

Spectralink VIEW Certified Configuration Guide

LANCOM Systems

LANCOM LN-170xB, LN-830U, LN-86xacn

Copyright Notice

© 2019 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Contact Information

US Location

+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location

+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location

+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com

Contents

Chapter 1: Introduction	4
Certified Product Summary.....	4
Known Limitations.....	5
Spectralink References	5
Support Documents.....	6
White Papers.....	7
Product Support	7
Chapter 2: Network Topology.....	8
Chapter 3: LANCOM Configuration	9
Configuring a New Access Point (AP) Starting from Factory Defaults	9
First Connection to the AP after the Setup Wizard.....	19
Installing Firmware	20
Chapter 4: Configure General Settings	24
Configure Wireless LAN General Settings.....	24
Configure IGMP for PTT	25
Configure Date & Time	27
Configure Event Logging	29
Chapter 5: LAN Settings	31
Configure Radio Settings (Physical WLAN settings)	31
Configure SSID Settings (Logical WLAN settings).....	35
Configure general SSID settings	35
Configure security settings	37

Chapter 1: Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Spectralink Wireless Telephones and wireless LAN (WLAN) infrastructure products.

Certified Product Summary

Manufacturer:	LANCOM Systems		
Certified products:	Standalone	AP models: LN-170xB, LN-830U, LN-86xacn	
AP Radio(s):	Radio1 (Dual 802.11n radio) 2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n) Radio 2 (802.11ac radio) 5 GHz (802.11ac)		
Security:	None, WPA2-PSK, WPA2-Enterprise (TLS and PEAPv0/MSCHAPv2) with OKC and FT (802.11r) roaming. Please see Known Limitations section below for specific information.		
QoS:	Wi-Fi Standard for Versity models, 84-series models		
Network topology:	Bridged at AP		
AP and WLC software versions approved:	LANCOM 10.32.0021		

<i>Handset* models tested:</i>	<i>Spectralink Versity 95-Series and 96-Series ***</i>			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a & 802.11an & 802.11ac
Meets VIEW minimum call capacity per AP**:	10	10	10	12

<i>Handset models tested:</i>	<i>Spectralink 84-Series</i>			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a
Meets VIEW minimum call capacity per AP:	8	8	8	10

*Spectralink handset and smartphone models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “phones” or “handsets”. Versity smartphones may be referred to as “smartphones”.

**Maximum calls tested per the VIEW Certification Test Plan. The certified product may support a higher number of maximum calls

***Higher maximum calls are for networks with Versity smartphones by themselves. When both 84-Series and Versity smartphones were include, the lower number passed.

Known Limitations

- Using the LN-1700B, the 84-series phones could not perform an OKC roam on the 802.11ac radio. It was successful with the 802.11bgn/an radio. Recommended workaround: use WPA2-PSK with the 84-series phones.
- Using the LN-830U or the LN-86xacn APs, the 84-series phones could not perform an OKC roam on the 802.11bgn/an radio. It was successful with the 802.11ac radio. Recommended workaround: use WPA2-PSK with the 84-series phones.
- The 802.11bgn/an radios in all products did not pass multicast in a manner to support the Spectralink PTT feature. The feature did work correctly on the 802.11ac radios in all products.
- The TSPEC/WMM_AC function is not supported in LANCOM products, nor is it planned to ever be supported. There are no plans to support this function in the Spectralink Versity models.
- 84-series handsets must be operated in an 802.11n disabled mode for best network resource usage.
- 84-series handsets do not support 802.11r (Fast) roaming. They do support OKC roaming.
- Versity handset versions 1.6 and below have an issue with 802.11r (Fast) roaming. The 1.6 version has a workaround to prefer PMK/OKC roaming if available. When the issue is fixed (currently scheduled for the 1.7 release) the phone will prefer to roam with FT. The easiest configuration solution is to advertise all types of roaming in the SSID's.

Spectralink References

All Spectralink support documents are available at <http://support.spectralink.com>.

To go to a specific product page:

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

Support Documents

Spectralink Versity Deployment Guide provides a high-level overview of the deployment process for Spectralink Versity smartphones. This includes the interface with an EMM, the method for getting Versity connected to the wireless LAN, and the interface with the Spectralink Application Management (SAM) server.

Spectralink 84-Series Wireless Telephone Administration Guide provides a comprehensive list of every parameter available on Spectralink 84-Series Wireless Telephones.

The *Spectralink 84-Series Deployment Guide* is your essential reference for provisioning and deploying Spectralink 84-Series handsets in any environment.

The *Web Configuration Utility User Guide* explains how to use a web browser to configure the Spectralink 84-Series handsets on a per handset basis.

White Papers

Spectralink White Papers are available at <http://www.spectralink.com/resources/white-papers>.

For the Spectralink 84-Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 84-Series Handsets* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

For additional details on RF deployment please see *The challenges of ensuring excellent voice quality in a Wi-Fi workplace* and *Deploying Enterprise-Grade Wi-Fi Telephony*.

These White Papers identify issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

Product Support

LANCOM Support Portal:

<https://www.lancom-systems.com/service-support/support-warranty/support-contact/>

Support for End customers and NON-LANCOM Partners:

Support for End customers

LANCOM Support Portal

For submission and processing of written support requests, we provide you with our support portal.

[Open Support Portal](#)

Important:

- > Please note that we **give preference to support requests from our partners**. For this reason, we point out that there may be longer waiting times when processing your request.
- > With the **chargeable LANCOM Emergency Support**, you can alternatively get short-term and solution-oriented access to the LANCOM support with a **maximum response time of 30 minutes**. All required information is available on the [product website](#).

Support for LANCOM Partners:

Support for LANCOM partners

LANCOM partners receive a phone number with preferred support according to their partner status.

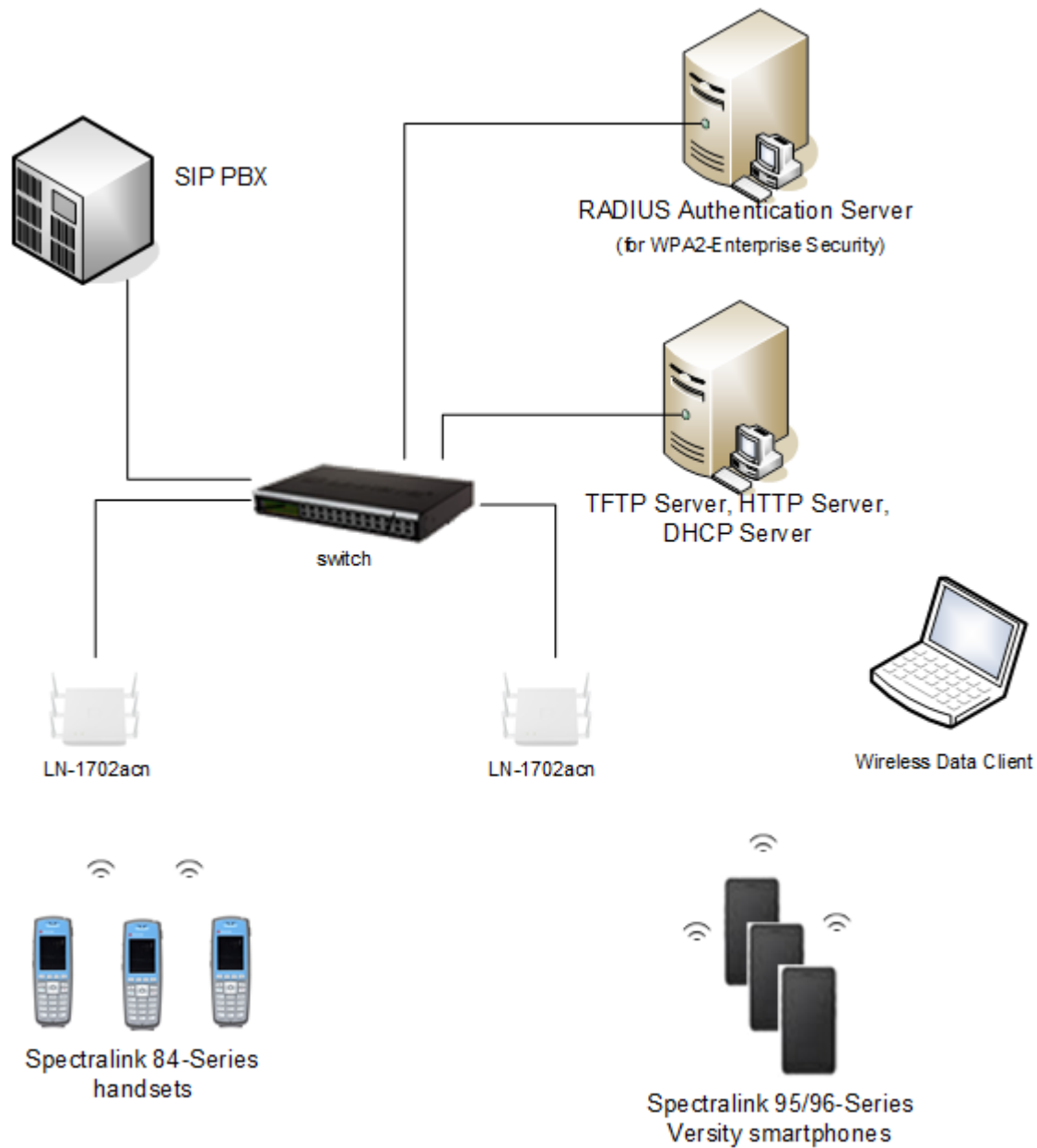
Important:

- > E-mail support for LANCOM partners remains available from the usual contact addresses – now in an improved format. A portal solution for LANCOM partners is currently under development.

LANCOM Knowledge Base (Configuration Guidance):

<https://www.lancom-systems.com/service-support/instant-help/knowledge-base/>

Chapter 2: Network Topology



Note: Example configuration shown

This is a modified diagram and not all components are shown for every system type.

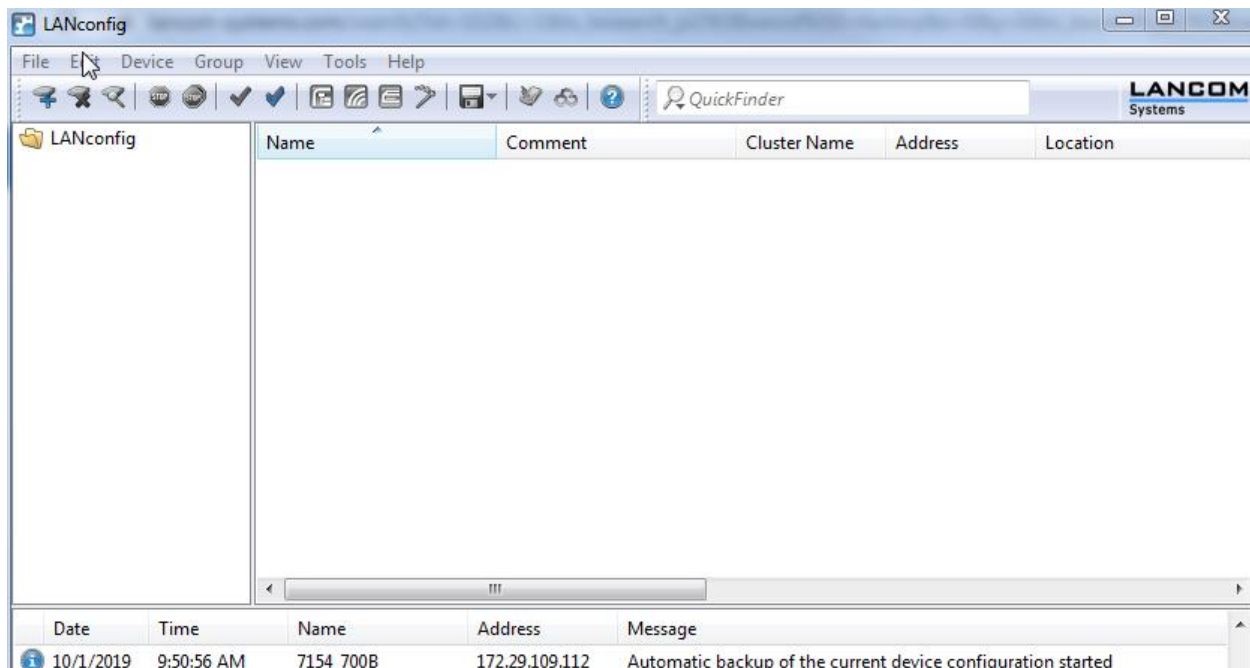
Chapter 3: LANCOM Configuration

This document will focus on those places where the configuration needed to support Spectralink wireless handsets differs from the factory default configuration

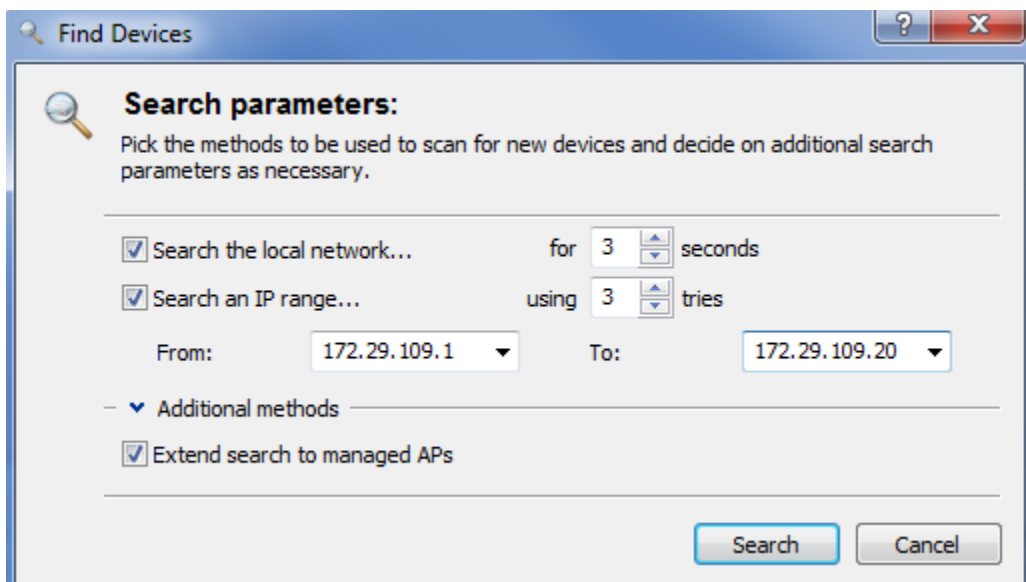
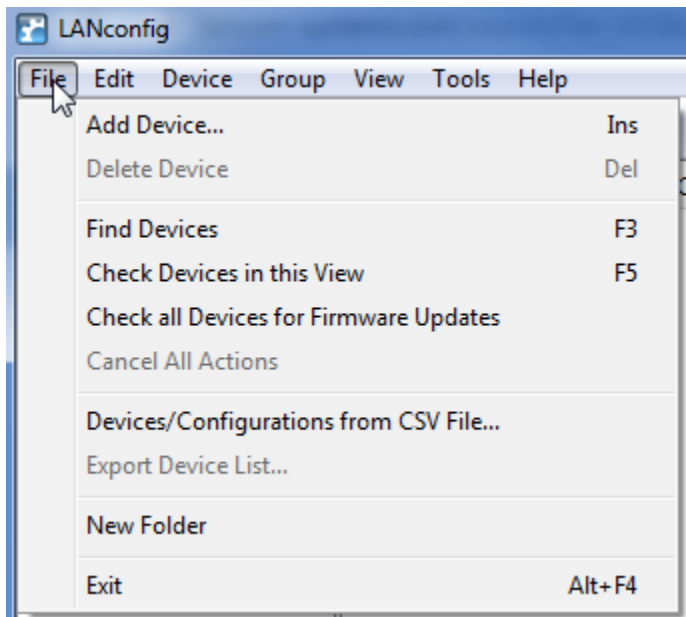
There are several ways to configure LANCOM System APs including WEBConfig, LANConfig, controller-based, and from the cloud. The VIEW testing was performed using LANConfig, with WEBConfig used where necessary. These directions are described below. Another method may be used if the same settings are achieved.

