

A Addendum zur LCOS-Version 7.8

A.1 Übersicht

- 'DHCP-Cluster' →Seite 1
- 'Abschalten von Ethernet-Schnittstellen' →Seite 2
- 'ARF-Netzwerk für IAPP' →Seite 2
- 'Routen von lokalen Diensten/ARP-Handling schaltbar' →Seite 3
- 'XAUTH mit externem RADIUS-Server' →Seite 3
- 'Erweiterte Zertifikats-Unterstützung' →Seite 4
- 'Wildcard Matching von Zertifikaten' →Seite 5
- 'Mehrere WLAN-Profil im Client-Modus' →Seite 6
- 'Mittelwert der CPU-Lastanzeige' →Seite 7
- 'TACACS+-Umgehung' →Seite 8
- 'Erweiterungen für die seriellen COM-Ports' →Seite 8
- '32 zusätzliche Gateways für PPTP-Verbindungen' →Seite 10
- 'Zusätzliche Kommentarfelder zur Beschreibung der Geräte' →Seite 11
- 'DHCP-Optionen mit LANconfig' →Seite 12
- 'Ermittlung des Routing-Tags für lokale Routen' →Seite 13
- 'Globale Einstellung von DiffServ für SIP & RTP' →Seite 13
- 'Erhöhter DoS-Schwellwert für Zentralgeräte' →Seite 14

A.2 DHCP-Cluster

A.2.1 Einleitung

Wenn mehrere DHCP-Server in einem Netz aktiv sind, dann "verteilen" sich die Stationen im Netz gleichmäßig auf diese Server. Der DNS-Server der LANCOM-Geräte löst allerdings nur die Namen der Stationen richtig auf, denen der eigene DHCP-Server die Adressinformationen zugewiesen hat. Damit der DNS-Server auch die Namen anderer DHCP-Server auflösen kann, können die DHCP-Server im Cluster betrieben werden. In dieser Betriebsart verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern im Cluster angemeldet haben.

A.2.2 Konfiguration

Der Betrieb eines DHCP-Servers im Cluster kann für jedes einzelne ARF-Netz in den zugehörigen DHCP-Einstellungen aktiviert bzw. deaktiviert werden.

WEBconfig: LCOS-Menübaum ► Setup ► DHCP ► Netzliste

■ Cluster

Wählen Sie hier aus, ob der DHCP-Server für dieses ARF-Netz im Cluster oder separat betrieben werden soll.

Mögliche Werte:

- Ja: Wenn der Cluster-Betrieb aktiviert ist, verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern in Cluster angemeldet haben. Diese Stationen werden in der DHCP-Tabelle mit dem Flag "cache" gekennzeichnet.
- Nein: Der DHCP-Server verwaltet nur Informationen über die bei ihm selbst angeschlossenen Stationen.

Default:

- Nein



Wenn die Lease-Time der über DHCP zugewiesenen Informationen abläuft, schickt eine Station eine Anfrage zur Erneuerung an den DHCP-Server, von dem sie die Informationen erhalten hat (Renew-Request).

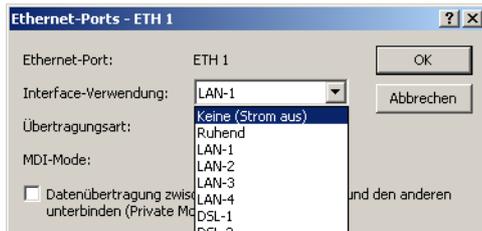
Falls der ursprüngliche DHCP-Server auf diesen Request nicht antwortet, versendet die Station eine Anfrage nach einer neuen DHCP-Anbindung (Rebinding Request) als Broadcast an alle erreichbaren DHCP-Server. Renew-Requests werden von den DHCP-Servern im Cluster ignoriert – so wird ein Rebinding erzwungen, damit alle im Cluster vorhandenen DHCP-Server über den Broadcast ihren Eintrag für die Station erneuern können.

Auf den Rebind-Request antwortet zunächst nur der DHCP-Server, bei dem die Station ursprünglich regist-

riert war. Wird der Rebind-Request von einer Station wiederholt, dann gehen alle DHCP-Server im Cluster davon aus, dass der ursprünglich zuständige DHCP-Server im Cluster nicht mehr aktiv ist und beantworten die Anfrage. Diese Antwort enthält zwar die gleiche IP-Adresse für die Station, kann aber unterschiedliche Gateway- und DNS-Serveradressen enthalten. Die Station sucht sich nun aus den Antworten einen neuen DHCP-Server aus, an den sie von nun an gebunden ist und übernimmt von ihm Gateway und DNS-Server (sowie alle anderen zugewiesenen Parameter).

A.3 Abschalten von Ethernet-Schnittstellen

Die Ethernet-Schnittstellen von öffentlich zugänglichen LANCOM-Geräten können ggf. von unbefugten Anwendern genutzt werden, um physikalischen Zugang zu einem Netzwerk zu erhalten. Um diesen Versuch zu verhindern, können die Ethernet-Schnittstellen der Geräte ausgeschaltet werden.



LANconfig: Schnittstellen ► LAN ► Interface-Einstellungen

WEBconfig: LCOS-Menübaum ► Setup ► Schnittstellen

■ Interface-Verwendung

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Mögliche Werte:

- Keine (Strom aus): Die Schnittstelle ist deaktiviert.
- Ruhend: Die Schnittstelle ist keiner Verwendung zugeordnet, sie ist allerdings physikalisch aktiv.
- LAN-1 bis LAN-n: Die Schnittstelle ist einem logischen LAN zugeordnet.
- DSL-1 bis DSL-n: Die Schnittstelle ist einem DSL-Interface zugeordnet.
- Monitor: Der Port ist ein Monitor-Port, d.h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z.B. ein Paket-Sniffer (wie Wireshark / Ethereal) angeschlossen werden.

