original DHCP server does not respond, the station then emits its rebinding request as a broadcast to all available DHCP servers.

DHCP servers in a cluster ignore renew requests, which forces a rebinding. The resulting broadcast is used by all of the DHCP servers to update their entries for the station.

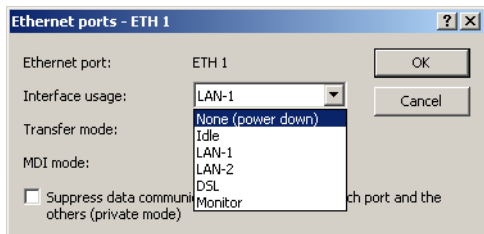
The only DHCP server to answer the rebind request is the one with which the station was originally registered. If a station repeats its rebind request, the all DHCP servers in the cluster assume that the original DHCP server is no longer active in the cluster, and they respond to the request. The responses received by

□ Deactivating Ethernet interfaces

the station will have the same IP address, but the gateway and DNS server addresses may differ. From these responses, the station selects a new DHCP server to connect with, and it updates its gateway and DNS server (and other relevant parameters) accordingly.

### A.3 Deactivating Ethernet interfaces

The Ethernet interfaces on any publicly accessible LANCOM device can potentially be used by unauthorized persons to gain physical access to a network. The Ethernet interfaces on the device can be disabled to prevent this.



LANconfig: Interfaces ► LAN ► Interface settings

WEBconfig: LCOS menu tree ► Setup ► Interfaces

#### ■ Interface usage

Here you select how this interface is to be used.

Possible values:

- None (power down): The interface is deactivated.
- Idle: The interface is not allocated to any particular task, but it remains physically active.
- LAN-1 to LAN-n: The interface is allocated to a logical LAN.
- DSL-1 to DSL-n: The interface is allocated to a DSL interface.
- Monitor: The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Wireshark / Ethereal can be connected to this port, for example.

Default:

- Depends on the particular interface or the hardware model.

### A.4 ARF network for IAPP

Access points use the IAPP protocol to communicate and pass information about the handovers of associated WLAN clients which are roaming. Access points regularly send out multicast announcements to inform the devices about the BSSIDs and IP addresses of the other access points. A roaming WLAN client initiates a handover by informing a new access point about its former AP. The access point uses the information supplied by the IAPP protocol to inform the former access point to remove the WLAN client from its list of associated clients.

Where an access point supports multiple ARF networks, the IAPP announcements are transmitted on all ARF networks. To limit these multicasts to one particular ARF network, it is possible to define an IAPP IP network.

WEBconfig: LCOS menu tree ► Setup ► WLAN

#### ■ IAPP-IP network

Here you select the ARF network which is to be used as the IAPP-IP network.

Possible values:

- Selection from the list of ARF networks defined in the device; max. 16 alphanumerical characters

Default:

- Blank

Special values:

- Blank: If no IAPP-IP network is defined, IAPP announcements are transmitted on all of the defined ARF networks.

## A.5 Routing of local services/ARP handling switchable

### A.5.1 Introduction

Response packets for internal services (such as telnet, http/https, tftp, etc.) from the LANCOM to recipients in the Ethernet (LAN or WAN) were, prior to LCOS version 7.80, always sent directly to the corresponding requester. This meant, among other things, that devices could be detected from within any LAN.

As of LCOS version 7.80, a switch provides the option to initiate an ARP request to determine a specific route, instead of using the direct address.

If, for example, a LANCOM router should be detected by LANconfig without any knowledge of the LAN topology, then the older method would be preferable. In this case, the sender of the TFTP broadcast (in this case LANconfig/device search) receives a direct unicast response from the router.

In scenarios where LANs use changing virtual MAC and IP addresses (e.g. when VRRP components are used in the LAN), direct addressing may lead to errors if the redundancy protocol has adjusted the MAC/IP assignments. In such cases it is preferable to activate the "route internal services" option.

