LCOS 10.72

Addendum

05/2024

LANCOM SYSTEMS

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

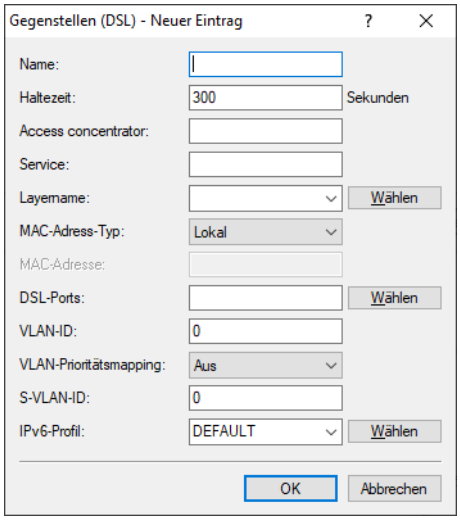
1 Addendum zur LCOS-Version 10.72

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.72 gegenüber der vorherigen Version.

2 Virtuelle LANs (VLANs)

2.1 Q-in-Q-VLAN

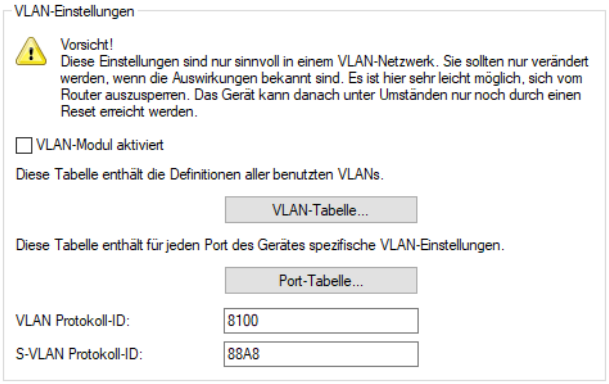
Ab LCOS 10.72 unterstützt der Router doppeltes VLAN-Tagging („stacked VLAN") bzw. Q-in-Q-VLAN nach IEEE 802.1ad auf WAN-Verbindungen. Mit Q-in-Q-VLAN können Service Provider Layer-2-Ethernetverbindungen zwischen Kundenstandorten ermöglichen und das kundeneigene VLAN unverändert übertragen. Das innere VLAN (C-VLAN) wird dabei vom Kunden verwendet, das äußere VLAN (S-VLAN) vom Service Provider.



LANconfig: **Kommunikation** > **Gegenstellen** > **Gegenstellen (DSL)**

S-VLAN-ID

Konfigurieren Sie hier das S-VLAN bei doppeltem VLAN-Tagging (Q-in-Q-VLAN-Verbindungen nach IEEE 802.1ad). Das VLAN wird auch als äußeres VLAN bezeichnet. Die verwendete S-VLAN-Protokoll-ID kann unter **Schnittstellen** > **VLAN** konfiguriert werden.



LANconfig: **Schnittstellen** > **VLAN**

S-VLAN Protokoll-ID

Definiert die VLAN-Tagging-ID für Q-in-Q-VLAN-Tagging. Der Ethernet2-Typ des VLAN-Tags wird als „Tag-Value" als 16 Bit-Hexadezimalwert konfiguriert. Default nach IEEE 802.1ad ist „88a8", ein anderer gängiger Wert für VLAN-Tagging wäre z. B. „8100".

2.1.1 Ergänzungen im Setup-Menü

S-VLAN-ID

Konfigurieren Sie hier das S-VLAN bei doppeltem VLAN-Tagging (Q-in-Q-VLAN-Verbindungen nach IEEE 802.1ad). Das VLAN wird auch als äußeres VLAN bezeichnet. Die verwendete S-VLAN-Protokoll-ID kann unter *2.32.6 S-Tag-Wert* auf Seite 6 konfiguriert werden.

SNMP-ID:

2.2.19.21

Pfad Konsole:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

0 … 4096

Default-Wert:

0

S-Tag-Wert

Definiert die VLAN-Tagging-ID für Q-in-Q-VLAN-Tagging. Der Ethernet2-Typ des VLAN-Tags wird als „Tag-Value" als 16 Bit-Hexadezimalwert konfiguriert. Default nach IEEE 802.1ad ist „88a8", ein anderer gängiger Wert für VLAN-Tagging wäre z. B. „8100".

SNMP-ID:

2.32.6

Pfad Konsole:

Setup > **VLAN**

Mögliche Werte:

max. 4 Zeichen aus `[0-9][a-f]`

Default-Wert:

88a8

3 Backup-Lösungen

3.1 Schalter für eine Master-Holddown-Zeit im VRRP

Ab LCOS 10.72 wird ein neuer Schalter für eine Master-Holddown-Zeit im VRRP unterstützt. Dazu wurde in LANconfig unter **IP-Router** > **VRRP** der Parameter **Master-Holddown-Zeit** hinzugefügt.

Master-Holddown-Zeit

Wenn hier eine Zeit konfiguriert ist, wechselt der virtuelle Router in den Zustand „Hold-Down“, sobald die überwachte WAN-Verbindung mit einem Fehler abgebaut wird und das Backup-Delay abläuft (also in den Backupzustand wechselt). Im Zustand „Hold-Down“ kann die überwachte WAN-Verbindung nicht mehr aufgebaut werden. Des Weiteren werden keine VRRP-Advertisements mehr geschickt.

Sobald die „Master-Holddown-Zeit“ abläuft, wechselt der virtuelle Router in den Zustand „Standby“, in dem die überwachte WAN-Verbindung wiederaufgebaut werden kann.