Configuring a New Access Point (AP) Starting from Factory Defaults

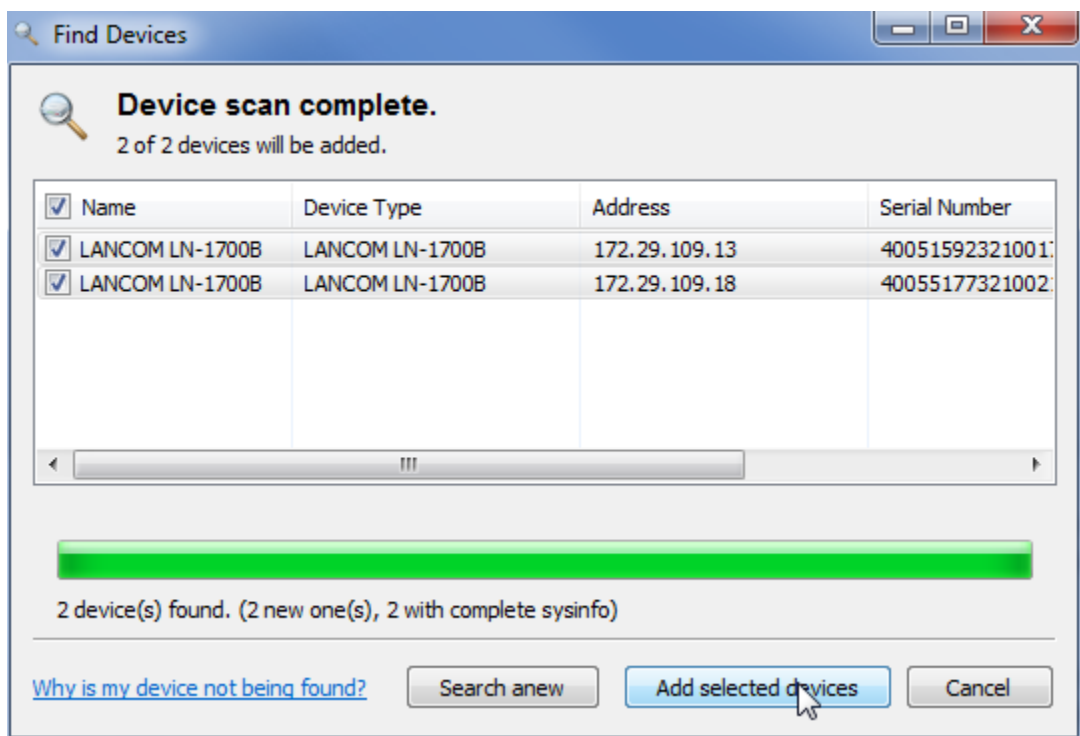
- 1 Download the LANconfig tool to a Windows PC or laptop from <https://www.lancom-systems.com/downloads/>
- 2 From a factory default state (press and hold the reset button for 5 seconds if needed), attach the AP to a network with a DHCP server.
- 3 Start the LANconfig tool on the PC.



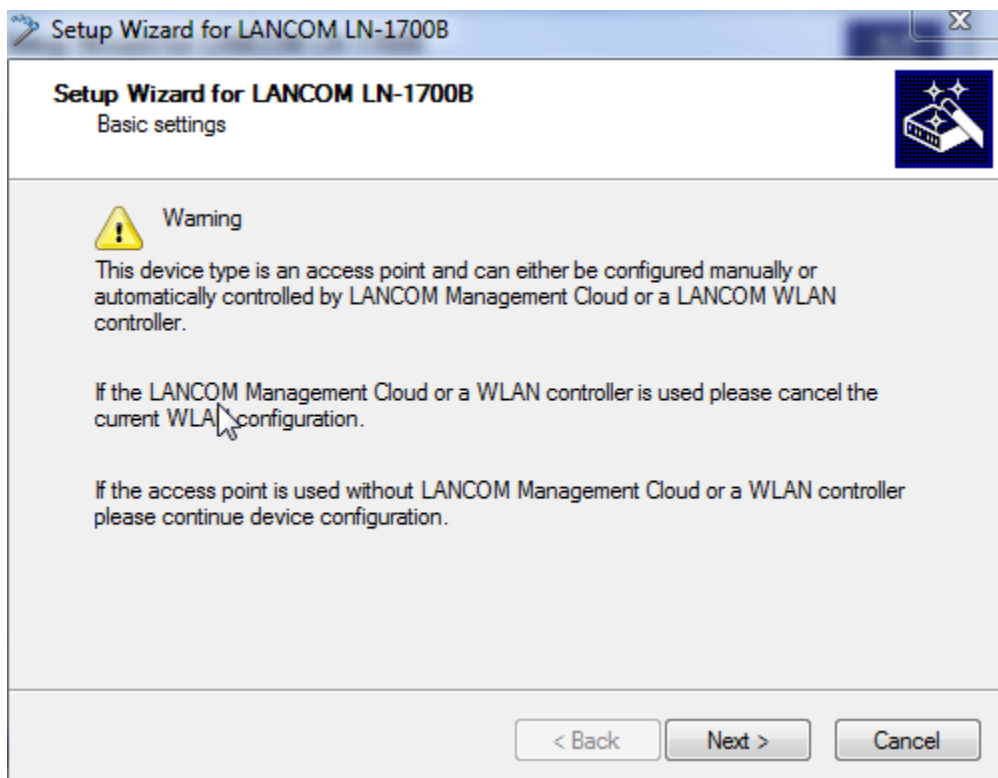
- 4 From the LANconfig main screen, choose **File>Find Devices**.
- 5 Enter an address range that matches the DHCP scope of the attached network.



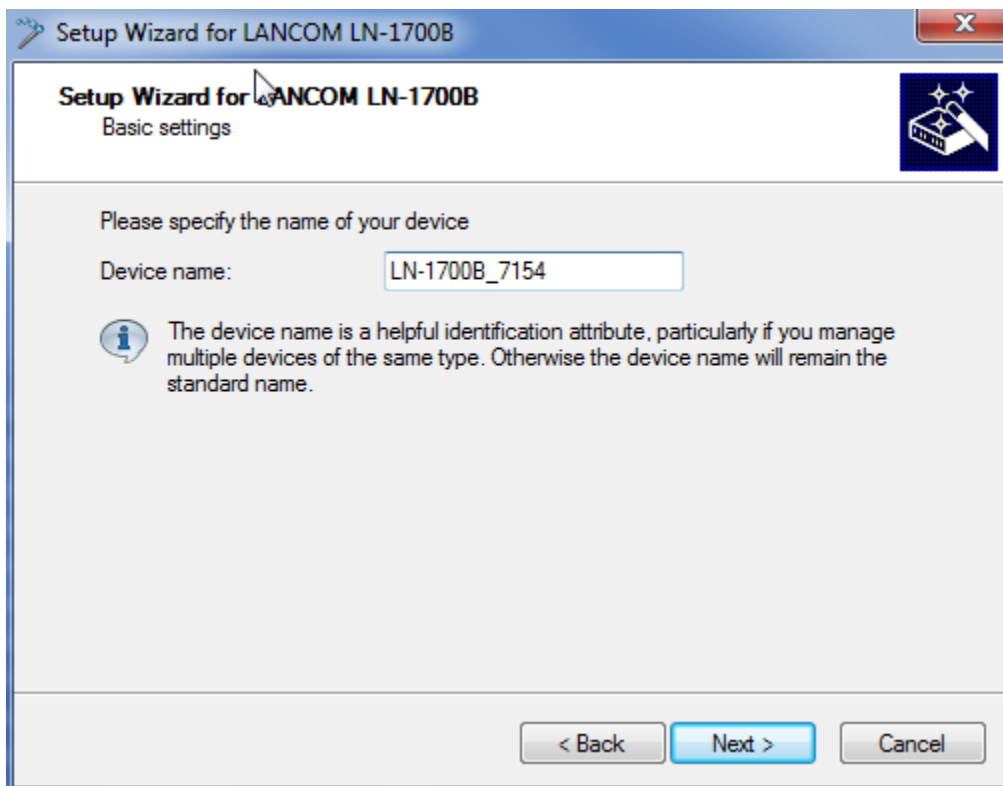
6 Click on **Add selected devices**.



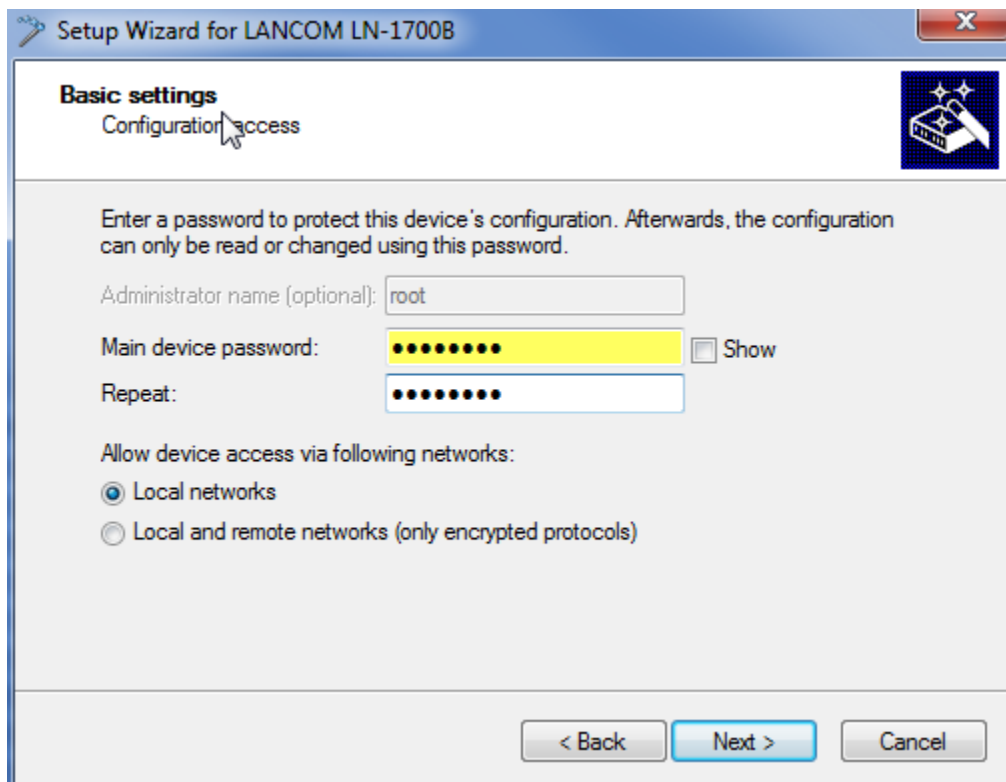
7 For each device, run the **Setup Wizard**. Start by clicking on **Next**.



- 8 Enter a name for each device.

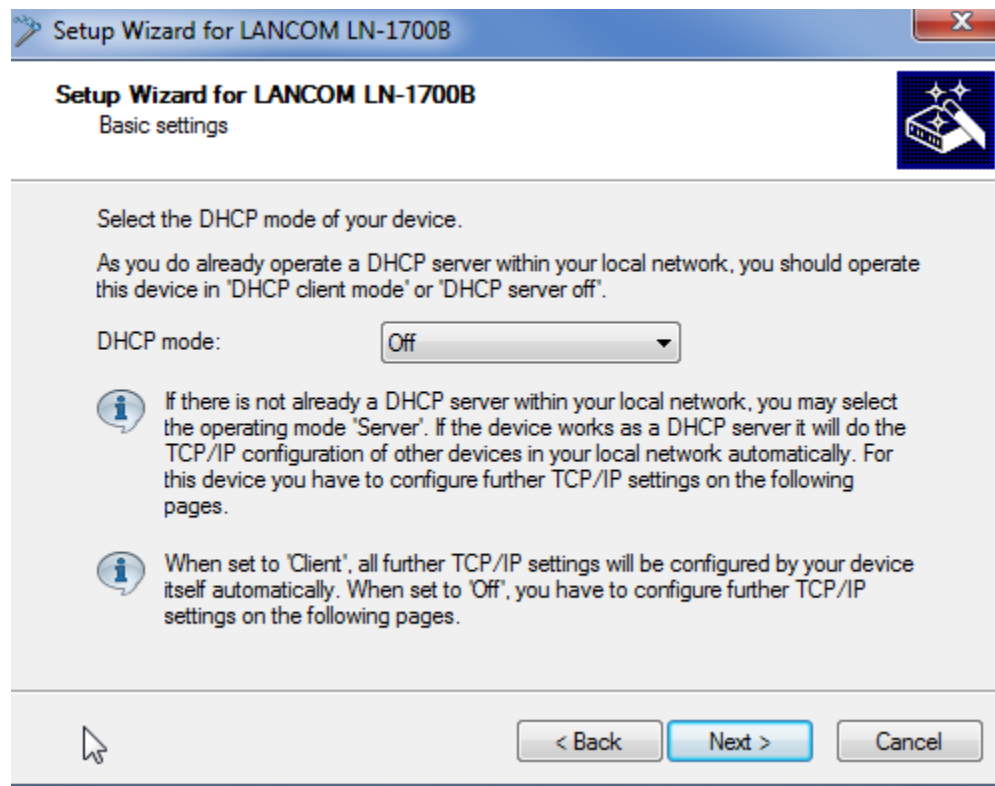


- 9 Give each device a root access password. Please remember the password, as the only way to recover it is to restore the device to factory defaults.

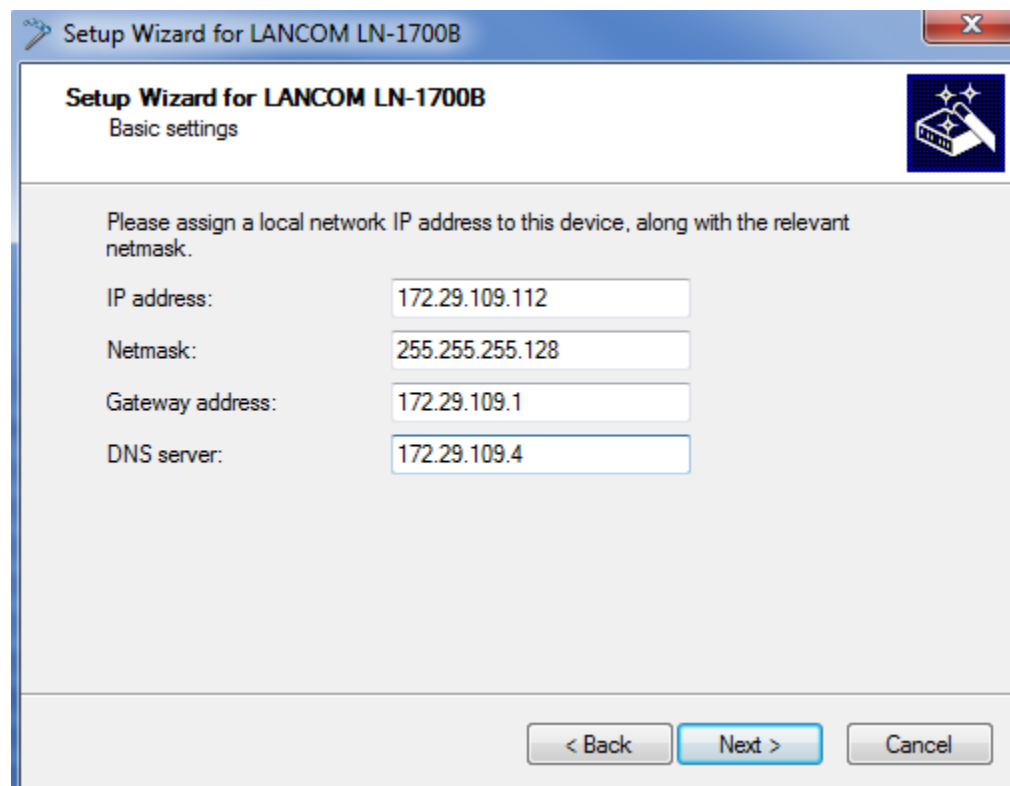


10 Select the DHCP mode of the AP.

- **Off** – if the AP has a static address
- **Client** – if the AP obtains its address for the network infrastructure
- **Server** - if the AP is to act as a server for the network. Be careful of this choice: the network should have only one DHCP server.



This example shows a static entry with a **Netmask**, **Gateway address**, and **DNS server**.