Default:

- Abhängig von der jeweiligen Schnittstelle bzw. dem spezifischen Hardware-Modell.

A.4 ARF-Netzwerk für IAPP

Access Points nutzen das IAPP-Protokoll, um sich über die Roaming-Vorgänge der eingebuchten WLAN-Clients zu informieren. Die Access Points senden dazu regelmäßig bestimmte Multicast-Nachrichten aus (Announces), mit deren Hilfe die Geräte die BSSIDs und IP-Adressen der anderen Access Points lernen. Bei einem Roaming-Vorgang informiert der WLAN-Client den neuen Access Point darüber, bei welchem Access Point er bisher eingebucht war. Der neue Access Point kann mit den aus den IAPP-Announces gelernten Informationen den bisherigen Access Point informieren, der den WLAN-Client umgehend aus seiner Tabelle der eingebuchten Clients entfernen kann.

Wenn in einem Access Point mehrere ARF-Netzwerke definiert sind, werden die IAPP-Announces in alle ARF-Netze ausgesendet. Um diese Multicasts auf ein bestimmtes ARF-Netz zu reduzieren, kann gezielt ein IAPP-IP-Netzwerk definiert werden.

WEBconfig: LCOS-Menübaum ► Setup ► WLAN

■ IAPP-IP-Netzwerk

Wählen Sie hier aus, welches ARF-Netzwerk als IAPP-IP-Netzwerk verwendet werden soll.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät definierten ARF-Netzwerke, maximal 16 alphanumerische Zeichen.

Default:

- leer

Besondere Werte:

- leer: Wenn kein IAPP-IP-Netzwerk definiert ist, werden die IAPP-Announces in alle definierten ARF-Netze versendet.

A.5 Routen von lokalen Diensten/ARP-Handling schaltbar

A.5.1 Einleitung

Antwortpakete für interne Dienste (z.B. telnet, http/https, tftp, ...) des LANCOM an Empfänger im Ethernet (LAN oder WAN) wurden bis zur LCOS-Version 7.80 immer direkt an die entsprechenden Absender gesandt, so dass dadurch z. B. auch Geräte von beliebigen LANs heraus gefunden werden konnten.

Ab der LCOS-Version 7.80 ist schaltbar, ob anstelle der direkten Adressierung eine vorherige ARP-Anfrage und das daraus resultierende Routing verwendet werden soll.

Soll beispielsweise ein LANCOM Router auch ohne Kenntnis bzw. Konfiguration der LAN-Topologie durch LANconfig gefunden werden können, so empfiehlt sich das bisherige Verhalten. In diesem Fall antwortet der Router direkt per Unicast an den Absender des TFTP-Broadcasts (hier: LANconfig/Gerätesuche).

In Szenarien, in denen wechselnde, virtuelle MAC- und IP-Adressen im LAN zum Einsatz kommen – beispielsweise bei Nutzung von VRRP-Komponenten im LAN – kann es mit der direkten Adressierung zu Fehlauflösungen kommen, sollte beispielsweise das Redundanzprotokoll eine andere MAC-/IP-Zuordnung vorgenommen haben. In diesen Fällen empfiehlt sich die Einstellung "Interne Dienste routen".

A.5.2 Konfiguration

Mit einer entsprechenden Option in den Einstellungen für das IP-Routing können die internen Dienste des LANCOM über den Router geleitet werden.

WEBconfig: LCOS-Menübaum ► Setup ► IP-Router ► Routing-Methode

■ Interne-Dienste-routen

Wählen Sie hier aus, ob die internen Dienste über den Router geleitet werden sollen.

Mögliche Werte:

- Ja: Die Pakete für die internen Dienste werden über den Router geleitet.
- Nein: Die Pakete werden direkt an den Absender zurückgeschickt.

Default:

- Nein

A.6 XAUTH mit externem RADIUS-Server

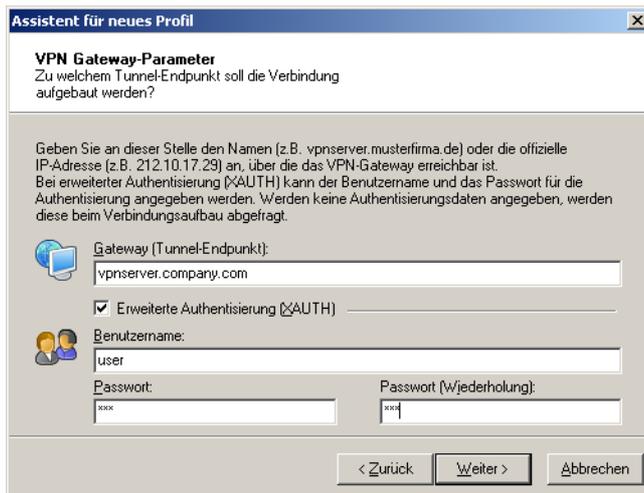
Seit der LCOS-Version 7.60 kann ein LANCOM die Gegenstelle auch über das Extended Authentication Protocol (XAUTH) identifizieren und authentifizieren. Zur Authentifizierung wurden dabei die Benutzerdaten aus der PPP-Liste herangezogen.