### A.5.2 Configuration

The appropriate settings for IP routing can be used to route the LANCOM's internal services via the router.

WEBconfig: LCOS menu tree ► Setup ► IP router ► Routing method

#### ■ Route internal services

This is where you select whether the internal services are to be directed via the router.

Possible values:

- Yes: Packets for internal services are directed via the router.
- No: Packets are returned straight to the sender.

Default:

- No

## A.6 XAUTH with external RADIUS servers

As of LCOS version 7.60, LANCOM devices can identify and authenticate remote stations with the Extended Authentication Protocol (XAUTH). Authentication referred to the user data in the PPP list.

As of LCOS version 7.80, XAUTH authentication can also be handled by an (external) RADIUS server. For example, this allows reference to existing RAS user data on the RADIUS server, assuming that RADIUS-authenticated dial-in via PPP has been set up for VPN with XAUTH.

To supplement VPN dial-in with XAUTH for authentication, please proceed as follows:

- ① Set up a VPN dial-in account, for example with the LANconfig Setup Wizard.
- ② Activate XAUTH in the VPN client at the station which is to dial in. The user name and password are the same as those stored on the RADIUS server.

**Assistant for New Profile**

**VPN Gateway Parameters**  
To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnsrvr.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.  
Using Extended Authentication (XAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint):  
vpnsrvr.company.com

Extended Authentication (XAUTH)

User ID:  
user

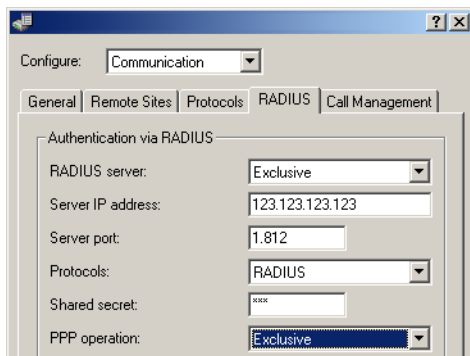
Password: max Password (confirm): max

< Back Next > Cancel

- ③ Activate the authentication of dial-in remote stations via the XAUTH protocol on an external RADIUS server. In LANconfig, access the configuration area **Communication** and the **RADIUS** tab to activate the "Exclusive"

□ Enhanced certificate support

operating mode for the RADIUS server. With this setting, all incoming XAUTH requests are authenticated by the RADIUS server.



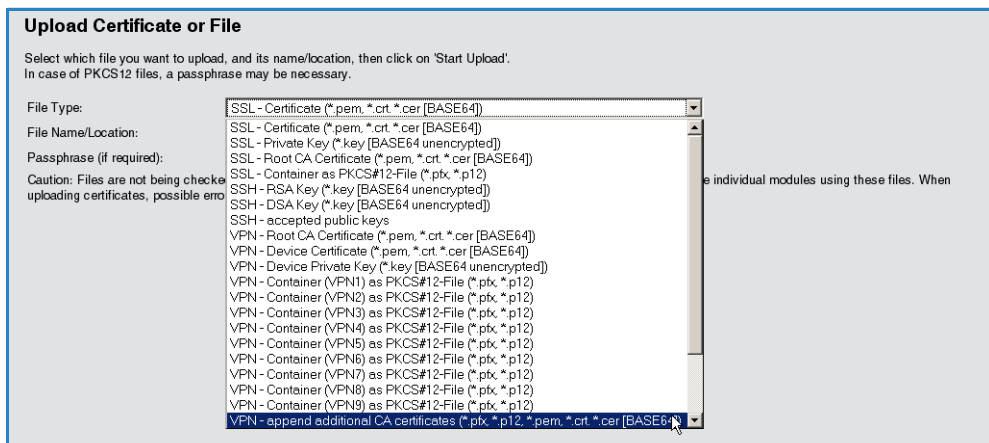
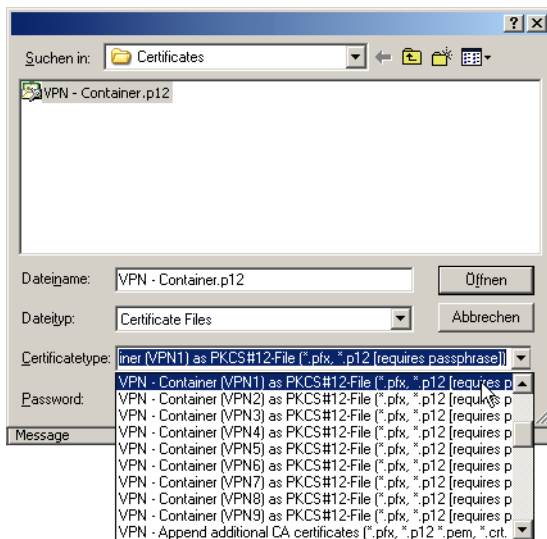
- ④ You should also specify the IP address, the port, and the key for the external RADIUS server.
- ⑤ Also set PPP operation to "Exclusive" so that incoming XAUTH requests are authenticated by the RADIUS server only.