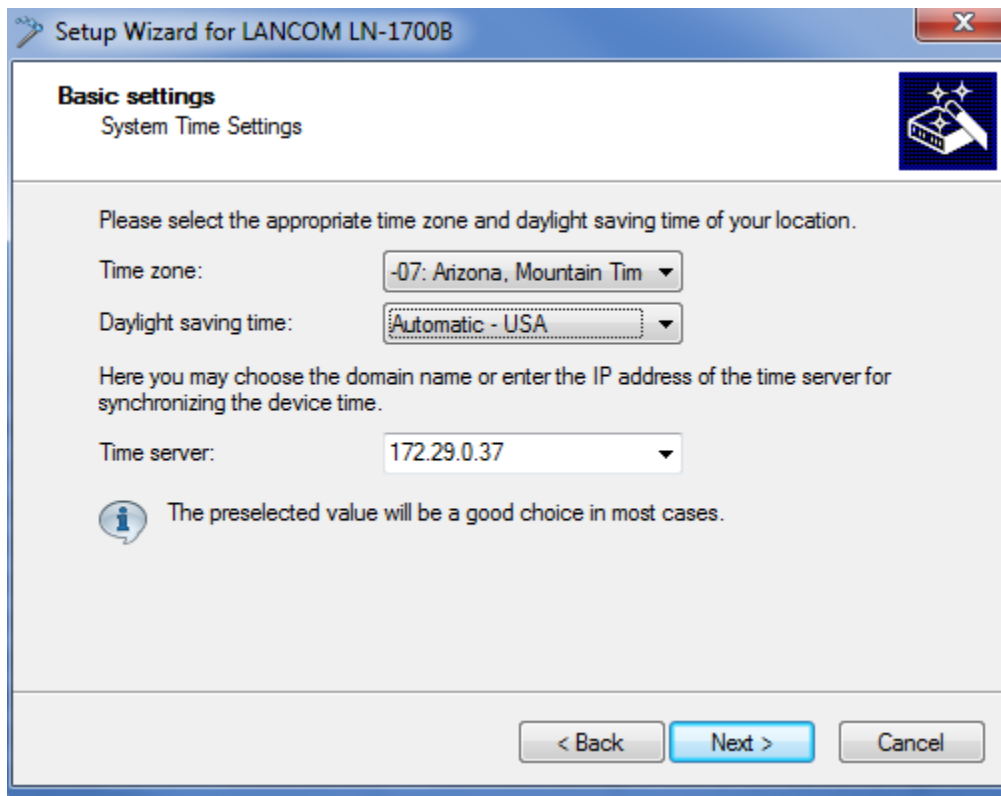


11 Enter the **Time zone**, **Daylight saving time**, and **Time server** (NTP server).

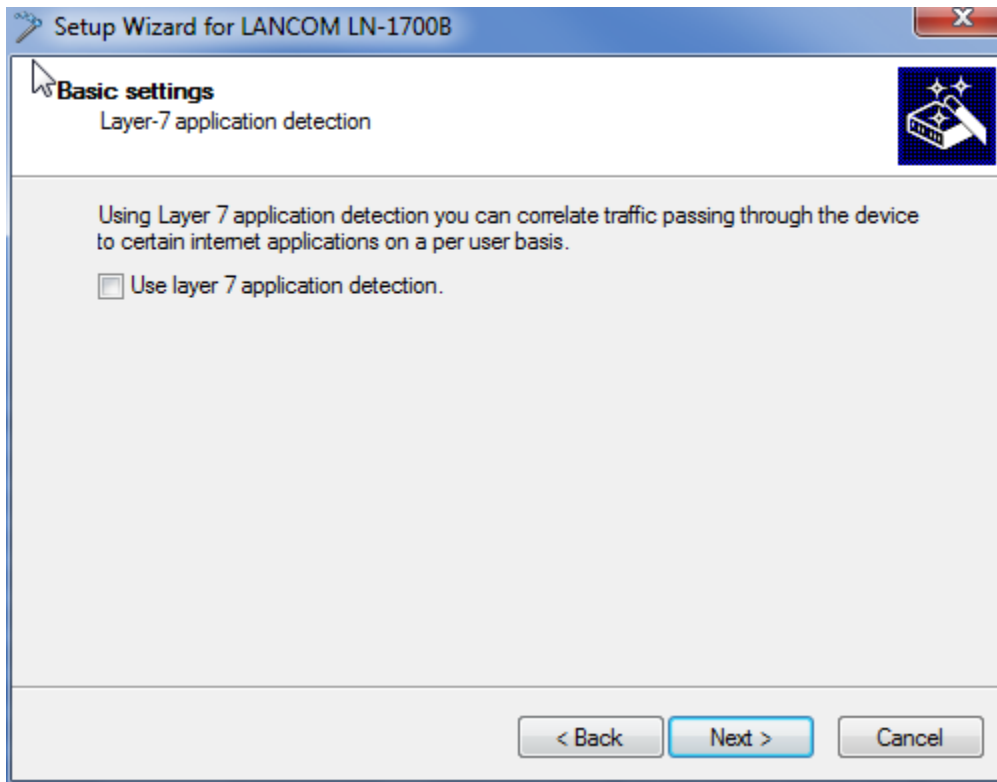


Note: 84-Series handsets require a time server for Enterprise security.

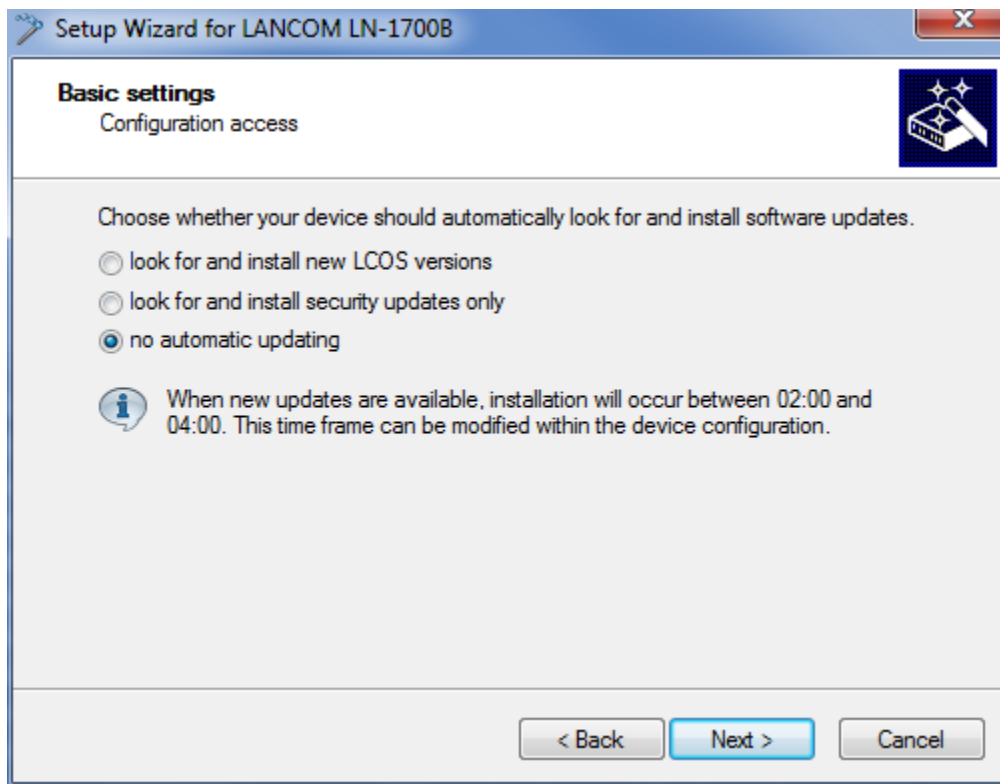
If the AP is not acting as a DHCP server, the 84-series will receive the time server from the DHCP server on the infrastructure if the DHCP option is given or from other provisioning methods.



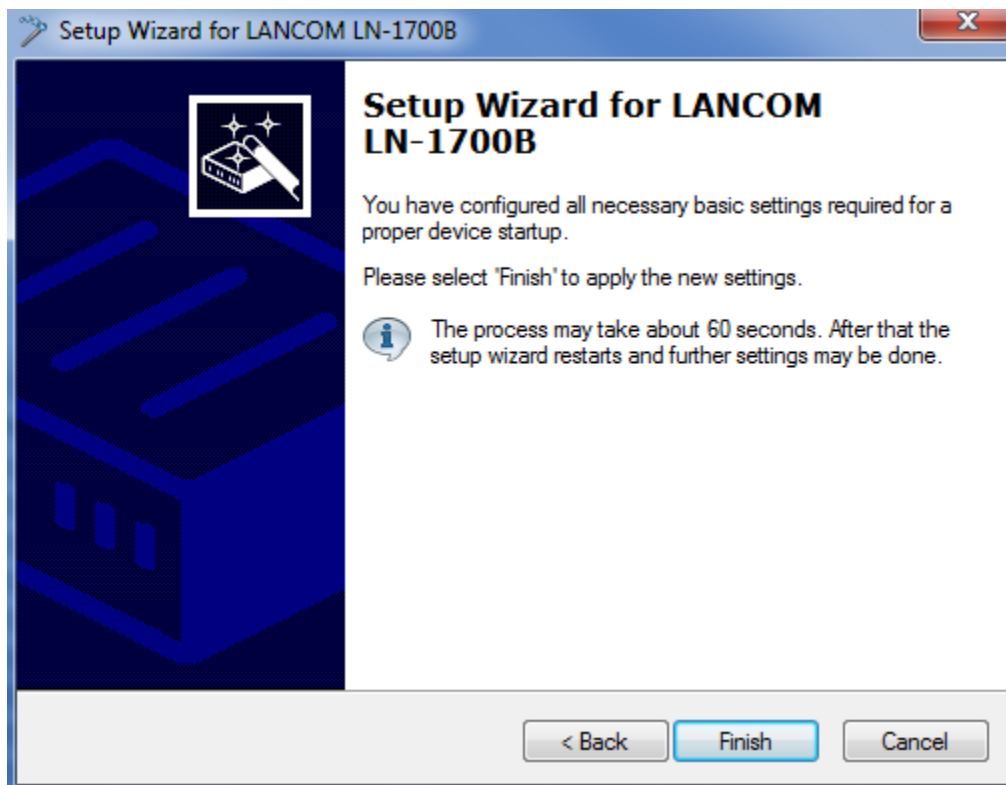
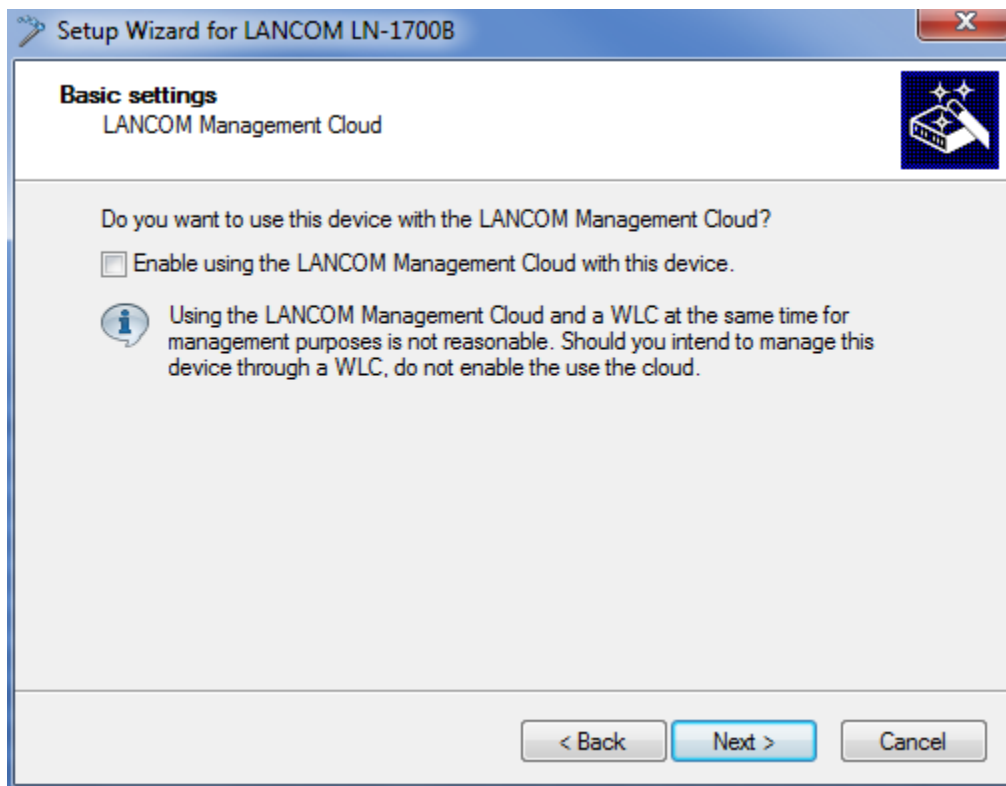
12 Application detection analyzes the inbound and outbound connections at each tracked interface, and it stores the statistics of the specified applications. See the Reference manual on the LANCOM support site for more information.



- 13 Choose the method for updating AP firmware. Note that this method obtains the updates from the LANCOM support site.

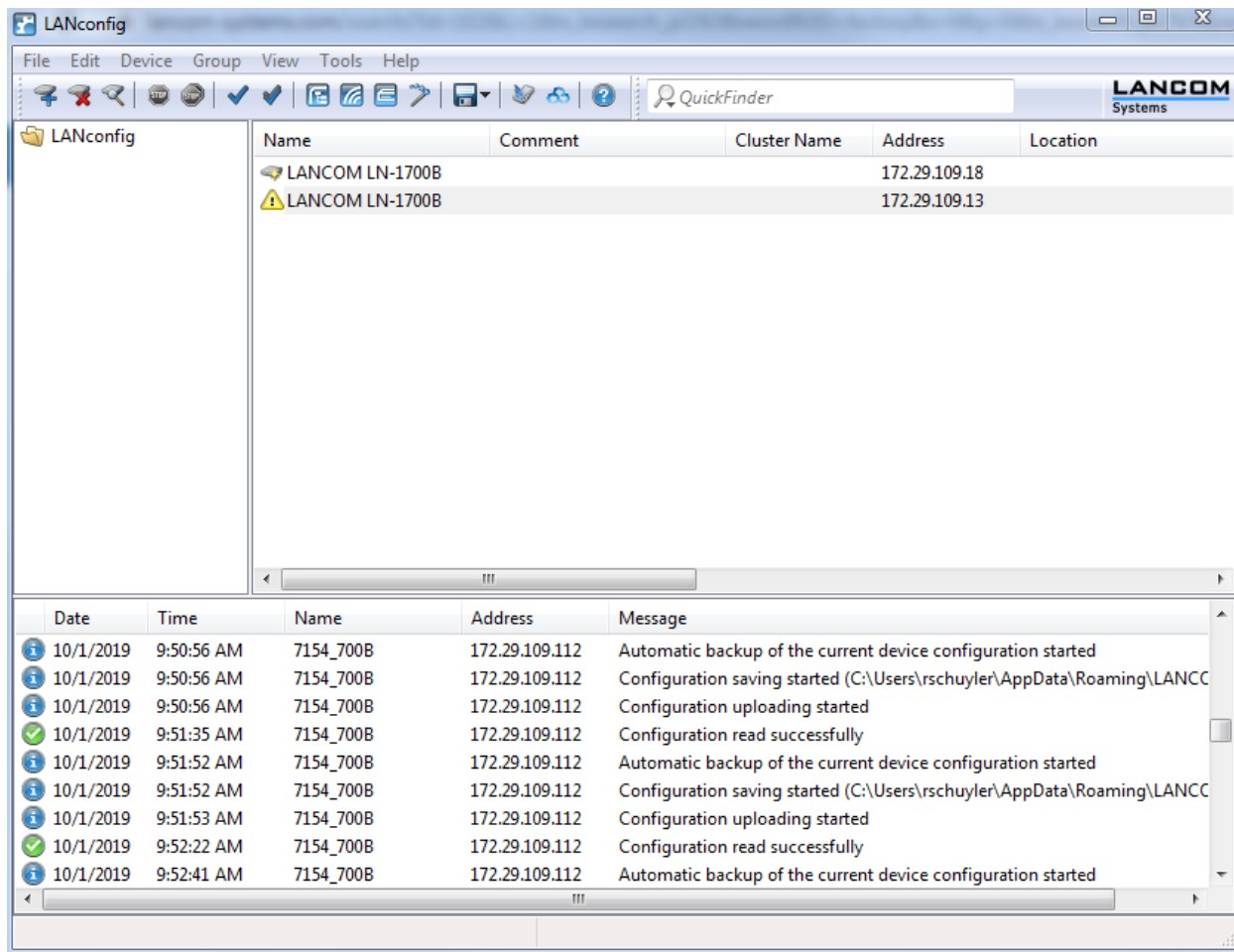


- 14 Choose cloud management if desired. A network of standalone APs was used for VIEW testing.