Ab der LCOS-Version 7.80 kann die XAUTH-Authentifizierung auch an einen (externen) RADIUS-Server weitergeleitet werden. So können z.B. die auf dem RADIUS-Server schon vorhandenen RAS-Benutzerdaten komfortabel weiter genutzt werden, wenn die RADIUS-authentifizierte Einwahl über PPP auf VPN mit XAUTH umgestellt wird.

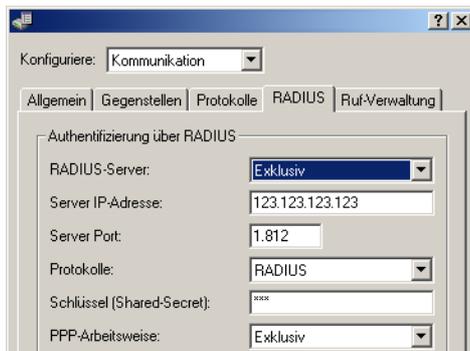
Um einen Einwahlzugang über VPN zusätzlich mit XAUTH zu authentifizieren, gehen Sie folgendermaßen vor:

- ① Richten Sie einen VPN-Einwahlzugang ein, z.B. mit dem Setup-Assistenten von LANconfig.
- ② Aktivieren Sie im VPN-Client der einwählenden Station die Verwendung von XAUTH. Tragen Sie als Benutzernamen und Kennwort die Werte ein, die auch im RADIUS-Server hinterlegt sind.

□ Erweiterte Zertifikats-Unterstützung



- ③ Aktivieren Sie die Authentifizierung der Einwahlgegenstellen über das XAUTH-Protokoll an einem externen RADIUS-Server. Aktivieren Sie unter LANconfig im Konfigurationsbereich **Kommunikation** auf der Registerkarte **RADIUS** für den RADIUS-Server die Betriebsart "Exklusiv". In dieser Einstellung werden die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert.



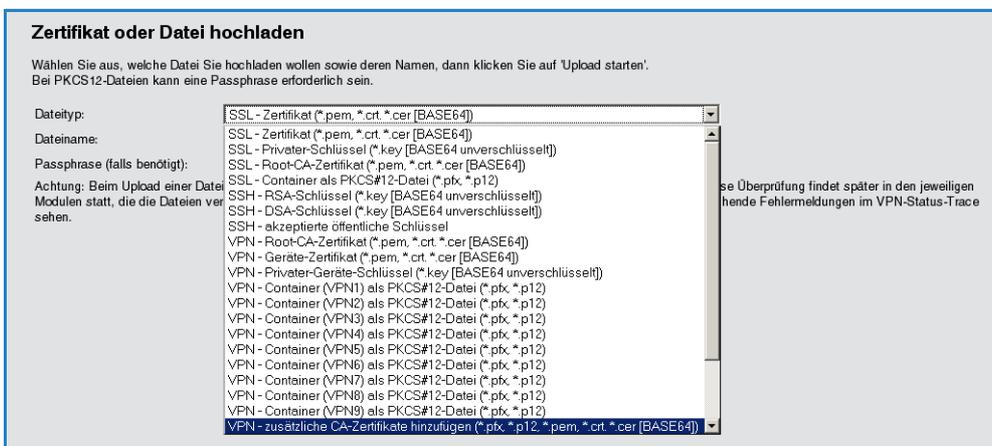
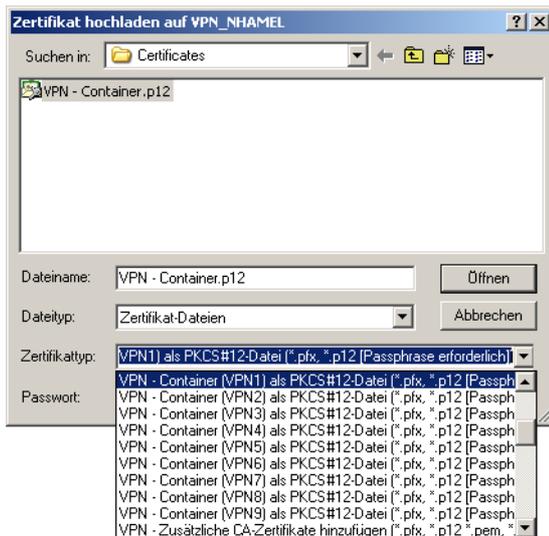
- ④ Geben Sie außerdem für den externen RADIUS-Server die IP-Adresse, den Port, das Protokoll und den Schlüssel an.
- ⑤ Stellen Sie auch die PPP-Arbeitsweise auf "Exklusiv" ein, damit die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert werden.

A.7 Erweiterte Zertifikats-Unterstützung

Zur Unterstützung von mehreren Zertifikats-hierarchien können ab der LCOS-Version 7.80 bis zu neun PKCS#12-Dateien in das Gerät geladen werden. Darüber hinaus können weitere Dateien mit zusätzlichen CA-Zertifikaten hochgeladen werden, in denen die Zertifikate einzeln oder als PKCS#12-Container enthalten sein können. Alle Zertifikats-hierarchien können manuell oder per SCEP verwaltet werden und können CRLs verwenden.

LANconfig: Gerät ▶ Konfigurations-Verwaltung ▶ Zertifikat als Datei hochladen

WEBconfig: Dateimanagement ▶ Zertifikat oder Datei hochladen



Die im Gerät vorhandenen Zertifikate können im Statusbereich eingesehen werden:

WEBconfig: Status ► Status ► Zertifikate ► Gerätezertifikate

Die Gerätezertifikate werden im internen Dateisystem der Geräte den Verwendungszwecken "VPN1" bis "VPN9" zugeordnet.