### A.7 Enhanced certificate support

In order to support multiple certificate heirarchies, LCOS as of version 7.80 allows up to nine PKCS#12 files to be uploaded to the device. Also, further files with individual additional CA certificates can be uploaded, which enclose the certificates either individually or as PKCS#12 containers. All certificate hierarchies can be managed manually or with SCEP, and they can use CRLs.

LANconfig: Device ► Configuration management ► Upload certificate from file

WEBconfig: File management ► Upload certificate or file



The certificates in the device can be viewed in the status area:

WEBconfig: Status ► Status ► Certificates ► Device certificates

The internal file system for the device classifies the device certificates as applications "VPN1" to "VPN9".

To use the certificate, either the certificate subject or this abbreviation can be used as "local identity" in the IKE keys of type ASN.1-Distinguished Name.



Using this abbreviation to reference the certificates allows subjects containing special characters to be used, such as German umlauts. This is not usually possible when working with the command-line interface configuration.

The abbreviation is entered as "Application" when configuring the certificates for the SCEP client.

## A.8 Wildcard matching of certificates

### A.8.1 Introduction

Generally speaking, the local identity and remote identity for certificate-based VPN connections are the certificate subjects. In the VPN configuration, these are stored in the form of (often complex) ASN.1 Distinguished Names (DN). During VPN negotiation, the local identity is used to select the certificate which is to be transmitted to the remote station, whereas the local value for the remote identity is compared with the received identity of the remote station and the subject of the received certificate.

Until now, the local and the remote identities had to be entered in full into the VPN configuration. Not only is this prone to error, it is sometimes desirable to specify only a part of the certificate subject. This is practical where different certificates with similar subjects are to be accepted automatically, for example where certificates can change, or where multiple parallel certificate hierarchies operate simultaneously.

This is facilitated by flexible identity comparison. The certificate subjects have to contain the components of an ASN.1 Distinguished Name (DN) (Relative Distinguished Names – RDNs) as included in the configured identities. The RDNs can be in any order. Also, the RDN values can include the wildcards '?' and '\*'. If the RDNs are to include wildcards, these must be entered in the form '\?' or '\\*'. Examples:

- Subject = '/CN=John Doe/O=\*ACME\*', DN = '/CN=John?Doe\*'
- Subject = '/CN=John Doe/O=\*ACME\*', DN = '/O=\\*ACME\\*'

### A.8.2 Configuration

This flexible method of identification comparison is activated or deactivated in the VPN configuration.

WEBconfig: LCOS menu tree ► Setup ► VPN

#### ■ Flexible ID comparison

Possible values:

- Yes, No

Default:

- No

Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

## A.9 Multiple WLAN profiles in client mode

### A.9.1 Introduction

If a device equipped with an Ethernet interface is to be connected to a wireless LAN, a LANCOM access point can be switched into client mode, causing it to act as conventional wireless LAN client and not as an access point.