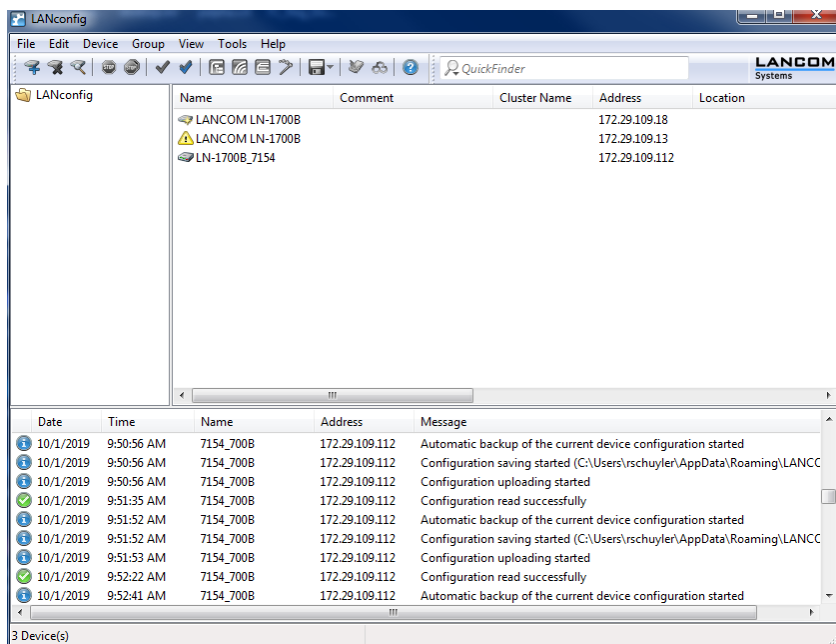
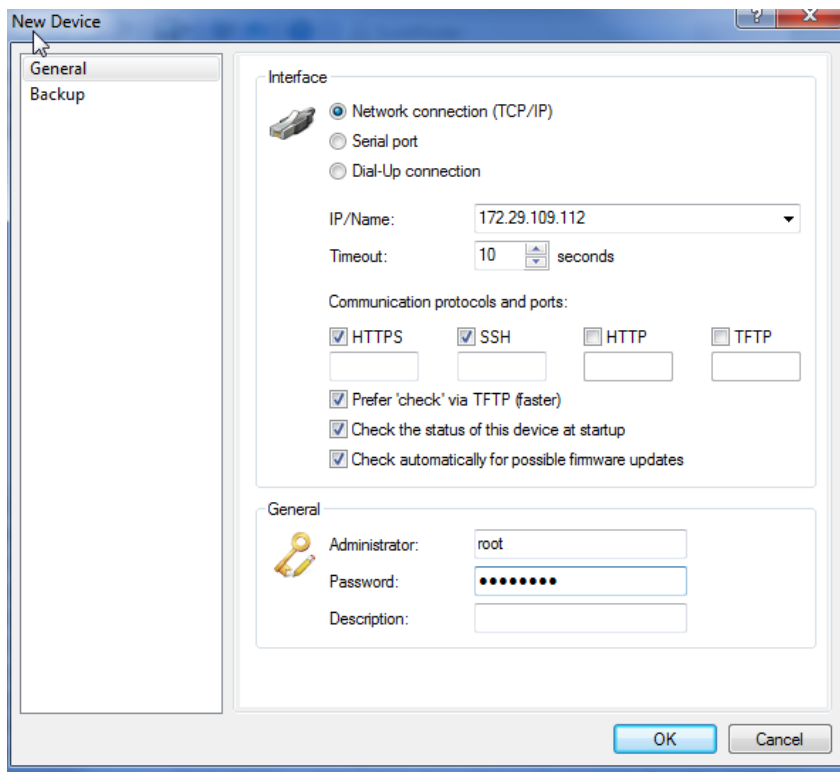


First Connection to the AP after the Setup Wizard

- 1 Open the LANconfig program on a Windows PC or laptop.



- 2 Enter the **IP/name** of the AP (in this example, a static address was entered in the wizard), **root** for the **Administrator**, and the password entered in the wizard for the **Password** field. The AP will appear in the list as shown in the second screenshot.

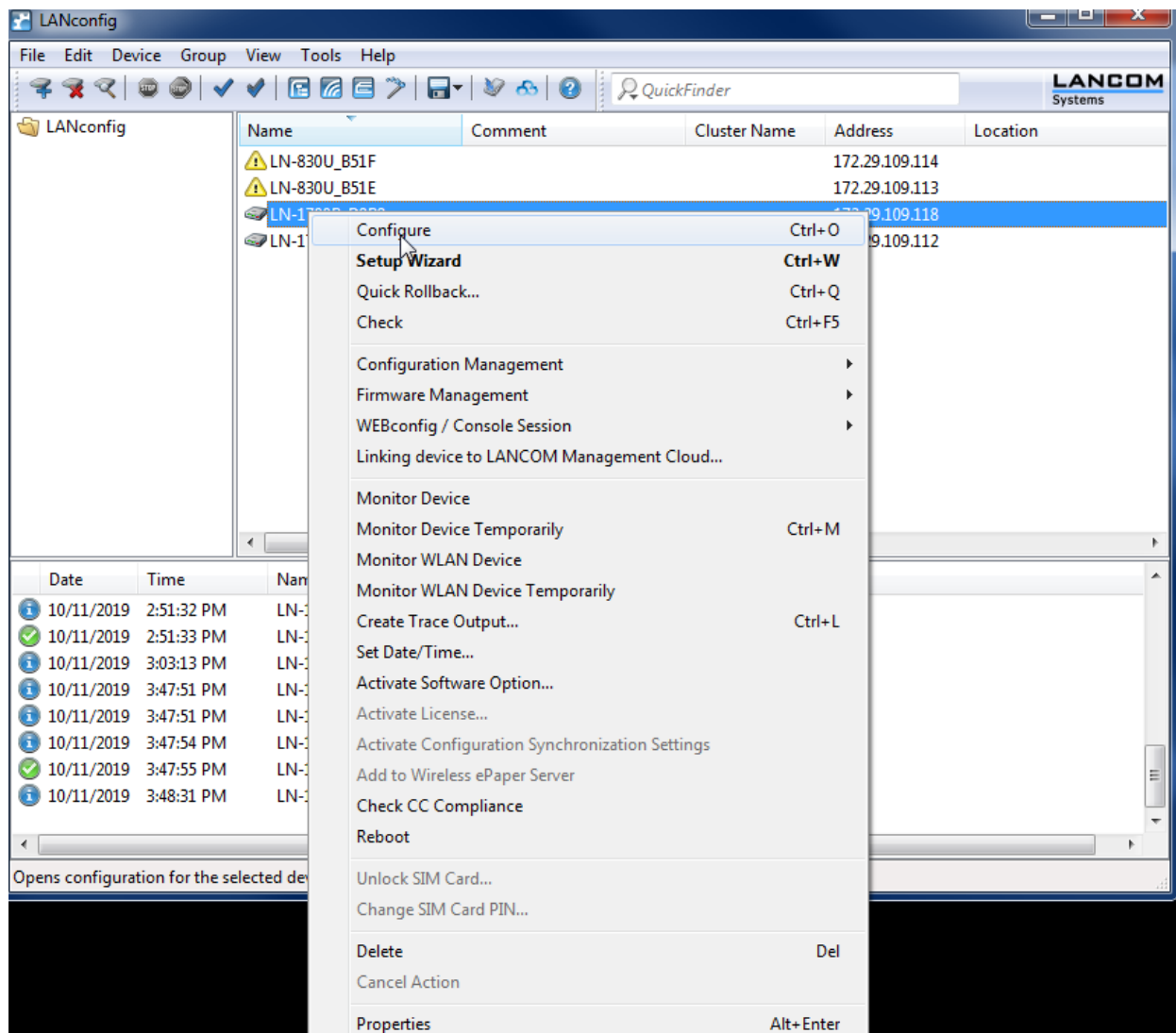


Installing Firmware

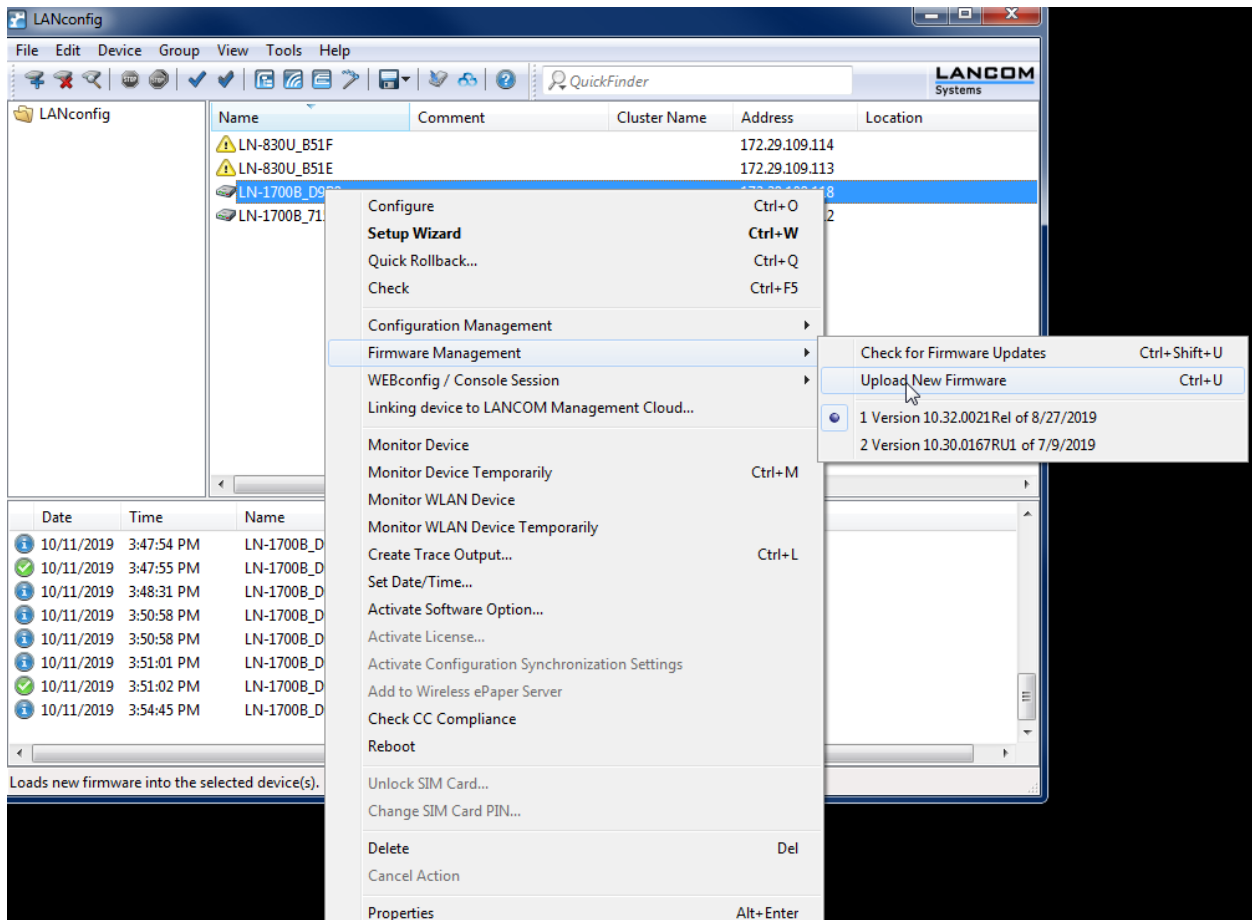
As shown in the setup wizard above, the firmware can be set to automatically update.

To update firmware by choice, perform the following steps:

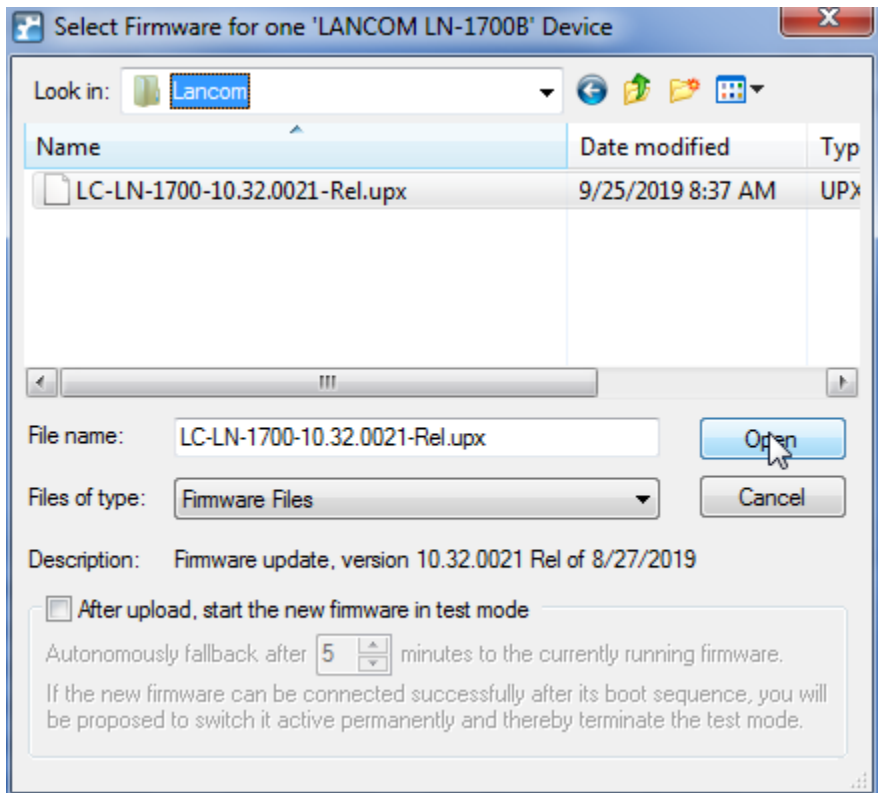
- 1 Open LANconfig.
- 2 Highlight the desired AP.
- 3 Right click.
- 4 Click on **Configure** from the dropdown menu.



- 5 Click on **Firmware Management>Upload New Firmware**.



- 6 Browse to the location of the desired firmware and click on **Open**. The firmware will be installed.

