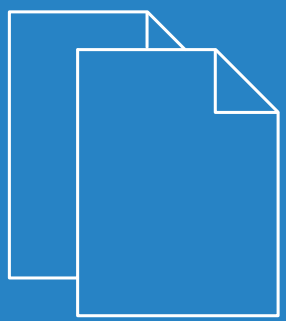
SICHER. **VERNETZT.**

LCOS LX 5.34

Addendum



07/2021

LANCOM Systems

Inhalt

1 Addendum zur LCOS LX-Version 5.34....4
2 Multicast-Snooping....5
2.1 Ergänzungen im Setup-Menü....7
2.1.1 Multicast-Snooping....7
2.1.2 Multicast-To-Unicast....8
3 USB-Ethernet-Support....9
3.1 Ergänzungen im Setup-Menü....9
3.1.1 USB....9

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS LX-Version 5.34

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 5.34 gegenüber der vorherigen Version.

2 Multicast-Snooping

Ab LCOS LX 5.34 können Sie Multicast-Snooping aktivieren.

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

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

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

Videostreams werden z. B. häufig als Multicast übertragen, aber nicht alle Stationen im Netzwerk sollen einen bestimmten Stream empfangen.

Verschiedene Anwendungen im medizinischen Bereich nutzen Multicasts, um Daten an bestimmte Endgeräte zu übertragen, die nicht an allen Stationen eingesehen werden sollen.

Bei einer LAN-Bridge im Gerät wird es daher auch Ports geben, an denen kein einziger Empfänger des Multicasts angeschlossen ist. Das „überflüssige“ Versenden der Multicasts auf Ports ohne Empfänger ist zwar kein Fehler, es führt aber gerade in WLAN-Netzwerken zu Performance-Problemen. Dort kann die unnötige Aussendung der Multicasts zu einer deutlichen Einschränkung der verfügbaren Bandbreite führen, da Multicasts im WLAN – genau wie Broadcasts – mit der niedrigst möglichen Übertragungsrate gesendet werden, damit diese von jedem WLAN-Teilnehmer empfangen werden können.

Mit dem Internet Group Management Protocol (IGMP) für IPv4 sowie Multicast Listener Discovery (MLD) für IPv6 stellt die TCP/IP-Protokollfamilie ein Protokoll bereit, mit dem die Netzwerkstationen dem Router, an dem sie angeschlossen sind, das Interesse an bestimmten Multicasts mitteilen können. Dazu registrieren sich die Stationen bei den Routern für bestimmte Multicast-Gruppen, von denen Sie die entsprechenden Pakete beziehen wollen (Multicast-Registration). IGMP nutzt dazu spezielle Nachrichten zum Anmelden (Join-Messages) und Abmelden (Leave-Messages).

Das Multicast-Snooping macht sich diese Nachrichten zunutze, um zu entscheiden, an welchen Port (also auch, an welche WLAN SSID) Multicasts gesendet werden müssen.

LANconfig: **Sonstige Dienste** > **Multicast Snooping**

Betrieb

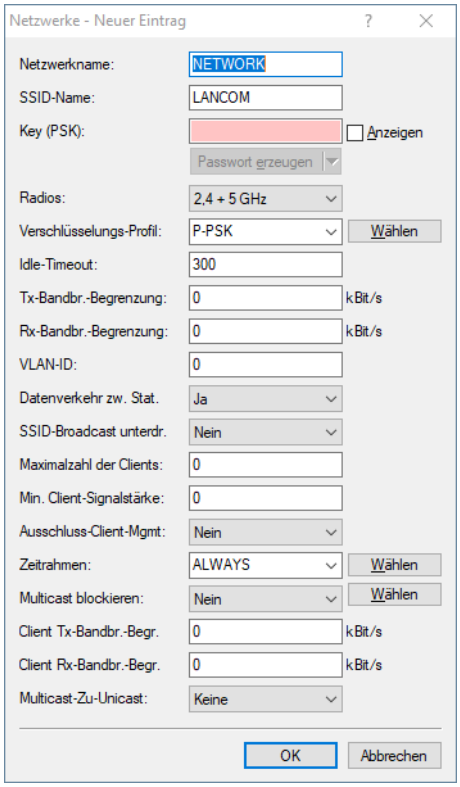
Schalten Sie Multicast-Snooping ein oder aus.