WLAN clients such as notebooks are generally able to save and manage various profiles which allow different access points to be selected depending on the environment (e.g. for a company WLAN or for another WLAN at home). These profiles store various information such as the WLAN SSID and the associated key. The WLAN client automatically selects the profile fitting to the strongest available or preferred WLAN.

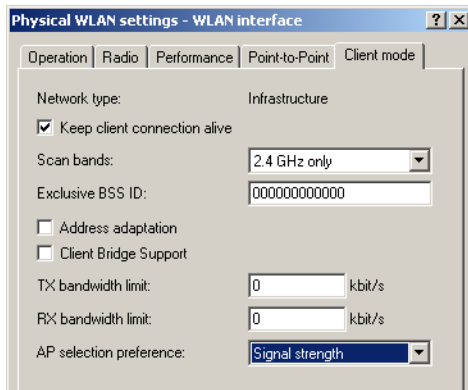
LANCOM access points can store up to eight different WLAN profiles for use in client mode. The profile in client mode activates the networking and transmission parameters, and also the encryption settings for the logical WLAN.



Please observe that a WLAN module in client mode only connects to one access point at a time, even if multiple WLAN profiles have been defined.

## A.9.2 Configuration

Not only can networking, transmission and encryption parameters be defined separately for each WLAN module, but also which criteria are to be used to select the client profile.



LANconfig: Wireless LAN ► General ► Physical WLAN settings ► Client mode

WEBconfig: LCOS menu tree ► Setup ► Interfaces ► WLAN ► Client modes ► WLAN-1

### ■ AP selection preference

Here you select how this interface is to be used.

Possible values:

- Signal strength: Selects the profile for the WLAN offering the strongest signal. This setting causes the WLAN module in client mode to automatically switch to a different WLAN as soon as it offers a stronger signal.
- Profile: Selects the profile for available WLANs in the order that they have been defined (WLAN index, e.g. WLAN-1, WLAN-2, etc.), even if another WLAN offers a stronger signal. In this setting, the WLAN module in client mode automatically switches to a different WLAN as soon as a WLAN with a lower WLAN index is detected (irrespective of signal strengths).

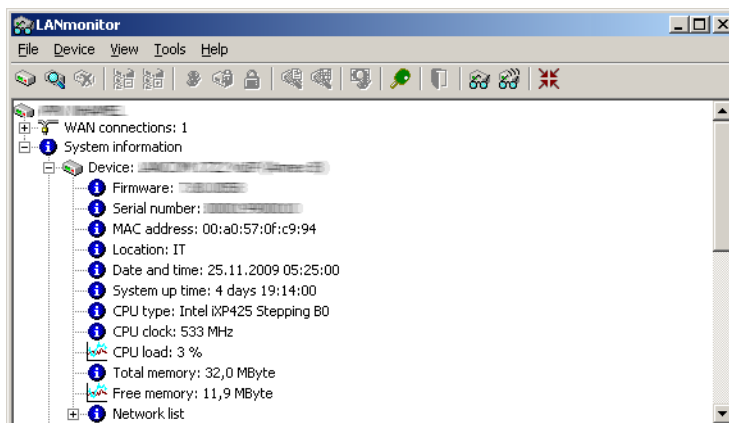
Default:

- Signal strength.

## A.10 Averaging of CPU-load display

### A.10.1 Introduction

The current CPU load for the device can be output in various ways (LANmonitor, WEBconfig, or CLI in the status area; some models have an integrated display).



### A.10.2 Configuration

You can set the time interval for averaging the value for the displayed CPU load.

WEBconfig: LCOS menu tree ► Setup ► Config

#### ■ CPU-load interval

You can select the time interval for averaging the CPU load. The CPU load displayed in LANmonitor, in the status area, in the display (if fitted), or by SNMP tools is a value which is averaged over the time interval set here. The

status area under WEBconfig or CLI additionally display the CPU load values for all four of the optional averaging periods.