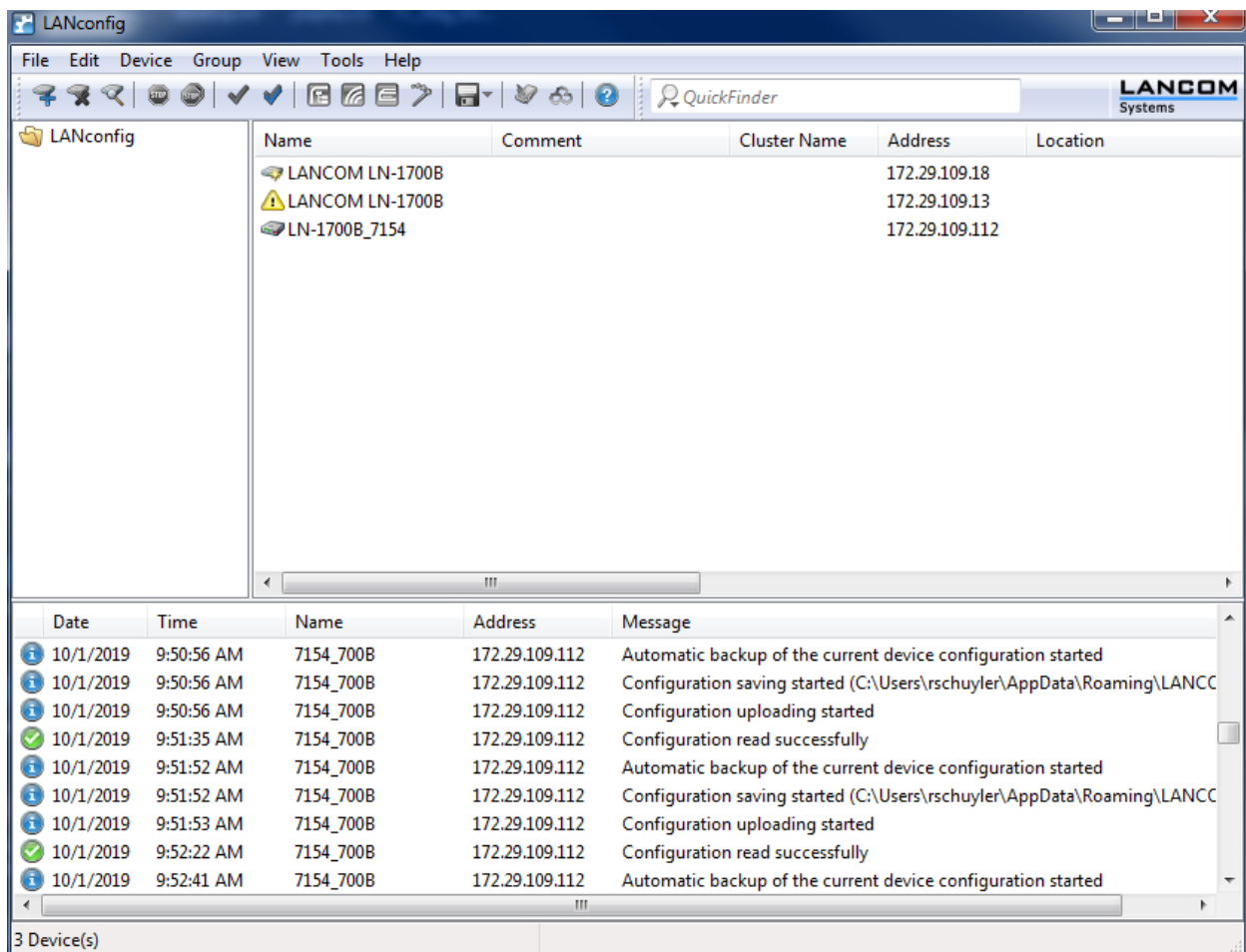


Chapter 4: Configure General Settings

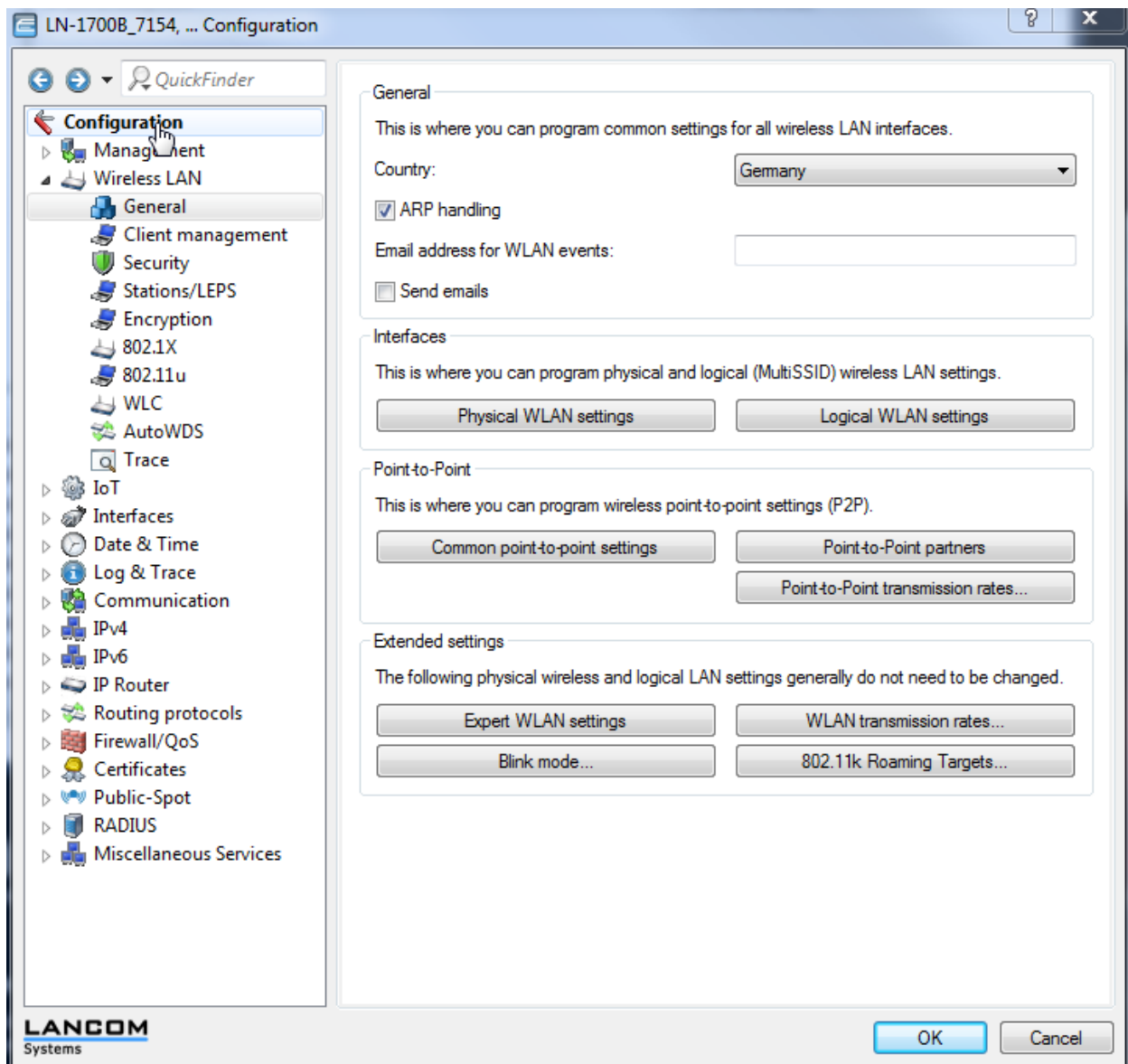
This section configures general settings for ARP, country, IGMP snooping (for Spectralink's PTT feature), the time source, and event logging (if desired).

Configure Wireless LAN General Settings

- 1 Open LANconfig on a Windows PC or laptop, highlight the desired AP name, and right click on **Configure** to reach the configuration for the desired AP.

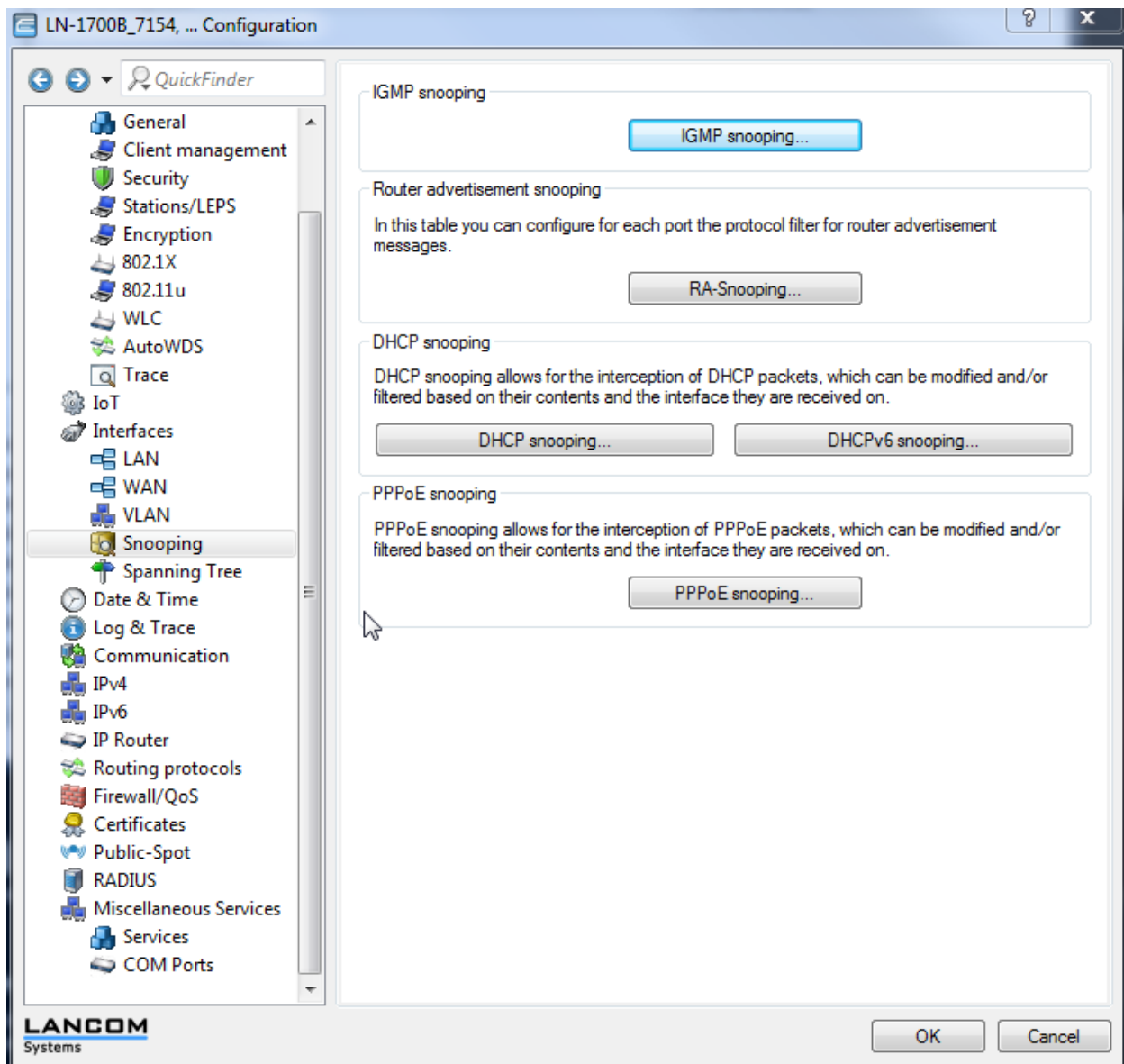


- 2 Navigate to **Configuration>Wireless LAN>General**.
- 3 Ensure **ARP handling** is checked.
- 4 Ensure the proper **Country** is selected. The channels available on a certain radio/country setting combination are described in the data sheets on the LANCOM support site.

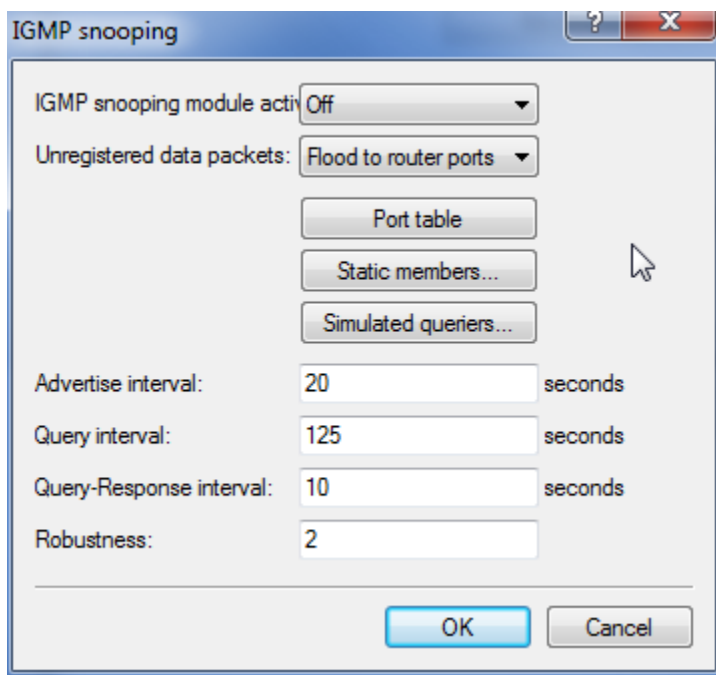


Configure IGMP for PTT

- 1 Open LANConfig, highlight an AP, and right click on **Configure** as before to begin the configuration process.
- 2 Navigate to **Interface>Snooping**.

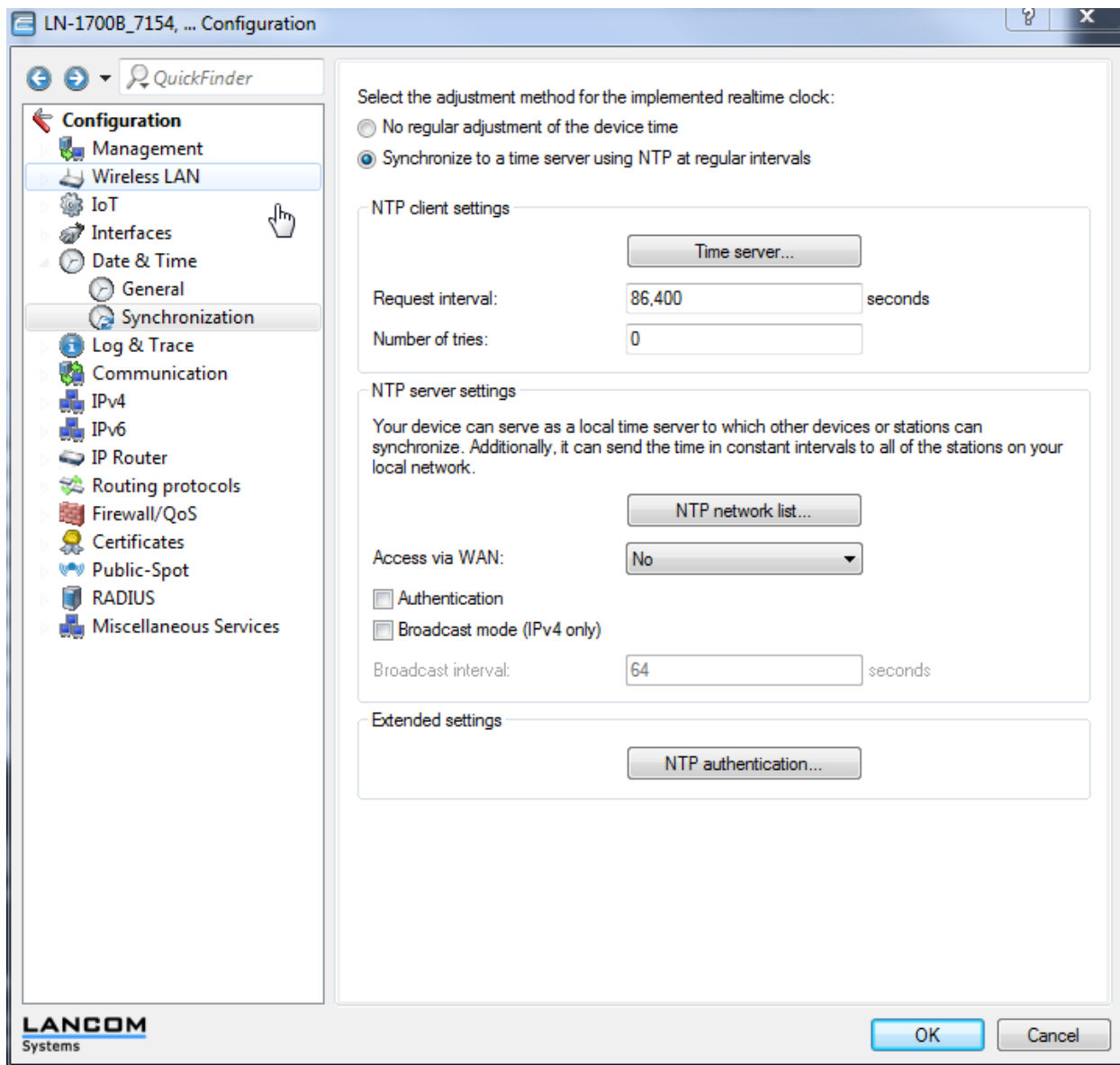


- 3 Turn **IGMP snooping module active** to **Off** for PTT multicast transmission. This will keep the data stream from experiencing a timeout and stopping the stream if it is idle.

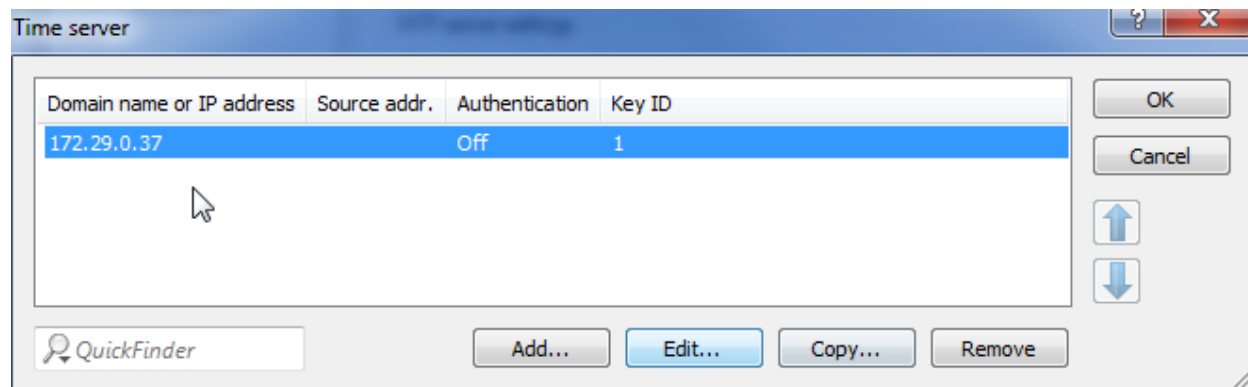


Configure Date & Time

- 1 Open LANConfig, highlight an AP, and right click on **Configure** as before to begin the configuration process.
- 2 Navigate to **Configuration>Data & Time > Synchronization**.