Zur Nutzung der Zertifikate kann in den IKE-Schlüsseln mit dem Typ ASN.1-Distinguished Name als "lokale Identität" entweder das Subject des Zertifikats oder diese Kurzbezeichnung verwendet werden.

i Durch die Referenzierung der Zertifikate über die Kurzbezeichnung können auch Subjects mit deutschen Umlauten oder anderen Sonderzeichen verwendet werden, die ansonsten aufgrund der Einschränkungen der CLI-Konfiguration nicht angesprochen werden können.

Die Kurzbezeichnung wird bei der Konfiguration der Zertifikate für den SCEP-Client als "Verwendung" eingetragen.

A.8 Wildcard Matching von Zertifikaten

A.8.1 Einleitung

Bei zertifikatsbasierten VPN-Verbindungen werden in der Regel die Subjects (Antragsteller) der verwendeten Zertifikate als lokale und entfernte Identität verwendet. Diese werden in der VPN-Konfiguration in Form von (oftmals komplexen) ASN.1 Distinguished Names (DN) hinterlegt. In der VPN-Verhandlung wird dann die konfigurierte lokale Identität zur Auswahl des eigenen Zertifikates benutzt und an die Gegenstelle übermittelt, während die konfigurierte entfernte Identität mit der empfangenen Identität der Gegenstelle und mit dem Subject des empfangenen Zertifikates verglichen wird.

Die lokale und die entfernte Identität müssen in der VPN-Konfiguration bisher immer vollständig angegeben werden. Dies ist zum einen fehleranfällig, und zum anderen ist es manchmal gewünscht, nur einen Teil des Subjects angeben zu müssen. Praktisch ist dies beispielsweise, um bei einem Zertifikatswechsel oder bei gleichzeitiger Verwendung mehrerer paralleler Zertifikatshierarchien verschiedene Zertifikate mit ähnlichem Subject automatisch zu akzeptieren.

Um dies zu ermöglichen, kann ein flexiblerer Identitätsvergleich verwendet werden. Die in den konfigurierten Identitäten enthaltenen Komponenten eines ASN.1-Distinguished Name (DN) (Relative Distinguished Names – RDNs) müssen in den relevanten Subjects dabei nur enthalten sein. Die Reihenfolge der RDNs ist dabei beliebig. Darüber hinaus können die Werte der RDNs die Wildcards '?' und '*' beinhalten. Werden die Wildcards als Teil des RDNs benötigt, müssen sie in Form von '\?' bzw. '*' angegeben werden. Beispiele:

- Subject = '/CN=Max Mustermann/O=*ACME*', DN = '/CN=Max?Muster*'
- Subject = '/CN=Max Mustermann/O=*ACME*', DN = '/O=*ACME*'

A.8.2 Konfiguration

Der flexible Identitätsvergleich kann in der VPN-Konfiguration aktiviert bzw. deaktiviert werden.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ VPN

■ Flexible-ID-Comparison

Mögliche Werte:

- Ja, Nein

Default:

- Nein

Der flexible Identitätsvergleich wird sowohl bei der Prüfung der (empfangenen) entfernten Identität als auch bei der Zertifikatsauswahl durch die lokale Identität eingesetzt.

A.9 Mehrere WLAN-Profil im Client-Modus

A.9.1 Einleitung

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können LANCOM Access Points in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-Client verhalten und nicht wie ein Access Point (AP).

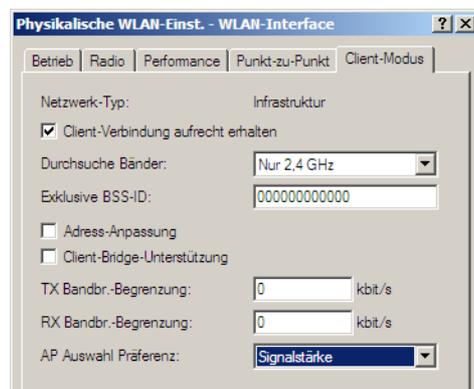
WLAN-Clients wie Notebooks können in der Regel über das Betriebssystem oder über die gerätespezifische Software verschiedene Profile speichern und verwalten, um je nach Umgebung auf verschiedene Access Points zuzugreifen (z.B. für ein WLAN im Unternehmen und für ein weiteres WLAN im Home-Office). In diesen Profilen sind u.a. die SSID des entsprechenden WLANs und die benötigten Schlüssel gespeichert. Der WLAN-Client wählt dann automatisch aus den verfügbaren WLANs das passende Profil für das stärkste oder das bevorzugte WLAN.

LANCOM Access Points können bis zu acht verschiedene WLAN-Profil für die Verwendung im Client-Modus speichern. Für die Profile werden im Client-Modus die Netzwerk- sowie Übertragungsparameter für die logischen WLANs sowie die Verschlüsselungseinstellungen verwendet.

 Bitte beachten Sie, dass Sie ein WLAN-Modul im Client-Modus sich zu jeder Zeit nur mit einem Access Point verbinden kann, auch wenn mehrere WLAN-Profil definiert sind.

A.9.2 Konfiguration

Neben den Netzwerk-, Übertragungs und Verschlüsselungsparametern kann für jedes WLAN-Modul separat definiert werden, nach welchem Kriterium das zu verwendende Client-Profil ausgewählt werden soll.