Possible values:

- 1, 5, 60 or 300 seconds.

Default:

- 60 seconds.



The default period of 60 seconds is specified by the HOST-RESOURCES-MIB, which is used by many SNMP tools to display CPU load in a tacho display. Please consider this specification when altering the CPU-load interval.

Hardware-Info	
Board-Revision	A
CPU-Clock-MHz	533
CPU-Load-1s-Percent	3
CPU-Load-300s-Percent	3
CPU-Load-5s-Percent	7
CPU-Load-60s-Percent	3
CPU-Load-Percent	3
CPU-Type	Intel iXP425 Stepping B0

## A.11 Bypassing TACACS+

### A.11.1 Introduction

TACACS+ enables every change to a network-device configuration to be subject to special authorization. TACACS+ accounting enables each of these steps to be logged. TACACS+ is a requirement for systems used in electronic payment (PCI compliance).

Strict monitoring of this type leads to an increase in traffic to and from the TACACS+ server(s). In large-scale scenarios, the TACACS+ communications caused when using scripts for centralized configuration changes or if CRON commands are run regularly could lead to an overload of the TACACS+ server.

### A.11.2 Configuration

To avoid overloading the TACACS+ server when carrying out automatic configuration changes, it is possible to exclude CRON, action tables and scripts from the authorization and accounting by TACACS+.

WEBconfig: LCOS menu tree ► Setup ► TACACS+

#### ■ Bypass-Tacacs-for-CRON/scripts/action-table

You can activate or deactivate the bypassing of TACACS+ authorization and TACACS+ accounting for various actions.

Possible values:

- Activated, deactivated.

Default:

- Disabled.



Please observe that this option influences the TACACS+ function for the entire system. Be sure that you restrict the use of CRON, the action tables, and scripts only to an absolutely trustworthy circle of administrators!

## A.12 Serial COM-port enhancements

### A.12.1 Introduction

The COM-port configuration has been enhanced with a number of parameters.

### A.12.2 Configuration

The additional parameters are located in the network settings for the COM port.

WEBconfig: LCOS menu tree ► Setup ► COM ports ► COM-port server ► Network settings

■ **Assume binary mode**

Some network devices connected to a serial COM port transmit data structures which may be interpreted as control characters (CR/LF – carriage return / line feed). In the default setting, the COM-ports in LANCOM devices process this information to control the data flow. "Binary mode" instructs a COM port to forward the data in binary format and ignore any control characters.

Possible values:

- Yes, No.

Default:

- No.

■ **Newline conversion**

Here you select the character to be output by the serial port when binary mode is activated.

This setting is independent of the application communicating via the serial port. If the port is connected to another LANCOM device, you can either enter CRLF here or just CR. This is because the outband interface of these devices expects a "carriage return" for the automatic determination of data-transfer speed. However, some Unix applications interpret CRLF as a prohibited double line feed character. In these cases enter either CR or LF.

Possible values:

- CRLF, CR, LF

Default:

- CRLF



This setting is only relevant if binary mode is **deactivated** for this port.

■ **TCP keepalive**

The RFC 1122 sets down a method of checking the availability of TCP connections, called TCP keepalive. An inactive transmitter queries the receive status from the remote station. If the TCP session to the remote site is available, then the remote responds with its receive status. If the TCP session to the remote site is not available, then the query is repeated for as long as it takes for the remote to respond with its receive status (after which a longer interval comes into play). As long as the basic connection functions, but the TCP session to the remote station is not available, then the remote station sends an RST packet which triggers the establishment of the TCP session by the requesting application.

Possible values:

- Inactive: TCP keepalive is not used.
- Active: TCP keepalive is active; only RST packets cause the disconnection of TCP sessions.
- Proactive: TCP keepalive is active, but the request for the receive status from the remote site is only repeated for the number of times defined under "TCP retry count". If this number of requests expires without a response with the receive status, then the TCP sessions is classified as "not available" and the application is informed. If an RST packet is received during the wait time, the TCP session will be disconnected prematurely.

