SMART HOPPING® infrastructure installation and service guide

User guide

Trademarks

RTX and all logos thereof are trademarks of RTX A/S, Denmark.
Other product names used in this publication are for identification purposes and may be trademarks of the respective companies.

Disclaimer

This document and the information contained is property of RTX A/S, Denmark. Unauthorized copying is not allowed. The information in this document is believed to be correct at the time of writing. RTX A/S reserves the right at any time to change said content, circuitry, and specifications.

Confidentiality

This document should be regarded as confidential.

Stroemmen 6, DK-9400 Noerresundby
Denmark
P. +45 96 32 23 00
F. +45 96 32 23 10
www.rtx.dk

Additional information:
Ref: HDJ
Reviewed by: BKI

Contents

Figures

Tables

1 About this guide

This Smart-hopping Infrastructure Installation and Service Guide provides complete instructions and procedures for installing, configuring, and servicing Smart-hopping 1.4/2.4-GHz networks. This section describes the document and includes:

- IEC 60601–1–2:2014 Compliance
- Audience
- Document Organization
- Notational Conventions
- References
- Terms and abbreviations
- Document history

1.1 IEC 60601–1–2:2014 Compliance

This document includes changes to the LAN cable requirements for certain Smart-hopping components. For more information, see the Required Use of Shielded Twisted-Pair (STP) Cables section. These STP cables enable compliance of specific components to EN 60601-1- 2:2015 (IEC 60601-1-2:2014) Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests.

1.2 Audience

The Smart-hopping Infrastructure Installation and Service Guide is written for qualified service personnel who install, configure, and service the Smart-hopping 1.4 or 2.4 GHz Infrastructure as part of an overall Network deployment.

1.3 Document organization

The information in this guide is organized and presented as follows:

- Chapter 1, Overview, describes the Smart-hopping Infrastructure and how it is used to provide a bidirectional data flow between the Information Center and a Patient Monitor.
- Chapter 2, Planning Your Deployment, provides information and procedures that must be followed to ensure a successful Smart-hopping Infrastructure deployment.
- Chapter 3, Installing and Configuring the Smart-hopping Infrastructure, gives complete procedures to install the Smart-hopping Infrastructure components and configure the Smart- hopping Access Point Controllers and Access Points.
- Chapter 4, Expanding or Modifying an Installed Smart-hopping infrastructure, lists procedures to expand or modify an existing, installed Smart-hopping Infrastructure.
- Chapter 5, Smart-hopping System Testing, includes procedures to test a Smart-hopping Infrastructure installation.
- Chapter 6, Troubleshooting System Issues, includes procedures to troubleshoot issues with your Smart-hopping infrastructure.
- Appendix A, Installing Multiple Smart-hopping systems at a Single Hospital Site, lists configuration rules and guidelines to enable you to install up to 22 independent Smart-hopping systems at a given installation site.

- Appendix B, Routed Topology Configuration Information, provides important information to help you configure a routed Smart-hopping Infrastructure topology.

- Appendix C, Upgrade Tool Warning and Error Messages, lists and describes messages generated by the Philips Upgrade Tool.

- Appendix D, Using the APC Serial Console, describes the menu options to configure the APC using the serial port console.

- Appendix E, Smart-hopping Network Deployments: Layer 2, Layer 3, Routed, and Non-Routed Explained, explains how the terminology Layer 2, Layer 3, Non-Routed, and Routed are used in the context of the Smart-hopping infrastructure user interfaces and this documentation.

- Appendix F, DHCP Option 43, describes the procedures to configure the DHCP Option 43.

- Appendix G, Configuring the Layer 3 Option on each AP, describes the procedures to configure the Layer 3 option on each AP for CSCN sites which are not using DHCP.

1.4 Notational conventions

This guide uses the following notational conventions to convey information:

Warning	A Warning alerts you to a potential serious outcome, adverse event or safety hazard. Failure to observe a warning may result in death or serious injury to the user or patient.
Caution	A Caution alerts you to where special care is necessary for the safe and effective use of the product. Failure to observe a caution may result in minor or moderate personal injury or damage to the product or other property, and possibly in a remote risk of more serious injury.
Note	A Note contains additional information on the product.

1.5 References

Refer to these other documents for more installation service information about the Smart-hopping infrastructure:

Reference	Name
1	Smart-hopping Access Point Controller Installation Guide - provides procedures to physically install and power the Smart-hopping Access Point Controller at the clinical site.
2	Smart-hopping Access Point Installation Guide (1.4 GHz) - provides procedures to install the Smart-hopping 1.4 GHz Access Point and remote Antennas at the clinical site to a wall, or above or below a ceiling tile.
3	Smart-hopping Access Point Installation Guide (2.4 GHz) - gives procedures to install the Smart-hopping 2.4 GHz AP at the clinical site to a wall, or above or below a ceiling tile.
4	Smart-hopping 1.4 GHz Remote Antenna Installation Guide - provides procedures to install the Smart-hopping 1.4 GHz Remote Antennas at the clinical site to a wall, or above or below a ceiling tile.
5	Smart-hopping Synchronization Unit Installation Guide - lists procedures to install the Smart-hopping Sync Unit at the clinical site.
6	Upgrading Smart-hopping Access Point Controllers and Access Points - gives procedures to use the Philips Smart-hopping APC and AP Upgrade Tool to install and synchronize the firmware version on Smart-hopping APCs and APs.