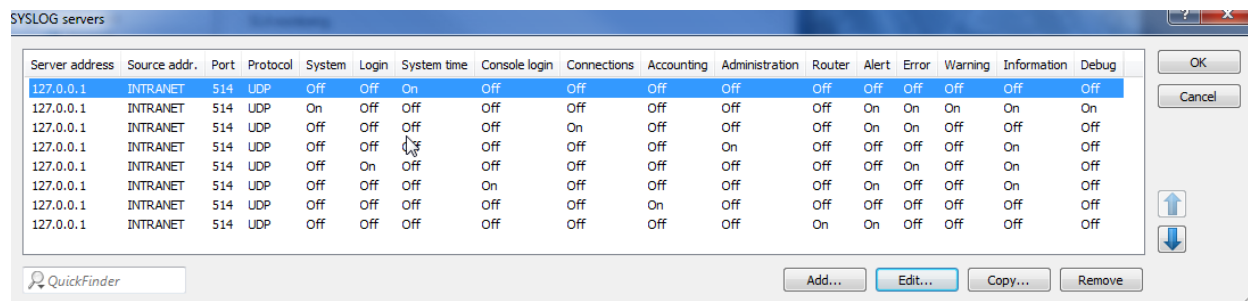


- 3 Click on **Time server** and enter the NTP address. Note: this is unnecessary if the step was performed while running the wizard when first connecting to the AP.



Configure Event Logging

- 1 Open LANConfig, highlight an AP, and right click on **Configure** as before to begin the configuration process.
- 2 Navigate to **Configuration>Log & Trace>General**.
- 3 Click on **SYSLOG servers** and enter a server if desired for system logging.



- 4 Click on **Edit**.
- 5 Enter the **Server address**.
- 6 Check the desired Priority for the types of messages saved in the log.

SYSLOG servers - Edit Entry

Server address: 172.29.109.109

Source address (opt.): INTRANET

Port: 514

Protocol: UDP

Source

<input type="checkbox"/> System	<input type="checkbox"/> Login
<input checked="" type="checkbox"/> System time	<input type="checkbox"/> Console login
<input type="checkbox"/> Connections	<input type="checkbox"/> Accounting
<input type="checkbox"/> Administrative	<input type="checkbox"/> Router

Priority

<input checked="" type="checkbox"/> Alert	<input checked="" type="checkbox"/> Error
<input checked="" type="checkbox"/> Warning	<input type="checkbox"/> Information
<input type="checkbox"/> Debug	

Chapter 5: LAN Settings

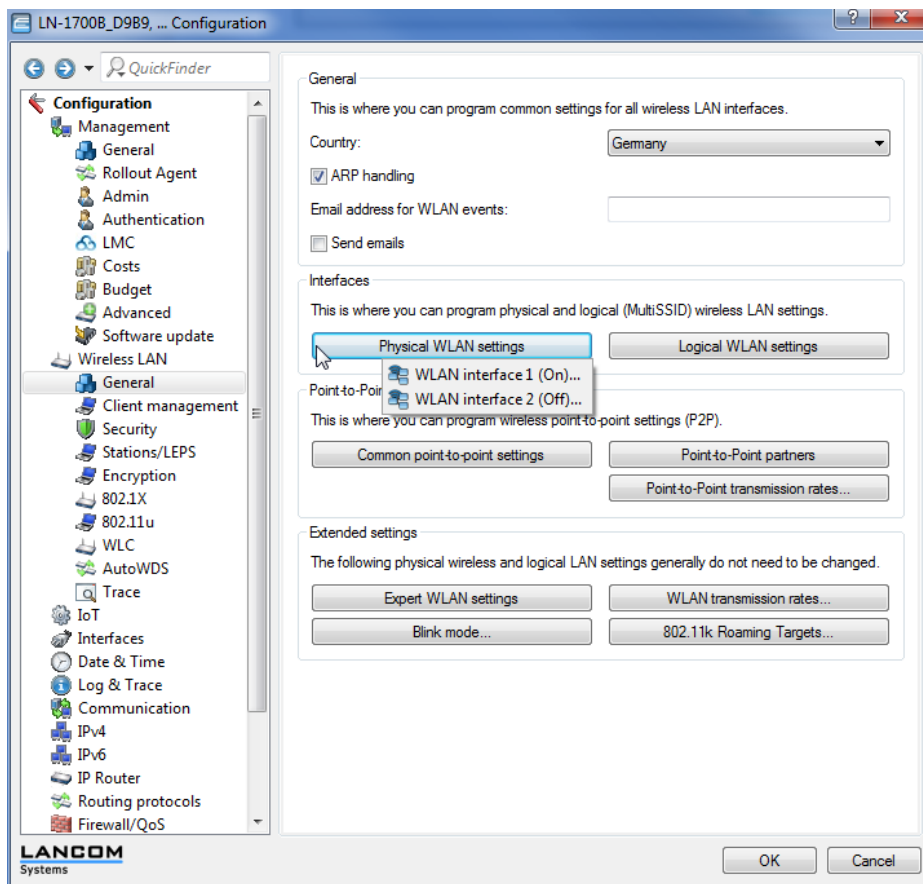
Configure Radio Settings (Physical WLAN settings)



Note: 84-Series handsets default to 802.11n disabled

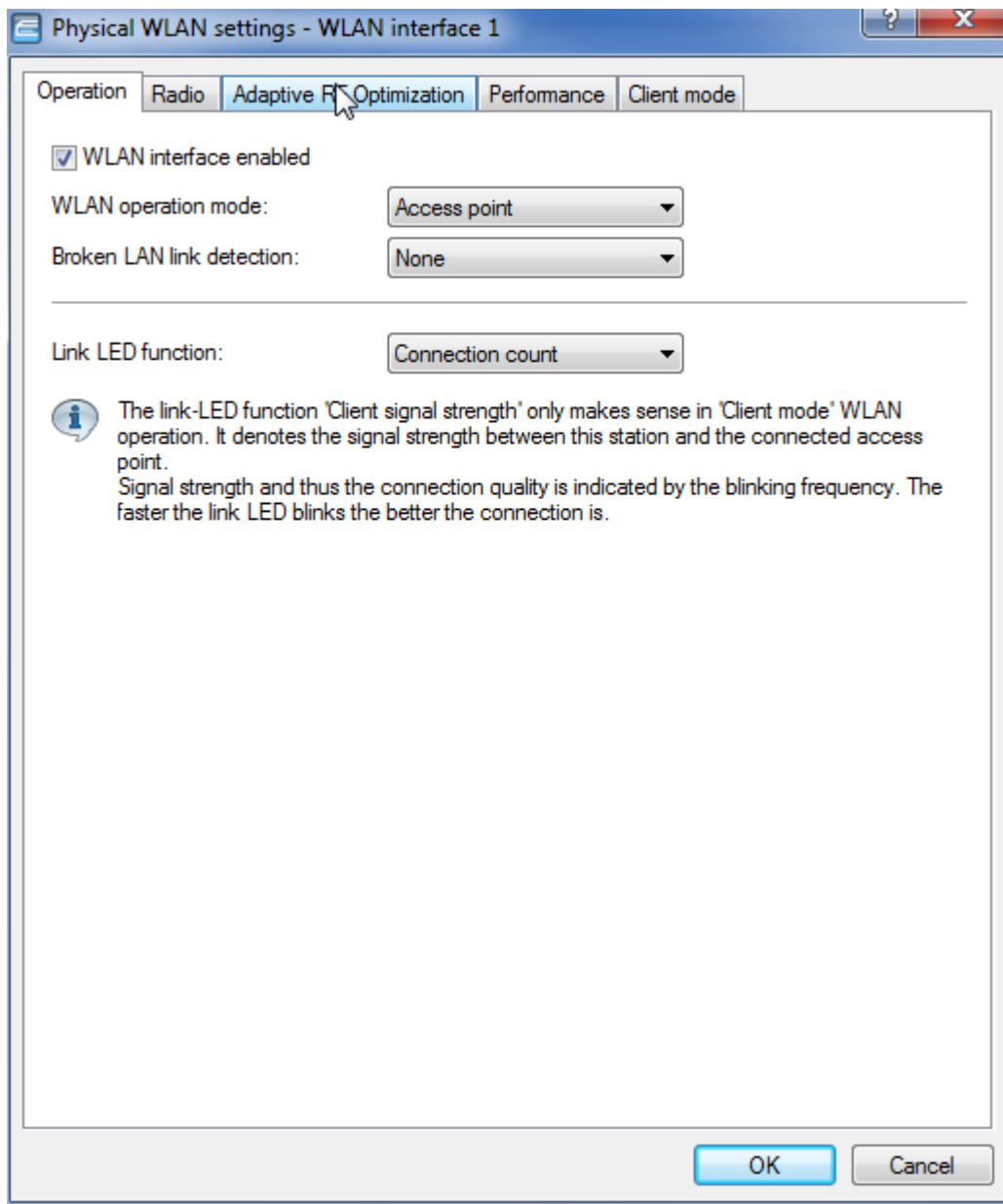
84-Series handsets manufactured with 5.3+ will default to 802.11n disabled. In other words, they will advertise as legacy a/b/g devices. They **must** have 802.11n disabled for best network interoperability.

- 1 Open LANConfig, highlight an AP, and right click on **Configure** as before to begin the configuration process.
- 2 Navigate to **Configuration>Wireless LAN>General**
- 3 Click on **Physical WLAN Settings**.



- 4 On the **Operation** tab, leave **WLAN interface enabled** for each operating radio.

5 Leave the WLAN operation mode as Access point.

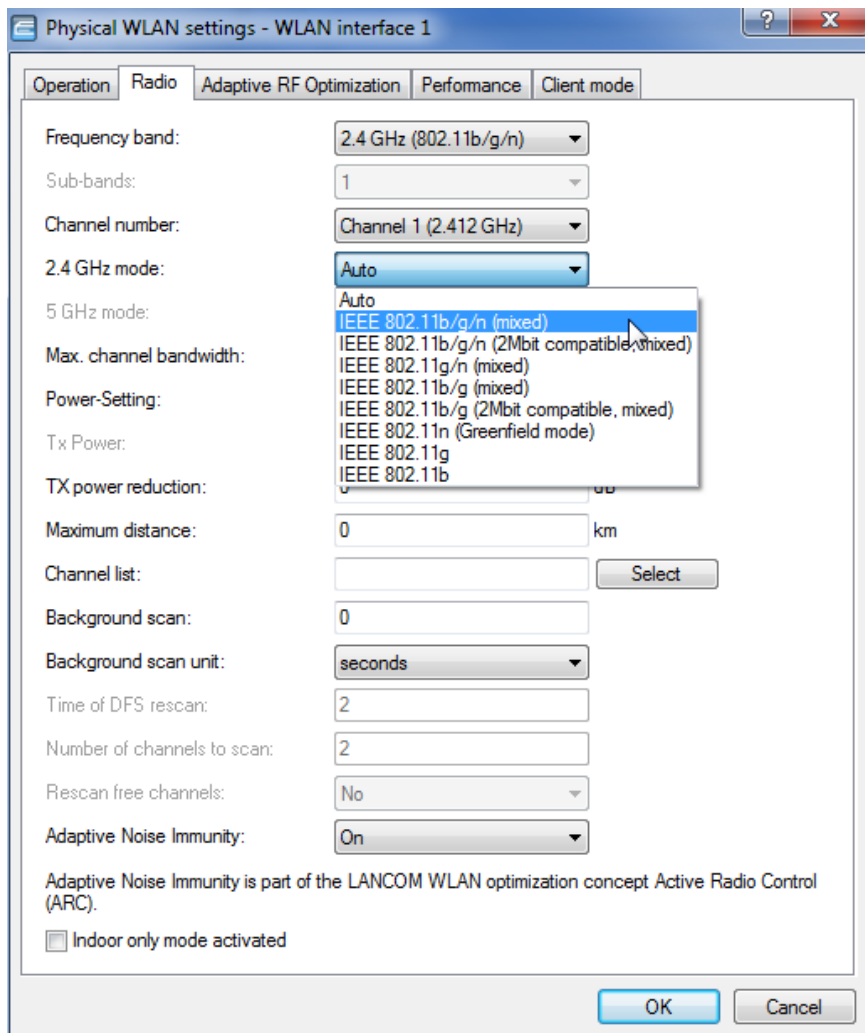


Note: 84-Series and PIVOT smartphones are not 802.11ac

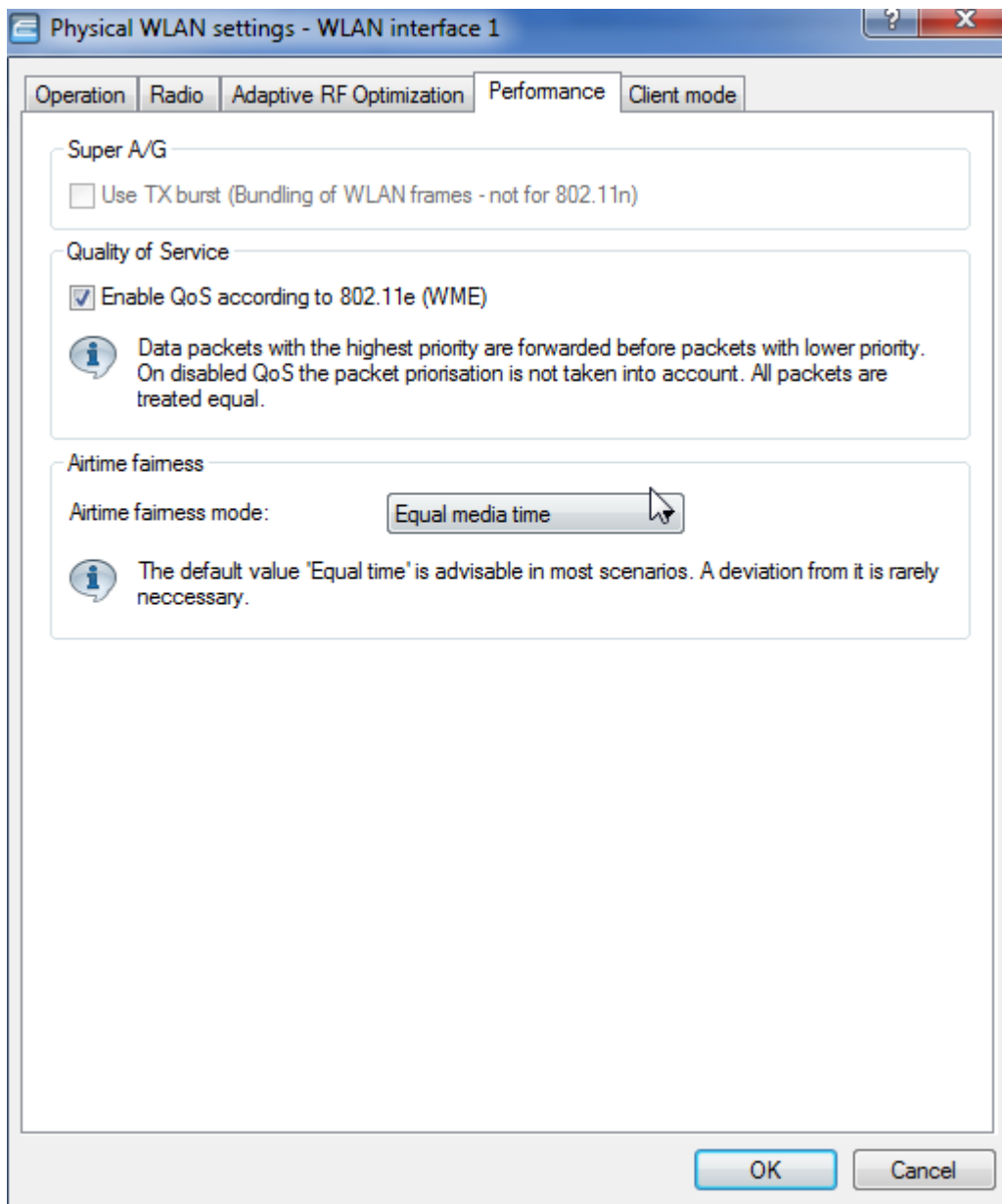
Some Spectralink phone models are not used in 802.11n and 802.11ac, so the Greenfield radio mode will not work.