Default:

- Inactive



The setting "active" is recommended for server applications.

■ **TCP keepalive interval**

This value defines the interval between sending requests for receive status if the first request is not affirmed. The associated timeout is defined as being interval/3 (max. 75 sec.).

Possible values:

- Maximum 10 characters

Default:

- 0

Special values:

- 0 activates the RFC 1122 default values (interval 7200 seconds, timeout 75 seconds).



■ **TCP retransmit timeout**

Maximum time for the retransmission timeout. This timeout defines the the interval between checking TCP-connection status and reporting the result to the application using the TCP connection.

Possible values:

- 0 to 99 seconds.

Special values:

- 0 activates the RFC 1122 default value (60 seconds).

Default:

- 0



The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

■ **TCP retry count**

The maximum number of attempts for checking TCP-connection status and reporting the result to the application using the TCP connection.

Possible values:

- 0 to 9

Special values:

- 0 activates the RFC 1122 default value (5 attempts).

Default:

- 0



The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

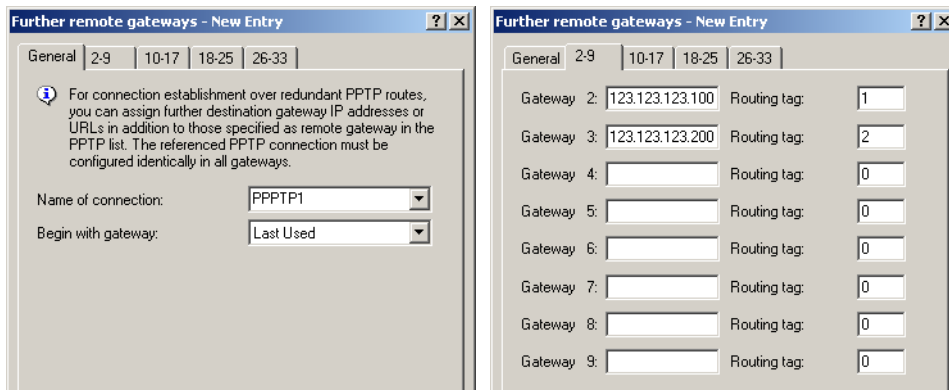
## A.13 32 additional gateways for PPTP connections

### A.13.1 Introduction

Up to 32 additional gateways can be configured to assure the availability of any PPTP remote station. Consequently, each PPTP remote station can use a total of up to 33 gateways.

### A.13.2 Configuration

The additional PPTP gateways are defined in a separate list.



LANconfig: Communication ► Protocols ► Further remote gateways

WEBconfig: LCOS menu tree ► Setup ► DHCP ► Additional PPTP gateways

■ **Name of connection**

Here you select the PPTP remote site that this entry applies to.

□ Additional commentary fields for describing the devices

Possible values:

- Select from the list of defined PPTP remote stations.

Default:

- Empty.

■ **Begin with**

Here you select the order in which the entries are to be tried.

Possible values:

- Last used: Selects the entry for the connection which was successfully used most recently.
- First: Selects the first of the configured remote sites.
- Random: Selects one of the configured remote sites at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

Default:

- Last used

■ **Gateway 2 to 33**

Enter the IP addresses of the additional gateways to be used for this PPTP remote station.

Possible values:

- IP address or 63 alphanumerical characters.

Default:

- Empty.

■ **Routing tag**


Enter the routing tag for setting the route to the relevant remote gateway.

Possible values:

- Maximum 5 characters.