Die „Master-Holddown-Time“ ist ein String von maximal 6 Zeichen, der die Ziffern 0-9 und den Doppelpunkt enthalten kann. Damit können Zeiten von maximal 999 Minuten 59 Sekunden (999:59) eingegeben werden.

Ist kein Doppelpunkt vorhanden (z. B. „30“) dann wird die Angabe als Minuten interpretiert. Hier ist dennoch maximal „999“ möglich.

Ist ein Doppelpunkt vorhanden, müssen nach dem Doppelpunkt zwei Zeichen kommen, die als Sekunden interpretiert werden. Hier sind maximal „59“ möglich.

Korrekte Zeitangaben sind also z. B. „5“ (5 Minuten), „5:30“ (5 Minuten, 30 Sekunden) oder „0:30“ (30 Sekunden).

Ein Wert von „0“ oder „0:00“ deaktiviert den Master-Holddown.

3.1.1 Ergänzungen im Setup-Menü

Master-Holddown-Zeit

Wenn hier eine Zeit konfiguriert ist, wechselt der virtuelle Router in den Zustand „Hold-Down“, sobald die überwachte WAN-Verbindung mit einem Fehler abgebaut wird und das Backup-Delay abläuft (also in den Backupzustand wechselt). Im Zustand „Hold-Down“ kann die überwachte WAN-Verbindung nicht mehr aufgebaut werden. Des Weiteren werden keine VRRP-Advertisements mehr geschickt.

Sobald die „Master-Holddown-Zeit” abläuft, wechselt der virtuelle Router in den Zustand „Standby“, in dem die überwachte WAN-Verbindung wiederaufgebaut werden kann.

Die „Master-Holddown-Time“ ist ein String von maximal 6 Zeichen, der die Ziffern 0-9 und den Doppelpunkt enthalten kann. Damit können Zeiten von maximal 999 Minuten 59 Sekunden (999:59) eingegeben werden.

Ist kein Doppelpunkt vorhanden (z. B. „30“) dann wird die Angabe als Minuten interpretiert. Hier ist dennoch maximal „999“ möglich.

Ist ein Doppelpunkt vorhanden, müssen nach dem Doppelpunkt zwei Zeichen kommen, die als Sekunden interpretiert werden. Hier sind maximal „59“ möglich.

Korrekte Zeitangaben sind also z. B. „5“ (5 Minuten), „5:30“ (5 Minuten, 30 Sekunden) oder „0:30“ (30 Sekunden).

Ein Wert von „0“ oder „0:00“ deaktiviert den Master-Holddown.

SNMP-ID:

2.8.21.6

Pfad Konsole:

Setup > **IP-Router** > **VRRP**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]:`

Default-Wert:

0

4 Weitere Dienste

4.1 BPjM-Modul mit Absendeadresse

Ab LCOS 10.72 wurde das BPjM-Modul um die optionale Angabe einer Absendeadresse erweitert. Dazu wurde in LANconfig unter **Sonstige Dienste** > **Dienste** > **BPjM-Filter** der Parameter **Absende-Adresse** hinzugefügt.

Absende-Adresse

Absende-Adresse, die vom BPjM-Modul verwendet wird, um den Server für BPjM-Signatur-Updates zu erreichen.

4.1.1 Ergänzungen im Setup-Menü

BPJM

Einstellungen des BPjM-Moduls.

SNMP-ID:

2.110.5

Pfad Konsole:

Setup > **Firewall** > **BPJM**

BPJM-Loopback-Adresse

Absende-Adresse, die vom BPjM-Modul verwendet wird um, den Server für BPjM-Signatur-Updates zu erreichen.

SNMP-ID:

2.110.5.1

Pfad Konsole:

Setup > **Firewall** > **BPJM**

Mögliche Werte:

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

Default-Wert:

leer

5 Ergänzungen im Menüsystem

5.1 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.2.22.28

Pfad Konsole:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.2 L2TP-Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.2.22.29

Pfad Konsole:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.3 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.11.81.1.10

Pfad Konsole:

Setup > **Config** > **RADIUS** > **Server**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.4 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.12.29.21

Pfad Konsole:

Setup > **WLAN** > **RADIUS-Zugriffspruefung**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.5 Backup-Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.12.29.22

Pfad Konsole:

Setup > **WLAN** > **RADIUS-Zugriffspruefung**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.6 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.19.36.9.1.1.11

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

nein
Access-Requests müssen keinen Message-Authenticator enthalten.

ja
Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.7 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.25.10.2.6

Pfad Konsole:

Setup > **RADIUS** > **Server** > **Clients**

Mögliche Werte:

nein
Access-Requests müssen keinen Message-Authenticator enthalten.

ja
Access-Requests müssen immer einen Message-Authenticator enthalten.

Nur-Proxy
Falls ein Access-Request ein Proxy-State-Attribut enthält, muss ein Message-Authenticator enthalten sein.

Default-Wert:

nein

5.8 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.25.10.3.18

Pfad Konsole:

Setup > **RADIUS** > **Server** > **Weiterleit-Server**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Default-Wert:

nein

5.9 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.72 RU8. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

SNMP-ID:

2.25.10.16.6

Pfad Konsole:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Mögliche Werte:

nein

Access-Requests müssen keinen Message-Authenticator enthalten.

ja

Access-Requests müssen immer einen Message-Authenticator enthalten.

Nur-Proxy

Falls ein Access-Request ein Proxy-State-Attribut enthält, muss ein Message-Authenticator enthalten sein.

Default-Wert:

nein