1.6 Terms and abbreviations

Note the following terms, acronyms, and abbreviations used throughout this document and in related documentation:

Abbreviation	Description
Access Point (AP)	A Smart-hopping component that provides bidirectional wireless access to the monitoring network for Patient Monitors.
Access Point Controller (APC)	A Smart-hopping component used to manage the operation of the Access Points. One APC is elected the Primary APC. The Primary APC supports the web interface to the system and manages the Primary configuration.
Access Point Group/AP Group	A logical grouping of Access Points. AP members of the same AP Group inherit common configuration settings (defaults). AP groups will often map logically to the clinical units in which the Smart-hopping Infrastructure is being installed.
IntelliVue Network	This term refers to the entire IntelliVue network. In a routed topology, the IntelliVue Network includes the routers, switches, firewalls, and the Smart-hopping Infrastructure wireless subnet.
Patient Monitor (PM)	The Patient Monitor relays real-time physiological waveforms and trends to the Philips Information Center server.
Smart-hopping infrastructure	Philips proprietary wireless network designed for continuous monitoring that provides two-way communications between Patient Monitors, and the Information Center.
Smart-hopping Infrastructure Service Tool	The software used to upgrade Smart-hopping APCs and APs, verify that APCs on your network are configured correctly, and display warning and error messages that you may use to troubleshoot any configuration errors that may exist on your Smart-hopping network. The Smart-hopping Infrastructure Service Tool is also referred to as the Upgrade Tool. This tool was previously referred to as the Upgrade Wizard.
Smart-hopping Wireless Subnet	This term is used to describe the Smart-hopping Infrastructure “network” that contains the infrastructure used in a routed topology to connect Smart-hopping Infrastructure devices.
Partnered APC -	Configurable element within an AP Group used to determine which APC manages the operation of the AP members of a particular AP Group.
Philips Patient Information Center (PIC) iX	This term refers to the Philips Patient Information Center iX.
Power over Ethernet (PoE) Switch	The Power over Ethernet (PoE) Switch is a 24-port Power- over-Ethernet device that provides 48-VDC power to Access Points (and also remote Sync Units if connected) via 100-Base-TX Ethernet LAN cabling. For systems using a Power over Ethernet Switch, the ITS4844A Tele Synchronization Unit is required to use the PoE feature of the PoE Switch.
RF Access Code	Configurable element in the Smart-hopping AP defaults shared among APs and Patient Monitors to control wireless access to the monitoring network. Portable devices only connect to access points with which they share access codes. The RF Access Code allows a specific wireless client that is programmed with a matching Access Point RF Access Code to connect to that Access Point.
Synchronization (Sync) Unit	The Smart-hopping Sync Unit provides a necessary common clock signal to synchronize all the Access Points in the system. As patients ambulate around the

Abbreviation	Description
	hospital coverage area, their transmitted data hands over from one AP to another seamlessly without interruption or data loss.
System ID	Configurable element in the APC Configuration to logically associate Access Points and Access Point Controllers operating within the same Smart-hopping Infrastructure.
Uninterruptible Power Supply (UPS)	The UPS supplies backup power to protect against hospital generator changeover interruptions, and short power line transients.

1.7 Document history

Revision	Resp.	Date	Comments
1.0	HDJ/BKI	30 Oct-2025	First published version.

2 Overview

This chapter provides a high-level overview of the Smart-hopping network and includes:

- Respecting patient care boundaries
- Product safety
- Introduction
- Smart-hopping network components
- Network data flow
- Defined bandwidth
- Supported topologies and system limits
- Smart-hopping infrastructure specifications
- Smart-hopping infrastructure product numbers
- New smart-hopping hardware features
- New smart-hopping software features

2.1 Respecting patient care boundaries

When planning your Smart-hopping infrastructure deployment, you must consider the boundaries of the patient care environment and the restrictions against installing network equipment within these boundaries. Use caution when installing network equipment. Typically, network equipment is not suitable for use within the patient environment.