- 6** Max. channel bandwidth should be set to 20 MHz.
- 7** Leave background scans at 0. Background scans are disruptive to the audio in phone calls.

- 8 Choose Indoor only mode activated if appropriate.
- 9 The channel number can be set to Auto, which lets AP algorithms choose the channel, or to a certain channel. The AP, during testing, frequently changed the channel when it detected interference. To test DFS channels, the AP was placed on Auto with only DFS channels available in the Channel list.



- 10 Open the **Performance** tab
- 11 Check **Enable QoS according to 802.11e (WME)**. If the option is grayed out, it means that the AP model sets it to always on. The option is not available to be turned off.



Note: DSCP Tags

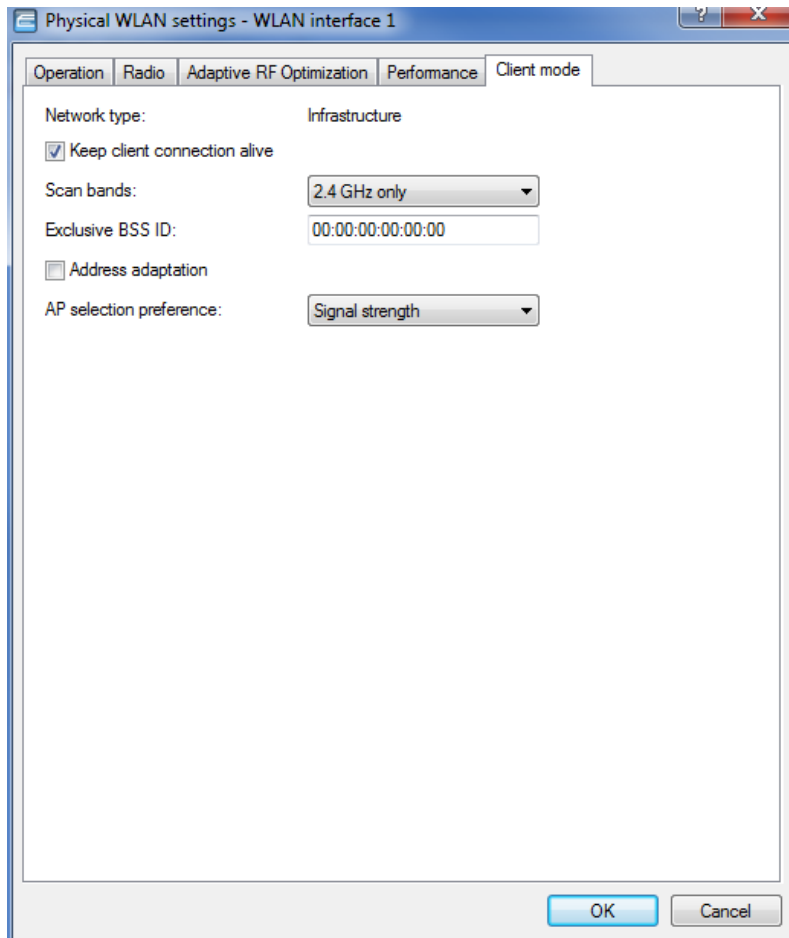
LANCOM Systems APs that do not act as routers do not adjust DSCP/ToS/CoS settings. They leave the DSCP tags unaltered and use the standard meanings of the DSCP/CoS/ToS mapping. If this is not appropriate for the given network setup, map a correspondence between the tags



Note: Versity and LANCOM don't support WMM_AC

Versity and LANCOM do not implement WMM_AC (Admission Control). Bandwidth can be controlled with the Airtime fairness setting. Use of this setting is beyond the scope of this document.

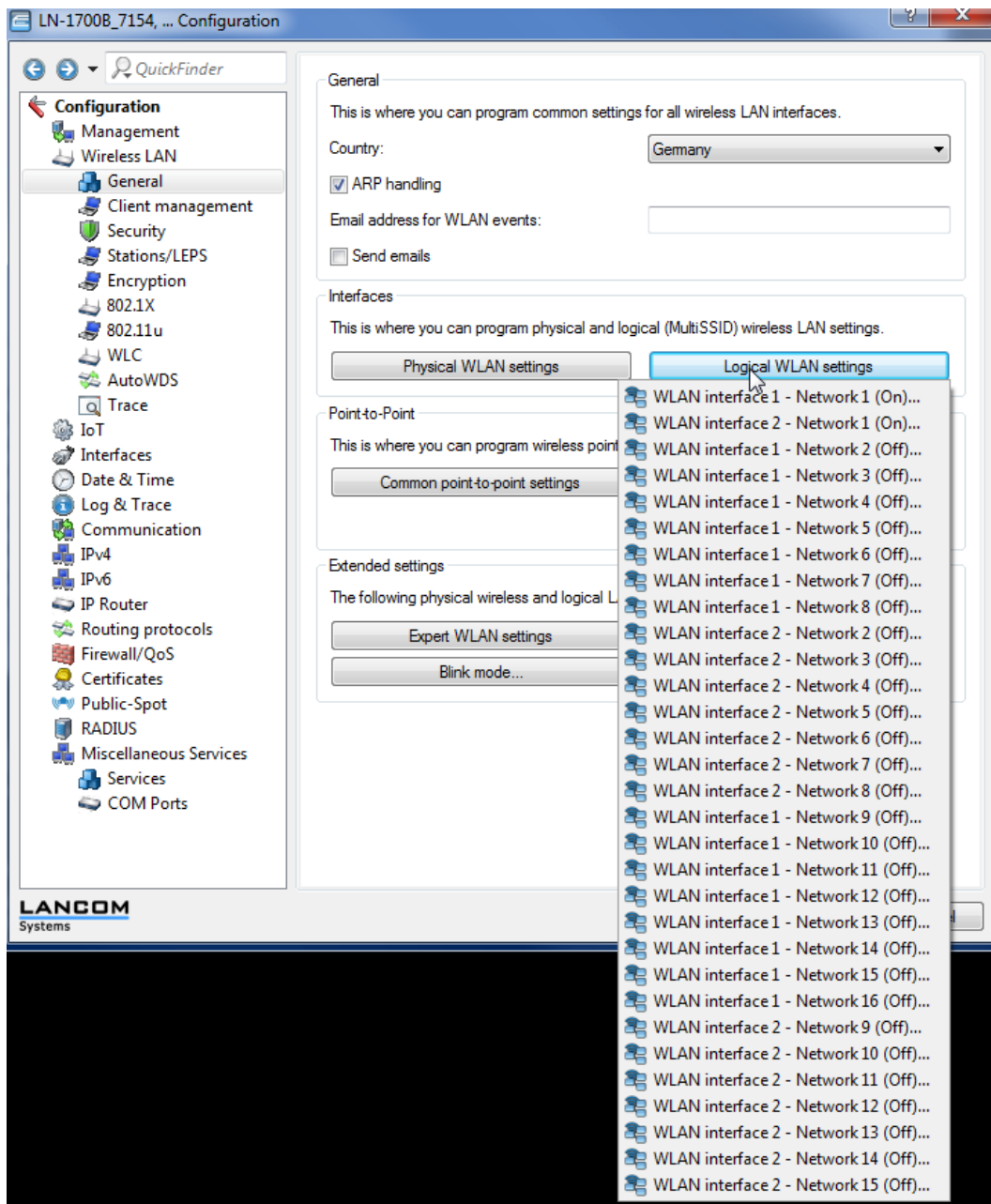
Client mode was tested in the default settings shown.



Configure SSID Settings (Logical WLAN settings)

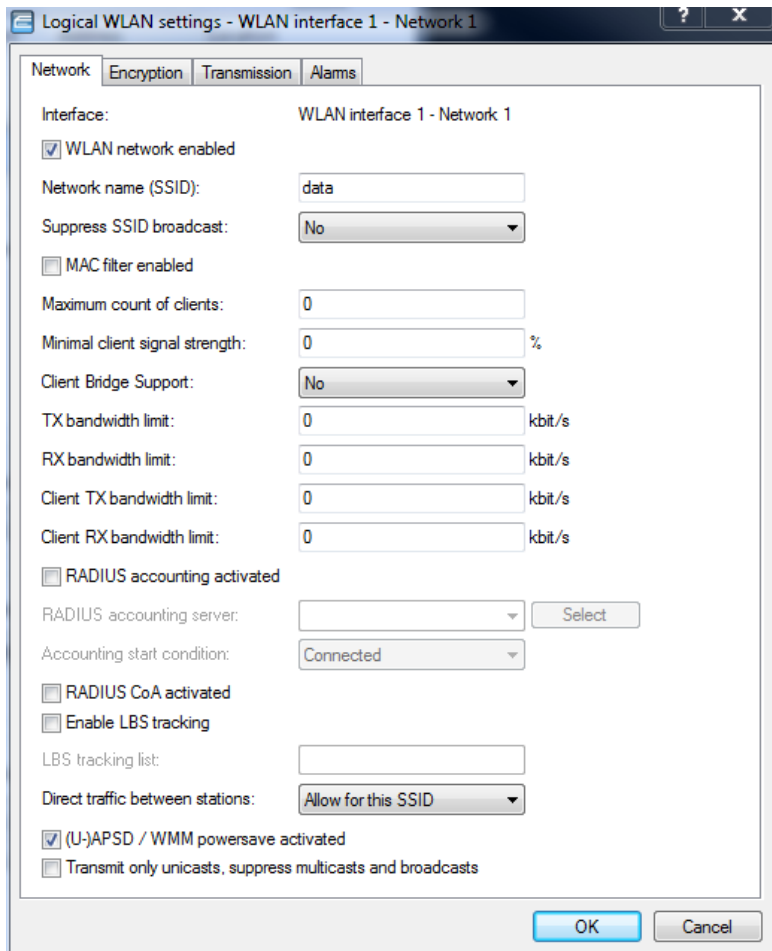
Configure general SSID settings

- 1 Open LANConfig, highlight an AP, and right click on **Configure** as before to begin the configuration process.
- 2 Navigate to **Configuration>Wireless LAN>General**
- 3 Click on **Logical WLAN Settings**.



- 1 Set **WLAN network enabled** for all active SSIDs.
- 2 Fill in **Network name (SSID)**.
- 3 For a hidden network, set **Suppress SSID broadcast** to Yes if desired.
- 4 For VIEW testing, **MAC filter enabled** was unchecked.
- 5 Choose **Allow for this SSID for Direct traffic between stations**. This allow peer-to-peer communication.

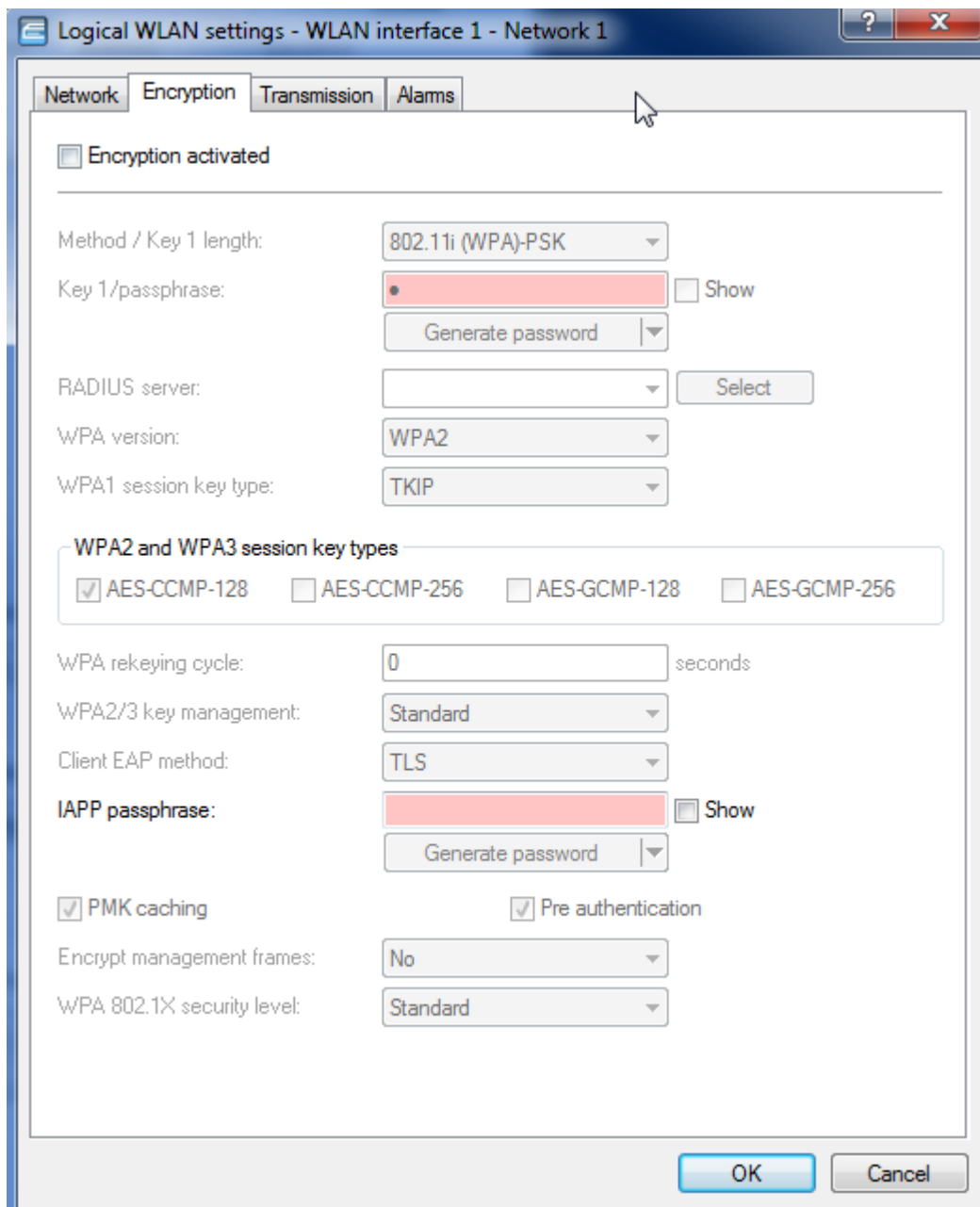
- 6 Check **(U-)APSD/WMM powersave activated**. The 84-series phones will not connect if this is not checked. They use WMM-PS to preserve battery life.
- 7 Ensure that **Transmit only unicasts, suppress multicasts and broadcast** is unchecked for PTT operation and for many 3rd party applications.



Configure security settings

Navigate to the **Encryption** tab for all security types.

For Open security, uncheck **Encryption activated**.



WPA2-PSK

- 1 From the **Encryption** tab, check **Encryption activated**
- 2 For **Method/Key 1 length**, select **802.11i (WPA)-PSK**
- 3 Enter a **Key 1/ passphrase**. Ensure that this is the same value that is entered for the **Password** in the Versity handsets and the **Passphrase** in the 84-series handsets.
- 4 Select **WPA2** for the WPA version.
- 5 Select **Standard** for **WPA2/3 key management**.

- 6 Enter a common value for the **IAPP passphrase** on each AP that will be providing the same SSID. This ties the standalone APs into a common network.
- 7 For 84-series use, enter **No** for **Encrypt management frames**. If there are only Versity handsets on the SSID, **Yes** can be selected.



Note: IAPP passphrase identifies network membership for standalone APs.

For phones to roam between standalone APs with the same SSID, they must have the same entry for the **IAPP passphrase**.



Note: For 84-series handsets, select only AES-CCMP-128.

During testing, it was found that the 84-series would only connect to networks that advertised **AES-CCMP-128** only for the **WPA2 and WPA3 session key types**.

The Versity phone would connect when all of the session key types were selected.

WPA2 – Enterprise

**Note: Spectralink handsets work with WPA1/WPA2/WPA3.**

During testing, it was found that the 84-series would only connect to networks that advertised **AES-CCMP-128** only for the **WPA2 and WPA3 session key types**.

The Versity phone would connect when all of the session key types were selected.

- 1 Check **Encryption activated**.
- 2 For **Method/Key 1 length**, select **802.11i (WPA)-802.1x**.
- 3 Add a RADIUS server. From the **Encryption** tab, click on **Select**.