LANconfig: WLAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Client-Modus

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Client-Einstellungen ▶ WLAN-1

■ AP Auswahl Präferenz

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Mögliche Werte:

- Signalstärke: Wählt das Profil, dessen WLAN aktuell das stärkste Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald diese ein stärkeres Signal bietet.
- Profil: Wählt aus den verfügbaren WLANs das zu verwendende Profil in der Reihenfolge der definierten Einträge (WLAN-Index, z.B. WLAN-1, WLAN-1-2 etc.), auch wenn ein anderes WLAN ein stärkeres Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald ein WLAN mit einem niedrigeren WLAN-Index erkannt wird (unabhängig von der Signalstärke dieses WLANs).

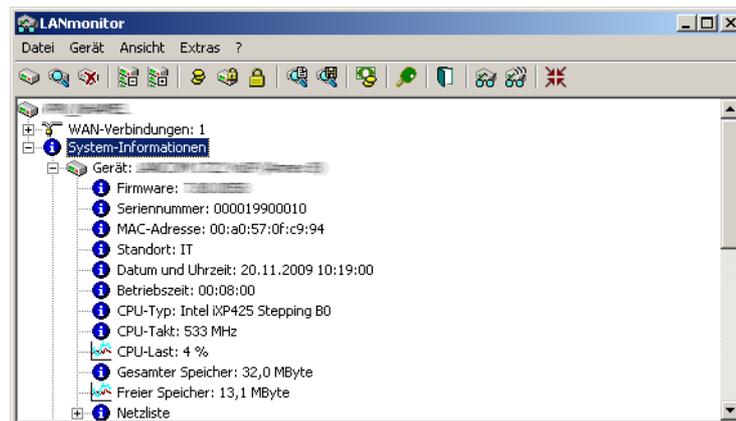
Default:

- Signalstärke.

A.10 Mittelwert der CPU-Lastanzeige

A.10.1 Einleitung

Die aktuelle CPU-Last der Geräte wird über verschiedene Ausgabemöglichkeiten angezeigt (LANmonitor, über WEBconfig oder CLI im Status-Bereich, bei einigen Modellen im Display).



A.10.2 Konfiguration

Je nach Bedarf können Sie einstellen, über welchen Zeitraum die angezeigte CPU-Last gemittelt werden soll.

WEBconfig: LCOS-Menübaum ► Setup ► Config

■ CPU-Last-Intervall

Hier können Sie die den Zeitraum zur Mittelung der CPU-Lastanzeige auswählen. Die Anzeige der CPU-Last im LANmonitor, im Status-Bereich, im Display (sofern vorhanden) sowie in evtl. genutzten SNMP-Tools basiert auf dem hier eingestellten Mittelungszeitraum. Im Status-Bereich unter WEBconfig oder CLI werden zusätzlich die CPU-Lastwerte für alle vier möglichen Mittelungszeiträume angezeigt.

Mögliche Werte:

- 1, 5, 60 oder 300 Sekunden.

Default:

- 60 Sekunden.



Die defaultmäßige Mittelung über 60 Sekunden ist in der HOST-RESOURCES-MIB vorgeschrieben, die von gängigen SNMP-Tools zur Anzeige der CPU-Last in einem Tacho-Display verwendet wird. Bitte beachten Sie diese Vorgabe bei der Anpassung des CPU-Last-Intervalls.

Hardware-Info	
Board-Revision	A
CPU-Last-1s-Prozent	4
CPU-Last-300s-Prozent	4
CPU-Last-5s-Prozent	7
CPU-Last-60s-Prozent	4
CPU-Last-Prozent	4
CPU-Takt-MHz	533
CPU-Typ	Intel iXP425 Stepping B0

A.11 TACACS+- Umgehung

A.11.1 Einleitung

Mit der Nutzung von TACACS+ können alle Konfigurationsschritte auf einem Netzwerkgerät einer besonderen Prüfung (Autorisierung) unterzogen werden. Gleichzeitig können über das entsprechende TACACS+-Accounting die durchgeführten Konfigurationsschritte protokolliert und so nachvollziehbar gemacht werden. Die Verwendung von TACACS+ ist u.a. in Systemen für den elektronischen Zahlungsverkehr erforderlich (PCI-Compliance).

Die strikte Überwachung der ausgeführten Konfigurationsschritte führt allerdings zu einem zusätzlichen Austauschen von Anfragen und Nachrichten mit dem oder den verwendeten TACACS+-Servern. In großen Szenarien kann die TACACS+-Kommunikation bei der Verwendung von Skripten für zentrale Konfigurationsänderungen oder bei regelmäßigen Aktionen über CRON-Befehle zu einer Überlastung der TACSACS+-Server führen.

A.11.2 Konfiguration

Um eine mögliche Überlastung der TACACS+-Server durch automatisierte Konfigurationsschritte zu vermeiden, können die Verwendung von CRON, die Aktionstabelle und der Einsatz von Skripten von der Autorisierung und dem Accounting über TACACS+ ausgenommen werden.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ TACACS+

■ Umgehe-Tacacs-fuer-CRON/Skripte/Aktions-Tabelle

Hier können Sie die Umgehung der TACACS-Autorisierung und des TACACS+-Accounting für verschiedene Aktionen aktivieren bzw. deaktivieren.

Mögliche Werte:

Aktiviert, deaktiviert.

Default:

Deaktiviert.



Bitte beachten Sie, dass die Funktion von TACACS+ für das gesamte System über diese Optionen beeinflusst wird. Beschränken Sie die Nutzung von CRON, der Aktionstabelle und von Skripten auf jeden Fall auf einen absolut vertrauenswürdigen Kreis von Administratoren!