Zusätzlich ist optional eine Konvertierung von Multicast-Datenströmen in Unicast möglich. Multicast-Datenströme, die über WLAN-Interfaces übertragen werden sollen, werden nach Aktivierung des Features in einzelne Unicast-Datenströme je Client auf dem MAC-Layer bzw. WLAN-Layer konvertiert. Die Pakete werden zwar je Client dupliziert, können aber, da es sich nun um Unicasts handeln, mit der für diesen Client höchstmöglichen Datenrate übertragen werden. Auch

wenn die Pakete nun dupliziert werden, wird durch die viel schnellere Übertragung in den meisten Szenarien insgesamt deutlich weniger Airtime verbraucht, die dann für andere Übertragungen zur Verfügung steht.

Multicast-zu-Unicast-Konvertierung

LANconfig: **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke**



Multicast-zu-Unicast

Konfigurieren Sie einzeln je WLAN-Netzwerk ob und wie eine Konvertierung von Multicasts in Unicasts vorgenommen werden soll.

Keine

Keine Konvertierung durchführen.

Konvertierung

Die Multicasts werden in Unicasts umgewandelt (Layer-2-Unicast auf dem WLAN-Layer mit Unicast-MAC-Adresse als Ziel). Dies entspricht dem Verhalten im LCOS.

Kapselung

Die Multicasts werden in Unicast-Aggregate gekapselt (A-MSDU mit Unicast-MAC-Adresse als Ziel, die einen einzelnen Layer-2-Multicast beinhaltet). Diese Variante sollte zum Einsatz kommen, wenn Ziel-Anwendungen die Ziel-MAC-Adresse überprüfen. Es ist aber zu beachten, dass Aggregate nicht von 802.11a/b/g-Clients unterstützt werden.

Damit das Feature funktioniert, ist es erforderlich, das IGMP-Snooping auf dem Gerät zu aktivieren und korrekt zu konfigurieren. Über das IGMP-Snooping ermittelt das Gerät, welcher Client welchen Multicast-Strom empfangen möchte. Der Multicast-Konvertierung stehen somit die passenden Ziel-Clients bzw -Adressen für die Konvertierung zur Verfügung.

Beim LW-500 kommt eine Basis-Variante des Multicast-Snooping zu Einsatz, die keine Umwandlung in Unicast unterstützt.

2.1 Ergänzungen im Setup-Menü

2.1.1 Multicast-Snooping

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

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

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

Videostreams werden z. B. häufig als Multicast übertragen, aber nicht alle Stationen im Netzwerk sollen einen bestimmten Stream empfangen.

Verschiedene Anwendungen im medizinischen Bereich nutzen Multicasts, um Daten an bestimmte Endgeräte zu übertragen, die nicht an allen Stationen eingesehen werden sollen.

Bei einer LAN-Bridge im Gerät wird es daher auch Ports geben, an denen kein einziger Empfänger des Multicasts angeschlossen ist. Das „überflüssige“ Versenden der Multicasts auf Ports ohne Empfänger ist zwar kein Fehler, es führt aber gerade in WLAN-Netzwerken zu Performance-Problemen. Dort kann die unnötige Aussendung der Multicasts zu einer deutlichen Einschränkung der verfügbaren Bandbreite führen, da Multicasts im WLAN – genau wie Broadcasts – mit der niedrigst möglichen Übertragungsrate gesendet werden, damit diese von jedem WLAN-Teilnehmer empfangen werden können.

Mit dem Internet Group Management Protocol (IGMP) für IPv4 sowie Multicast Listener Discovery (MLD) für IPv6 stellt die TCP/IP-Protokollfamilie ein Protokoll bereit, mit dem die Netzwerkstationen dem Router, an dem sie angeschlossen sind, das Interesse an bestimmten Multicasts mitteilen können. Dazu registrieren sich die Stationen bei den Routern für bestimmte Multicast-Gruppen, von denen Sie die entsprechenden Pakete beziehen wollen (Multicast-Registration). IGMP nutzt dazu spezielle Nachrichten zum Anmelden (Join-Messages) und Abmelden (Leave-Messages).