Logical WLAN settings - WLAN interface 1 - Network 1

Network Encryption Transmission Alarms

Encryption activated

Method / Key 1 length: 802.11i (WPA)-802.1x

Key 1/passphrase: • Show
Generate password

RADIUS server: EXTRADIUS

WPA version: WPA1/2/3

WPA1 session key type: TKIP/AES

WPA2 and WPA3 session key types

AES-CCMP-128 AES-CCMP-256 AES-GCMP-128 AES-GCMP-256

WPA rekeying cycle: 0 seconds

WPA2/3 key management: Fast roaming

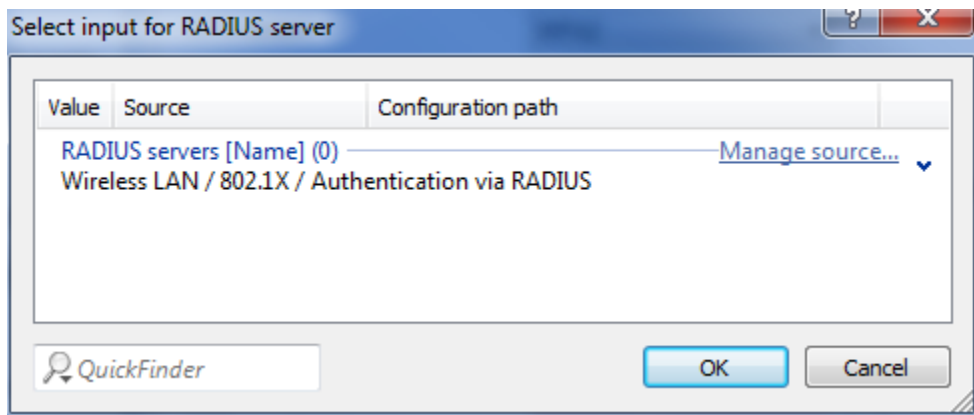
Client EAP method: PEAP/MSCHAPV2

IAPP passphrase: • Show
Generate password

PMK caching Pre authentication

Encrypt management frames: No

WPA 802.1X security level: Standard



- 4 Click on **Manage source** for an external server
- 5 Click on **Add**
- 6 Fill in the fields for:
 - » Name
 - » Server address
 - » Leave the default value for Server port
 - » Enter the Secret
 - » Repeat the secret
- 7 Click on **OK**.

RADIUS servers - New Entry

Name:

Server address:

Server port:

Attribute values:

Secret: Show

Repeat:

Monitoring profile:

Backup server:

The device determines the correct source IP address for the destination network automatically. If a certain source IP address should be used, insert it here symbolically or directly.

Source address (opt.):

Check the name and Click on **OK** to use the new RADIUS server definition in the SSID authentication.

RADIUS servers

Name	Server address	Server port	Attribute values	Monitoring profile	Backup server	Source addr.
EXTRADIUS	172.29.65.18	1,812				

- 8** Pick WPA1/2, WPA2, or WPA2/3 for the **WPA version**
- 9** Choose **AES-CCMP-128** for **WPA2 and WPA3 session key type**. The 84-series will not associate if the other options are also checked. The 84-series will not connect if **SHA256** is included for **WPA2/3 key management**.
- 10** Enter **Standard** for OKC roaming. Enter **Fast roaming** for 802.11r. It is recommended to select both fast roaming types for the most compatibility with other devices.

11 Select **PEAP/MSCHAPV2** for the Client EAP method, even if EAP-TLS is the desired security type.

12 Check **PMK caching** and **Preauthentication**

Logical WLAN settings - WLAN interface 1 - Network 1

Network Encryption Transmission Alarms

Encryption activated

Method / Key 1 length: 802.11i (WPA)-802.1x

Key 1/passphrase: • Show

Generate password

RADIUS server: EXTRADIUS

WPA version: WPA1/2/3

WPA1 session key type: TKIP/AES

WPA2 and WPA3 session key types

AES-CCMP-128 AES-CCMP-256 AES-GCMP-128 AES-GCMP-256

WPA rekeying cycle: 0 seconds

WPA2/3 key management: Standard & Fast roaming

Client EAP method: PEAP/MSCHAPV2

IAPP passphrase: • Show

Generate password

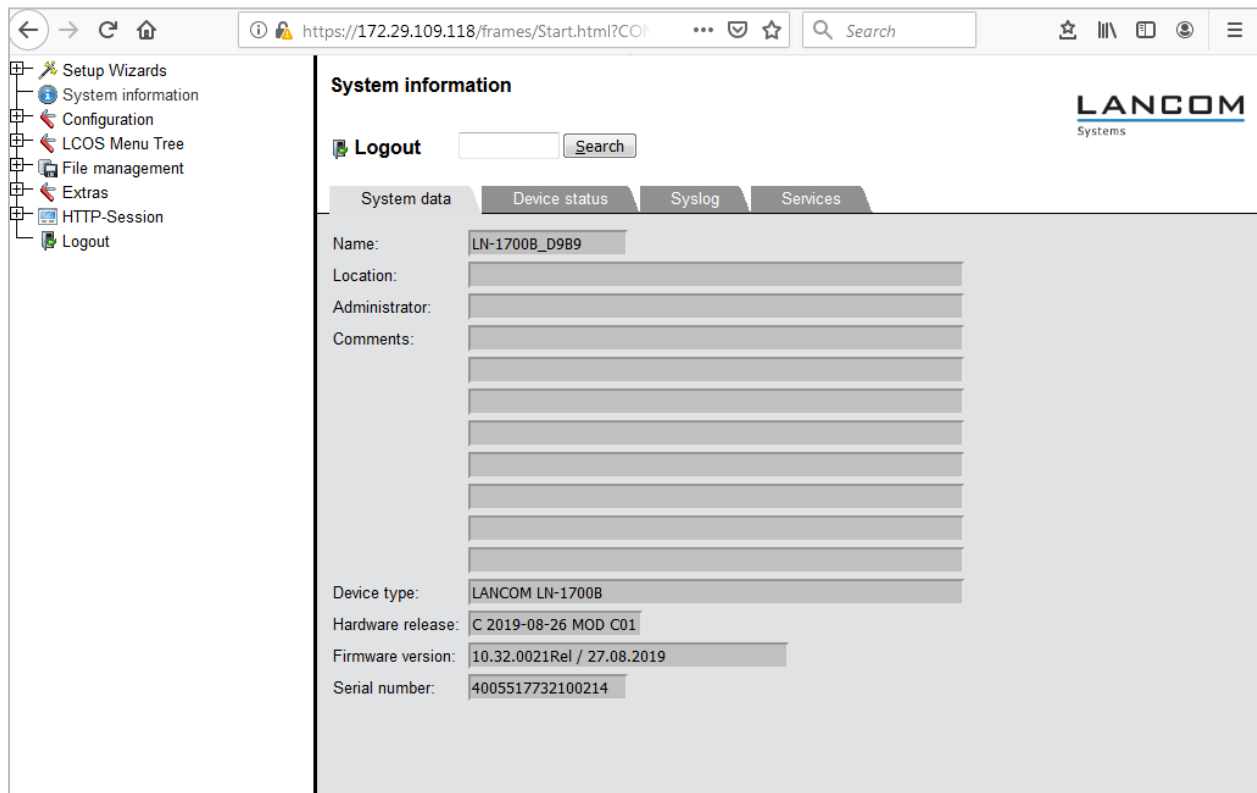
PMK caching Pre authentication

Encrypt management frames: No

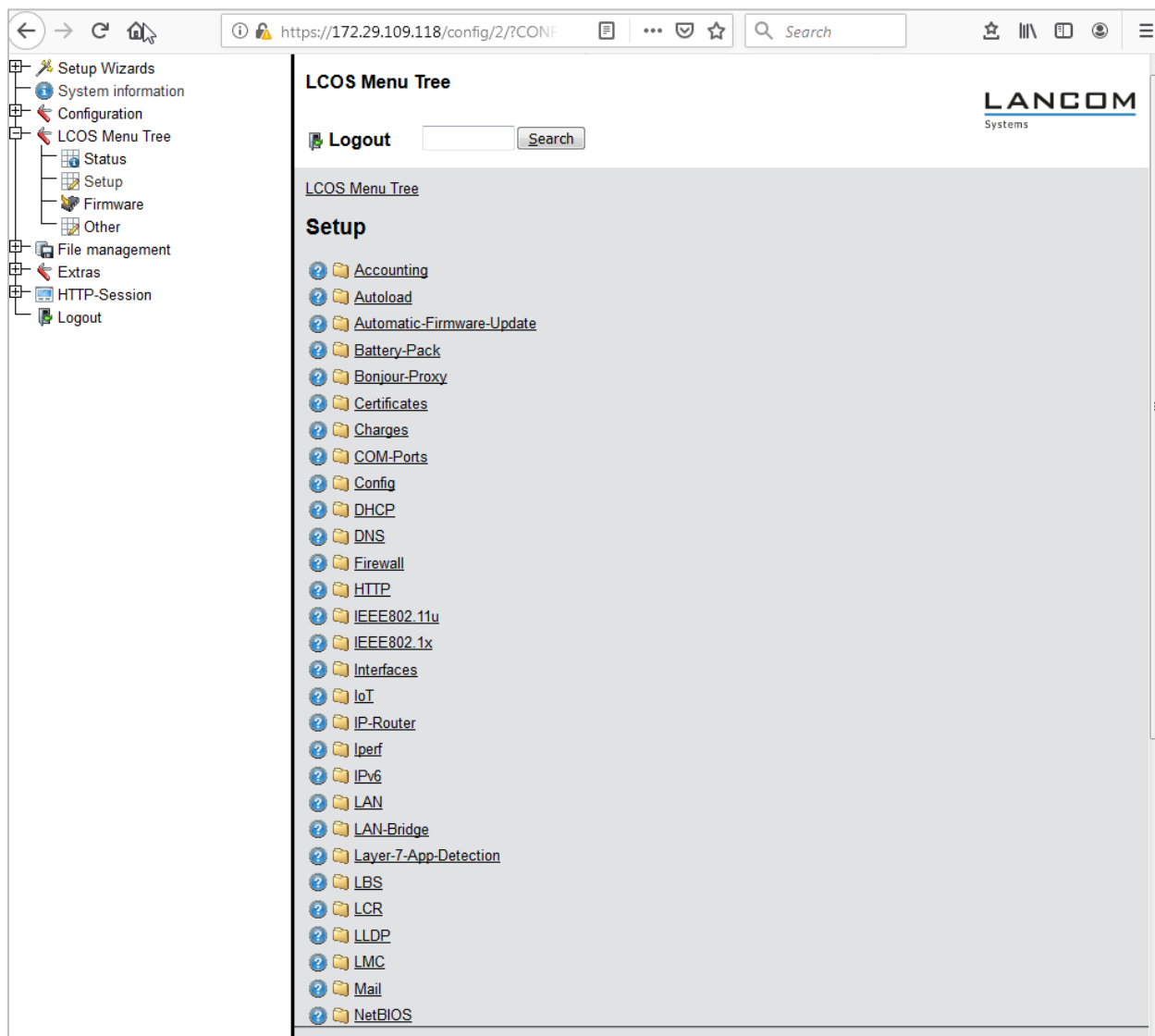
WPA 802.1X security level: Standard

13 Because of the lack of this feature in LANconfig, one setting must be set from WEBconfig. It is very important to perform the following steps for OKC roaming until the problem is fixed.

- a Open a browser window and type <https://xxx.xxx.xxx.xxx> where the x's represent the IP address of the AP.



b Navigate to LCOS Menu Tree>Setup.




- c Navigate further to Interfaces>WLAN>Encryption.
- d Highlight the desired SSID and click on it. The SSID's are numbered in this way:
 - The first SSID on the first radio is WLAN-1, the first SSID on the second radio is WLAN-2
 - The rest of the SSID's on a given radio are numbered as WLAN-1-2, WLAN-1-3, or WLAN-2-2, WLAN-2-3 etc.

The screenshot shows the LANCOM Systems configuration interface. On the left is a navigation tree with options like 'Setup Wizards', 'System information', 'Configuration', 'LCOS Menu Tree', 'Status', 'Setup', 'Firmware', 'Other', 'File management', 'Extras', 'HTTP-Session', and 'Logout'. The main area is titled 'COS Menu Tree' and contains a search bar and a 'Logout' button. Below this is the 'LCOS Menu Tree' with 'Setup', 'Interfaces', and 'WLAN' options. The 'Encryption' section displays a table with the following data:

Ifc	Encryption	Default-Key	Method	Key	RADIUS-Profile	WPA-Version	WPA1-Session-Keytypes	WPA2-3-Session-Keytypes	WPA-Rekeying-Cycle	WPA2-Key-Management	SAE-Groups	Prot.-Mgmt-Frames	PMK-Caching	Client-EAP-Method
WLAN-1	Yes	1	802.11i-WPA-802.1x	*	EXTRADIUS	WPA1/2/3	TKIP/AES	AES-CCMP-128	0	Fast-Roaming	secp256r1 secp384r1 secp521r1	No	Yes	PEAP/MSCH
WLAN-2	Yes	1	802.11i-WPA-PSK	*		WPA1/2/3	TKIP/AES	AES-CCMP-128	0	Fast-Roaming Standard	secp256r1 secp384r1 secp521r1	No	Yes	TLS
WLAN-1-2	No	1	802.11i-WPA-PSK	*		WPA2	TKIP	AES-CCMP-128	0	Standard	secp256r1 secp384r1 secp521r1	No	Yes	TLS
WLAN-1-3	Yes	1	802.11i-WPA-PSK	*		WPA2	TKIP	AES-CCMP-128	0	Fast-Roaming Standard	secp256r1 secp384r1 secp521r1	No	Yes	TLS

- e The settings should be the same as their values from the LANconfig tool (if they have been saved by touching OK before WEBconfig is opened). The important additional setting here is set OKC to **Yes**.

LCOS Menu Tree



Logout

LCOS Menu Tree

- Setup
 - Interfaces
 - WLAN

Encryption

- ifc
- Encryption
- Default-Key
- Method
- Key
 - (Repeat)
 - Key
- RADIUS-Profile
- WPA-Version
- WPA1-Session-Keytypes
- WPA2-3-Session-Keytypes
- WPA-Rekeying-Cycle
- WPA2-Key-Management
- SAE-Groups
- Prot.-Mgmt-Frames
- PMK-Caching
- Client-EAP-Method
- Pre-Authentication
- WPA-802.1X-Security-Level
- OKC
- Enhanced-Open-Groups
- PMK-IAPP-Secret
 - (Repeat)
 - PMK-IAPP-Secret
- Authentication

WLAN-1

Yes

1 (max. 1 characters)

802.11i-WPA-802.1x

• (max. 63 characters)

• (max. 63 characters)

EXTRADIUS (max. 16 characters)

WPA1/2/3

TKIP/AES

TKIP

AES-CCMP-128

AES-CCMP-256

AES-GCMP-128

AES-GCMP-256

0 (max. 10 characters)

Fast-Roaming

SHA256

Standard

secp256r1

secp384r1

secp521r1

No

Yes

PEAP/MSCHAPv2

Yes

Standard

Yes

secp256r1

secp384r1

secp521r1

• (max. 64 characters)

• (max. 64 characters)

Open-System



Note: Management Frame Protection is supported by Versity

Versity handsets support Management Frame Protection (802.11w). When WPA3 is in use, the industry security standard requires that Management Frame Protection be set to at least optional. The 84-Series handsets do not support Management Frame Protection. LANCOM is advertising optional even when set to No when WPA3 is selected. The APs are properly detecting whether the handset can handle encrypted management frames with all settings.



Note: Fast roaming supported by Versity

Fast roaming (802.11r) is supported by Versity. It is not supported by the 84-series handsets. Advertising **Standard & Fast roaming** in the **WPA2/3 key management** setting is the best way for one SSID to support both handset model families.



Note: Fast roaming issue on Versity

There is an issue at the radio chip level on Versity phones with Fast roaming. It is present on all version prior to 1.7. It is expected to be fixed in 1.7. In versions 1.0 to 1.5, fast roaming is chosen above other roaming choices. In 1.6, as a workaround, OKC is preferred. When fast roaming is fixed, 1.7 will return to preferring fast roaming.



Note: Set OKC to Yes from WEBconfig

Until the OKC setting is added to LANconfig on the LANCOM tool, it is necessary to use WEBconfig to set it to yes.



Note: Problem with 84-series and roaming

Using the LN-170xB, the 84-series phones could not perform an OKC roam on the 802.11ac radio. It was successful with the 802.11bgn/an radio. Using the LN-830U or the LN-86Xacn, the 84-series phones could not perform an OKC roam on the 802.11bgn/an radio. It was successful with the 802.11ac radio. Recommended workaround: use WPA2-PSK with the 84-series phones

END DOCUMENT