A.12 Erweiterungen für die seriellen COM-Ports

A.12.1 Einleitung

Die Konfiguration der COM-Ports wurde um verschiedene Parameter erweitert.

A.12.2 Konfiguration

Die zusätzlichen Parameter befinden sich in den Netzwerkeinstellungen der COM-Ports.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Netzwerk-Einstellungen

■ Nehme-Binaermodus-an

Manche Netzwerkgeräte, die an einem seriellen COM-Port angeschlossen sind, versenden Datenstrukturen, die als Steuerzeichen (CR/LF – Carriage Return / Line Feed) interpretiert werden können. In der Standardeinstellung werten die COM-Ports in den LANCOM-Geräten diese Informationen aus, um den Datenfluss zu steuern. Mit dem "Binärmodus" kann ein COM-Port angewiesen werden, alle Daten binär weiterzuleiten und keine Anpassungen dieser Steuerzeichen vorzunehmen.

Mögliche Werte:

Ja, nein.

Default:

Nein.

■ Newline-Konversion

Wählen Sie hier aus, welches Zeichen auf dem seriellen Port ausgegeben wird, wenn der Binär-Modus aktiviert ist.

Die Einstellung ist abhängig von der Anwendung, die über den seriellen Port kommunizieren wird. Wenn an den Port ein weiteres LANCOM-Gerät angeschlossen ist, können Sie hier entweder CRLF oder nur CR wählen, da die Outband-Schnittstelle dieser Geräte ein "Carriage Return" zur automatischen Bestimmung der Datenübertragungsgeschwindigkeit erwartet. Manche Unix-Anwendungen würden CRLF allerdings als unerlaubte doppelte Zeilenschaltung interpretieren, in diesem Fall wählen Sie CR oder LF.

Mögliche Werte:

- CRLF, CR, LF

Default:

- CRLF



Diese Einstellung wird nur ausgewertet, wenn für diesen seriellen Port der Binär-Modus **deaktiviert** ist.

■ TCP-Keepalive

Der RFC 1122 definiert ein Verfahren, mit dem die Verfügbarkeit von TCP-Verbindungen geprüft werden kann (TCP-Keepalive). Ein inaktiver Transmitter sendet nach diesem Verfahren Anfragen nach dem Empfängerstatus an die Gegenstelle. Wenn die TCP-Sitzung zur Gegenstelle verfügbar ist, antwortet diese mit ihrem Empfängerstatus. Wenn die TCP-Sitzung zur Gegenstelle nicht verfügbar ist, wird die Anfrage in einem kürzeren Intervall solange wiederholt, bis die Gegenstelle mit ihrem Empfängerstatus antwortet (danach wird wieder ein längeres Intervall verwendet). Sofern die zugrunde liegende Verbindung funktioniert, die TCP-Sitzung zur Gegenstelle allerdings nicht verfügbar ist, sendet die Gegenstelle ein RST-Paket und löst so den Abbau der TCP-Sitzung bei der anfragenden Applikation aus.

Mögliche Werte:

- inaktiv: Der TCP-Keepalive wird nicht verwendet.
- aktiv: Der TCP-Keepalive ist aktiv, nur RST-Pakete führen zum Abbau von TCP-Sitzungen.
- proaktiv: Der TCP-Keepalive ist aktiv, wiederholt die Anfrage nach dem Empfängerstatus der Gegenstelle aber nur für den als "TCP-Wdh.-Zahl" eingestellten Wert. Sofern nach dieser Anzahl von Anfragen keine Antwort mit dem Empfängerstatus vorliegt, wird die TCP-Sitzung als "nicht verfügbar" eingestuft und an die Applikation gemeldet. Wird während der Wartezeit ein RST-Paket empfangen, so löst dieses vorzeitig den Abbau der TCP-Sitzung aus.

Default:

- inaktiv



Für Serverapplikationen wird die Einstellung "aktiv" empfohlen.

■ TCP-Keepalive-Intervall

Dieser Wert gibt an, in welchen Intervallen die Anfragen nach dem Empfängerstatus versendet werden, wenn die erste Anfrage nicht erfolgreich beantwortet wurde. Der dazu gehörende Timeout wird gebildet als Intervall / 3 (maximal 75 Sekunden).

Mögliche Werte:

- maximal 10 Ziffern

Default:

- 0

Besondere Werte:

- 0 verwendet den Standardwert nach RFC 1122 (Intervall 7200 Sekunden, Timeout 75 Sekunden).

■ TCP-Wdh.-Timeout

Maximale Zeit für den Retransmission-Timeout. Dieser Timeout gibt an, in welchen Intervallen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

Mögliche Werte:

- 0 bis 99 Sekunden.

Besondere Werte:

□ 32 zusätzliche Gateways für PPTP-Verbindungen

- 0 verwendet den Standardwert nach RFC 1122 (60 Sekunden).

Default:

- 0



Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

■ **TCP-Wdh.-Zahl**

Maximale Anzahl der Versuche, mit denen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

Mögliche Werte:

- 0 bis 9

Besondere Werte:

- 0 verwendet den Standardwert nach RFC 1122 (5 Versuche).

Default:

- 0



Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

A.13 32 zusätzliche Gateways für PPTP-Verbindungen

A.13.1 Einleitung

Zur Sicherung der Erreichbarkeit können für jede PPTP-Gegenstelle bis zu 32 zusätzliche Gateways konfiguriert werden, so dass insgesamt pro PPTP-Gegenstelle 33 Gateways genutzt werden können.