Das Multicast-Snooping macht sich diese Nachrichten zunutze, um zu entscheiden, an welchen Port (also auch, an welche WLAN SSID) Multicasts gesendet werden müssen.

SNMP-ID:

2.40

Pfad Konsole:

Setup

Operating

Schalten Sie Multicast-Snooping ein oder aus.

SNMP-ID:

2.40.1

Pfad Konsole:

Setup > **Multicast-Snooping**

Mögliche Werte:

No

Multicast-Snooping ausgeschaltet.

Yes

Multicast-Snooping eingeschaltet.

2.1.2 Multicast-To-Unicast

Konfigurieren Sie einzeln je WLAN-Netzwerk ob und wie eine Konvertierung von Multicasts in Unicasts vorgenommen werden soll.

SNMP-ID:

2.20.1.29

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

None
Conversion

Die Multicasts werden in Unicasts umgewandelt (Layer-2-Unicast auf dem WLAN-Layer mit Unicast-MAC-Adresse als Ziel). Dies entspricht dem Verhalten im LCOS.

Encapsulation

Die Multicasts werden in Unicast-Aggregate gekapselt (A-MSDU mit Unicast-MAC-Adresse als Ziel, die einen einzelnen Layer-2-Multicast beinhaltet). Diese Variante sollte zum Einsatz kommen, wenn Ziel-Anwendungen die Ziel-MAC-Adresse überprüfen. Es ist aber zu beachten, dass Aggregate nicht von 802.11a/b/g-Clients unterstützt werden.

3 USB-Ethernet-Support

Ab LCOS LX 5.34 werden ausgewählte USB-Ethernet-Geräte an Access Points mit USB-Port unterstützt. Hierbei kommt das Protokoll CDC-EEM zum Einsatz. Dazu wird das USB-Ethernet-Gerät mit dem LAN des Access Points gebridget. Die Angabe einer VLAN-ID zur Netzsegmentierung ist möglich. Stellen Sie daher sicher, dass das USB-Ethernet-Gerät in Ihrem Netzwerk und ggf. VLAN entsprechend der Herstellerangaben kommunizieren kann. Folgende USB-Ethernet-Geräte können mit LCOS LX-basierten Access Points betrieben werden:

- Hanshow HS_C09978 ESL Controller
- SoluM EGU200NA0X ESL GEN2 USB Gateway

Die speziellen Einstellungen für den USB-Ethernet-Support erfolgen in LANconfig unter **IoT** > **USB**.

Betrieb

Schalten Sie den USB-Ethernet-Support hier ein.

VLAN-ID

Optionale Angabe einer VLAN-ID.

3.1 Ergänzungen im Setup-Menü

3.1.1 USB

Konfigurieren Sie hier die Einstellungen für den USB-Ethernet-Support.

SNMP-ID:

2.111.1

Pfad Konsole:

Setup > **IoT**

CDC-EEM-Support

Konfigurieren Sie hier die Einstellungen des Protokolls CDC-EEM für den USB-Ethernet-Support.

SNMP-ID:

2.111.1.1

Pfad Konsole:

Setup > **IoT** > **USB**

Operating

Schalten Sie den USB-Ethernet-Support hier ein oder aus.

SNMP-ID:

2.111.1.1.1

Pfad Konsole:

Setup > **IoT** > **USB** > **CDC-EEM-Support**

Mögliche Werte:

No

USB-Ethernet-Support ausgeschaltet.

Yes

USB-Ethernet-Support eingeschaltet.

Default-Wert:

No

VLAN-ID

Optionale Angabe einer VLAN-ID.

SNMP-ID:

2.111.1.1.2

Pfad Konsole:

Setup > **IoT** > **USB** > **CDC-EEM-Support**

Mögliche Werte:

0 … 4095