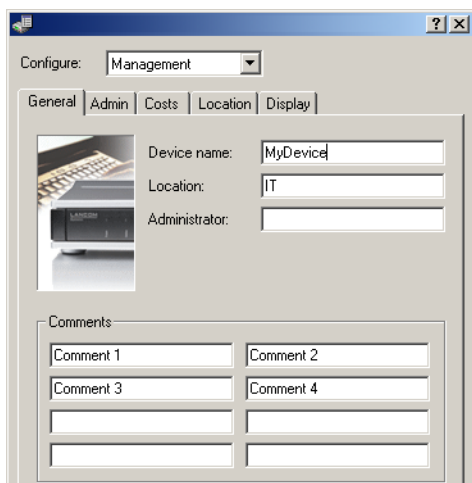
Default:

- 0.

 If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the PPTP connection list will be taken for the associated gateway.

## A.14 Additional commentary fields for describing the devices

Up to eight comments can be entered to describe the LANCOM devices.



LANconfig: Management ► General

WEBconfig: LCOS menu tree ► Setup ► SNMP

■ **Comment 1 to 8**

Enter a comment here.

Possible values:

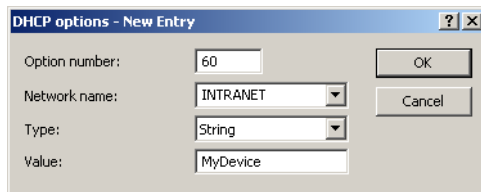
- Maximum 255 alphanumerical characters.

Default:

- Blank

## A.15 DHCP options with LANconfig

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows e. g. the type of device. This table allows additional options for DHCP operations to be defined.



LANconfig: Management ► General

WEBconfig: LCOS menu tree ► Setup ► DHCP ► Additional options

### ■ Option number


Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP.

Possible values:

- Maximum 3 characters.

Default:

- Blank

 You can find a list of all DHCP options in RFC 2132 – "DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

### ■ Network name

Name of the IP network where this DHCP option is to be used.

Possible values:

- Selection from the list of IP networks defined in the device; max. 16 characters

Default:

- Blank

### ■ Type

Entry type. This value depends on the respective option. For option "35" according to RFC 1232, e.g. the ARP cache time is defined as follows:

ARP cache timeout option

This option specifies the timeout in seconds for ARP cache entries.

The time is specified as a 32-bit unsigned integer.

The code for this option is 35, and its length is 4.

Code	Len	Time			
35	4	t1	t2	t3	t4


This description tells you that this the type "32-bit integer" is used for this option.

Possible values:

- String, Integer8, Integer16, Integer32, IP address

Default:

- String

 You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

■ **Value**

This field defines the contents of the DHCP option.

IP addresses are specified with the usual notation for IPv4 addresses, e.g. as "123.123.123.100", integer types are entered as normal decimal numbers, and strings as simple text.


Multiple values in a single field are separated with commas, e.g. "123.123.123.100, 123.123.123.200".

Possible values:

- Maximum 128 characters.

Default:

- Blank

 You can find out the possible length of the option value either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

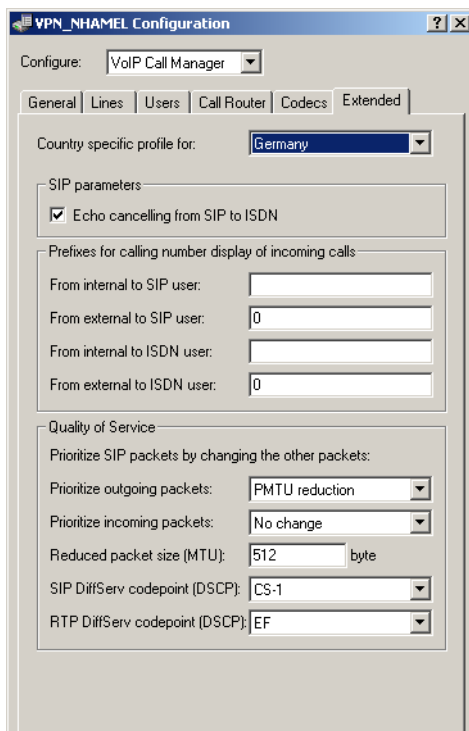
## A.16 Setting the routing tag for local routes