A.13.2 Konfiguration

Die zusätzlichen PPTP-Gateways werden in einer separaten Liste definiert.



LANconfig: Kommunikation ▶ Protokolle ▶ Weitere entfernte Gateways

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WAN ▶ Zusätzliche-PPTP-Gateways

■ **Name der Verbindung**

Wählen Sie hier aus, für welche PPTP-Gegenstelle dieser Eintrag gelten soll.

Mögliche Werte:

- Auswahl aus der Liste der definierten PPTP-Gegenstellen.

Default:

- leer.

■ **Anfangen mit**

Wählen Sie hier aus, in welcher Reihenfolge die Einträge versucht werden sollen.

Mögliche Werte:

- Zuletzt benutzt: Wählt den Eintrag, zu dem zuletzt erfolgreich eine Verbindung hergestellt werden konnte.
- Erstem: Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.
- Zufall: Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load Balancing für die Gateways in der Zentrale.

Default:

- Zuletzt benutzt

■ **Gateway 2 bis 33**

Tragen Sie hier die IP-Adressen der zusätzlichen Gateways ein, die für diese PPTP-Gegenstelle verwendet werden können.

Mögliche Werte:

- IP-Adresse oder 63 alphanumerische Zeichen.

Default:

- leer.

■ **Routing-Tag**

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Mögliche Werte:

- maximal 5 Ziffern.

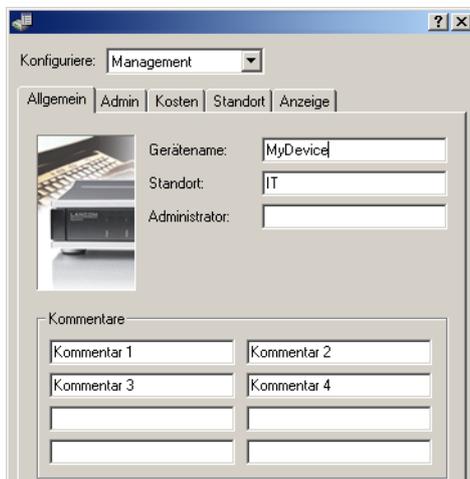
Default:

- 0.

 Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

A.14 Zusätzliche Kommentarfelder zur Beschreibung der Geräte

Zur Beschreibung der LANCOM-Geräte können bis zu acht Kommentare eingetragen werden.



LANconfig: Management ► Allgemein

WEBconfig: LCOS-Menübaum ► Setup ► SNMP

■ **Kommentar 1 bis 8**

Tragen Sie hier einen Kommentar ein.

Mögliche Werte:

- maximal 255 alphanumerische Zeichen.

Default:

- leer

A.15 DHCP-Optionen mit LANconfig

Mit den DHCP-Optionen können zusätzliche Konfigurationsparameter an die Stationen übertragen werden. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt so z. B. den Gerätetyp an. In dieser Tabelle werden zusätzliche Optionen für den DHCP-Betrieb definiert.



LANconfig: Management ► Allgemein

WEBconfig: LCOS-Menübaum ► Setup ► DHCP ► Zusätzliche-Optionen

■ Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. "17" (Root Path) für den Pfad zu einem Boot-Image für einen PC ohne eigene Festplatte, der über BOOTP sein Betriebssystem bezieht.

Mögliche Werte:

- maximal 3 Ziffern.

Default:

- leer



Eine Liste aller DHCP-Optionen finden Sie im RFC 2132 – DHCP Options and BOOTP Vendor Extensions der Internet Engineering Task Force (IETF).

■ Netzwerkname

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät definierten IP-Netzwerke, maximal 16 Zeichen.

Default:

- leer

■ Typ

Typ des Eintrags. Dieser Wert ist abhängig von der jeweiligen Option. Für die Option "35" wird hier im RFC 2132 z. B. der ARP Cache Timeout so definiert:

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

Aus dieser Beschreibung können Sie ablesen, dass für diese Option der Typ "32-Bit-Integer" verwendet wird.

Mögliche Werte:

- String, Integer8, Integer16, Integer32, IP-Adresse

Default:

- String



Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DHCP-Optionen der jeweiligen Herstellerdokumentation.

■ Wert

In diesem Feld wird der Inhalt der DHCP-Option definiert.

IP-Adressen werden in der üblichen Schreibweise von IPv4-Adressen angegeben, also z. B. als "123.123.123.100", Integer-Typen werden als normale Dezimalzahlen eingetragen, Strings als einfacher Text.

Mehrere Werte in einem Feld werden mit Kommas separiert, also z. B. "123.123.123.100, 123.123.123.200".

Mögliche Werte:

Maximal 128 Zeichen.

Default:

leer



Die mögliche Länge des Optionswertes entnehmen Sie bitte dem entsprechenden RFC bzw. bei hersteller-spezifischen DHCP-Optionen der jeweiligen Herstellerdokumentation.

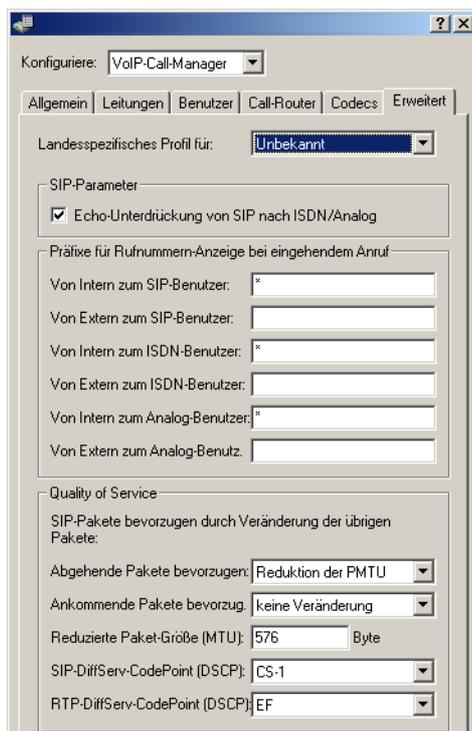
A.16 Ermittlung des Routing-Tags für lokale Routen

Mit der Definition von Schnittstellen-Tags können im Rahmen des Advanced Routing and Forwarding (ARF) virtuelle Router genutzt werden, die nur einen Teil der gesamten Routing-Tabelle verwenden. Für ein von einem anderen lokalen Router empfangenes Paket wird das Schnittstellen-Tag in den folgenden Schritten ermittelt:

- ① Wenn die Absenderadresse eines Pakets direkt einem im Gerät definierten IP-Netz zugeordnet werden kann, dann wird das Schnittstellen-Tag des IP-Netzes verwendet.
- ② Wenn an dem Interface, über das ein Paket empfangen wurde, nur ein IP-Netz gebunden ist, dann wird das Schnittstellen-Tag dieses IP-Netzes verwendet.
- ③ Wenn die Möglichkeiten ① und ② kein eindeutiges Ergebnis liefern, versucht das Gerät anhand der MAC-Adresse die IP-Adresse des Next-Hops zu ermitteln (reverse ARP-Lookup). Anhand dieser IP-Adresse versucht das Gerät, das zugehörige IP-Netz und so das Schnittstellen-Tag zu ermitteln.
- ④ Wenn die Möglichkeiten ① bis ③ kein eindeutiges Ergebnis liefern, versucht das Gerät anhand der Einträge in der Routing-Tabelle das zugehörige IP-Netz und so das Schnittstellen-Tag zu ermitteln.

A.17 Globale Einstellung von DiffServ für SIP & RTP

Der Voice-Call-Manager markiert SIP- und RTP-Pakete mit sogenannten DiffServ-CodePoints (DSCP), um es nachgeschalteter Hardware zu ermöglichen, diese Pakete zu erkennen und richtig zu priorisieren.



LANconfig: Voice- Call- Manager ► Erweitert

WEBconfig: LCOS-Menübaum ► Setup ► Voice- Call- Manager ► General

■ **SIP-DiffServ-CodePoint (DSCP)**

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die SIP-Pakete (Anruf-Signalisierung) markiert werden.

Mögliche Werte:

- 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

i Die Verwendung von CS-1 ist heute überholt und zur Erhaltung der Abwärts-Kompatibilität als Default gesetzt. Typische Werte für aktuellen VoIP-Installationen sind CS-3, AF-31 oder AF-41. Wegen großer Verbreitung im Markt empfehlen wir den Einsatz von CS-3.

■ **RTP-DiffServ-CodePoint (DSCP)**

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die RTP-Pakete (Voice-Datenstrom) markiert werden.

Mögliche Werte:

- 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

i Bei der Einstellung DSCP BE bzw. CS-0 werden die Pakete ohne Markierung versendet. Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel "QoS".

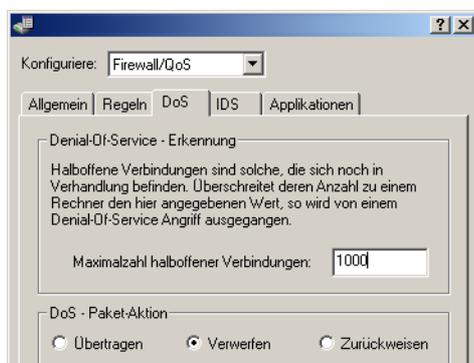
A.18 Erhöhter DoS-Schwellwert für Zentralgeräte

Denial-Of-Service Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementierungen aus.

- Zu den Angriffen, die prinzipielle Schwächen ausnutzen, gehören z.B. SYN-Flood und Smurf.
- Zu den Angriffen, die fehlerhafte Implementierungen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z.B. Teardrop) oder mit gefälschten Absenderadressen arbeiten (z.B. Land).

Ihr Gerät erkennt die meisten dieser Angriffe und kann mit gezielten Gegenmaßnahmen reagieren. Für diese Erkennung wird die Anzahl der Verbindungen ermittelt, die sich noch in Verhandlung befinden (halboffene Verbindungen). Überschreitet die Anzahl der halboffenen Verbindungen einen Schwellwert, geht das Gerät von einem DoS-Angriff aus. Die dann resultierenden Aktionen und Maßnahmen können wie bei Firewall-Regeln definiert werden.

! Für Zentralgeräte befinden sich aufgrund der zumeist höheren Anzahl der angeschlossenen Benutzer auch ohne DoS-Angriff eine große Zahl von Verbindungen im halboffenen Zustand. Aus diesem Grund verwenden diese Geräte einen höheren Standard-Schwellwert für die Erkennung der DoS-Angriffe.



LANconfig: Firewall/QoS ► DoS

WEBconfig: LCOS-Menübaum ► Setup ► IP-Router ► Firewall

■ **Maximalzahl halboffene Verbindungen**

Legen Sie hier fest, ab welcher Anzahl von halboffenen Verbindungen die Aktionen zur Abwehr von DoS-Angriffen ausgelöst werden sollen.

Mögliche Werte:

0 bis 9999

Default:

100

1000 für Zentralgeräte wie 7100, 7111, 8011, 9100, 4025(+), 4100.