The definition of interface tags in Advanced Routing and Forwarding (ARF) facilitates the use of virtual routers, which only use a part of the overall routing table. The interface tag for a packet received from another local router is set according to the following procedure:

- ① If the a packet's sender address is recognized as coming from an IP network which is defined in the device, then the interface tag for that IP address is used.
- ② If the interface receiving the packet is connected to just one IP network, then the interface tag for that IP network is used.
- ③ If there is no unique result from steps ① and ②, the device attempts to use the MAC address to determine the IP address of the next hop (reverse ARP lookup). The devices uses this IP address in an attempt to identify the relevant IP network, and thus the corresponding interface tag.
- ④ If there is no unique result from options ① to ③, then the device attempts to identify the relevant IP network (and interface tag) from the routing table.

## A.17 Global settings, DiffServ for SIP & RTP

The Voice Call Manager marks SIP and RTP packets with DiffServ CodePoints (DSCP), which enables other hardware to recognize and prioritize these packets.



LANconfig: Voice Call Manager ► Advanced

WEBconfig: LCOS menu tree ▶ Setup ▶ Voice Call Manager ▶ General

■ **SIP DiffServ CodePoint (DSCP)**


This defines which DiffServ CodePoints (DSCP) the SIP packets (for call signaling) are to be marked with.

Possible values:

- BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

Default:

- CS-1

 The option CS-1 is actually outdated now, but it is set as the default value to ensure backwards compatibility. Common values for modern VoIP installations are CS-3, AF-31 or AF-41. We recommend using CS-3, one of the most widespread settings on the market.

■ **RTP DiffServ CodePoint (DSCP)**


This defines which DiffServ CodePoints (DSCP) the RTP packets (voice data stream) are to be marked with.

Possible values:

- BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

Default:

- EF


 With DSCP set to BE or CS-0 the packets are sent unmarked. Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

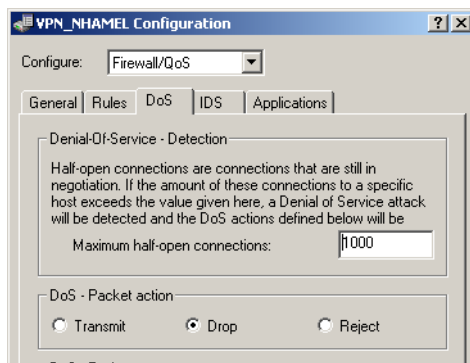
## A.18 Increased DoS threshold value for central devices

Denial-of-Service attacks take advantage of inherent weaknesses in the TCP/IP protocol in combination with poor implementations.

- Attacks which target these inherent weaknesses include SYN Flood and Smurf.
- Attacks which target erroneous implementations include those operating with erroneously fragmented packets (e.g. Teardrop) or with fake sender addresses (e.g. Land).

Your device detects most of these attacks and reacts with appropriate countermeasures. Detecting these attacks relies on counting the number of connections which are concurrently under negotiation (half-open connections). If the number of half-open connections exceeds a certain threshold value, then the device assumes that a DoS attack is underway. The actions and measures which are taken in this case can be defined, similar to firewall rules.

 Central devices are connected to a large number of users, so it is possible for a large number of half-open connections to exist without being caused by a DoS attack. For this reason, a higher default threshold value is required for the accurate detection of DoS attacks.



LANconfig: Firewall/QoS ▶ DoS

WEBconfig: LCOS menu tree ▶ Setup ▶ IP router ▶ Firewall

■ **Maximum half-open connections**

Specifies the number of half-open connections which triggers DoS-attack countermeasures.

Possible values:

□ *Increased DoS threshold value for central devices*

- 0 to 9999

Default:

- 100
- 1000 for central-site devices such as the 7100, 7111, 8011, 9100, 4025(+), 4100.