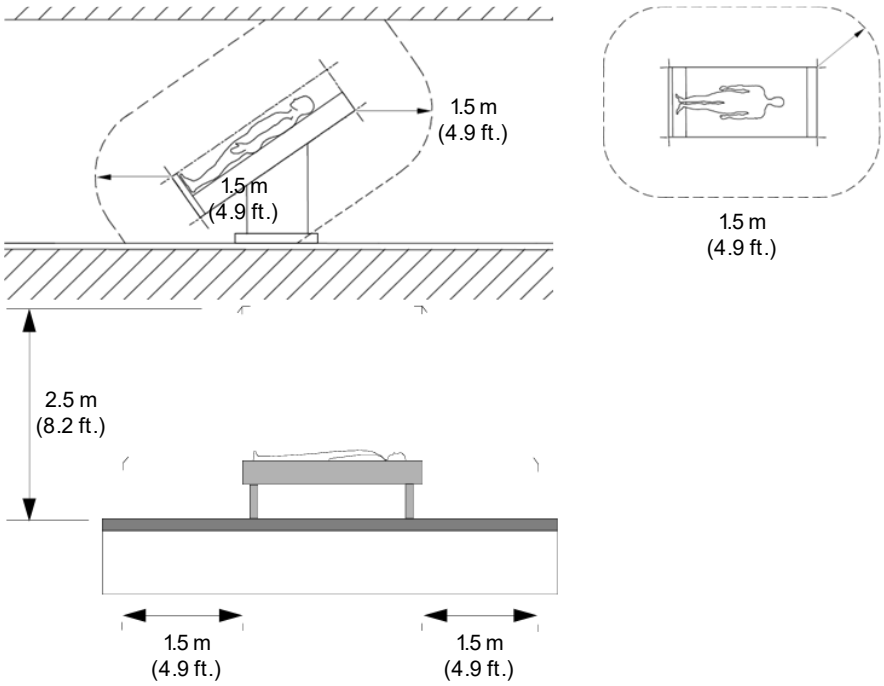


Figure 1: *Patient Environment Boundaries*

Warning Network system components are not suitable for installation in the Patient Care Vicinity (Patient Environment) -- any area within 1.5 meters (4.9 ft.) horizontally and 2.5 m (8.2 ft.) vertically above the floor from any patient care location in which medical diagnosis, monitoring, or treatment of the patient is carried out.

Note also the general restriction concerning location of Smart-hopping Access Points.

Warning The Smart-hopping Access Points must be operated at least 15 cm (6 inches) from any person. This is necessary to ensure that the product is operated in accordance with the Radio Frequency (RF) Guidelines for Human Exposure.

2.2 Product safety

This section consolidates the general safety warnings associated with the Smart-hopping infrastructure devices. These warnings are repeated throughout the product documentation in context where relevant.

Warning Installations without APC Redundancy can impact client devices, resulting in a potential loss of central monitoring if APC fails.

Smart-hopping device failures may impact multiple client devices. To minimize a single point of failure in clinical use areas, deploy multiple Synchronization Units, Access Points, Remote Antennas, and Access Point Controllers to mitigate single points of failure.

Stopping the upgrade process before completion may cause the Upgrade Tool software to become unstable.

Signal interference may impact multiple devices and lead to a loss of central monitoring.

Exceeding the Access Point capacity can lead to loss of central monitoring. See Chapter 2, ITS_Inf Design_and_Site_Prep.fm for more information.

Smart-hopping device installations must be performed by qualified personnel, abiding by all building and safety codes.

Warning To reduce the impact of EMC Interference, use shielded LAN Patch panel cables to connect the Synchronization Units and Access Point Controllers to the switch.

Only connect supported Remote Antennas to Smart-hopping Access Points.

Install Smart-hopping infrastructure devices in remote locations that are not in the vicinity of patients or clinical use areas.

Follow all documented steps, waiting intervals, and test and inspection procedures when installing and configuring APCs using the Serial Console (SSH) interface, web client, or Upgrade Tool software.

To prevent unexpected loss of network connectivity. use care when adding and connecting new APCs to the Smart-hopping network and when manually entering data. Make sure the devices start up and function as intended.

Use care when using APC and AP web-based interfaces. Navigating too quickly may cause the web page to freeze, information to not be entered correctly, and APCs to unexpectedly reboot, leading to temporary loss of network connectivity.

To prevent unexpected loss of network connectivity, make sure you have proper network device selection prior to upgrade, and read any errors carefully during the deployment process.

To ensure system coverage and performance, make sure all network devices are updated to a supported and compatible revision.

To reduce exposure to environmental particles, make sure all ceiling tile holes are covered by the Access Point or Remote Antenna.

To ensure proper Smart-hopping device setup, make sure Access Point and Remote Antenna cable connections are secure.

To ensure system coverage, roaming, and performance, make sure you follow all documented steps when configuring synchronization delay.

To ensure system coverage, roaming, and performance, make sure you follow all documented steps for Access Point and Remote Antenna installation

Caution To prevent unintended detachment of Smart-hopping devices (such as Access Points and Remote Antennas), make sure the devices are securely attached to the surface on which they are mounted.

Seal openings around Smart-hopping devices with fire resistant material (such as firestop putty) to Plenum space when installing APs. Vertical mount and Flush mount of APs is not supported in Plenum Spaces.

2.3 Introduction

The Smart-hopping Infrastructure is a proprietary wireless network to provide two-way communications between Patient Monitors and the Information Center.

Using the Smart-hopping wireless protocol, the Smart-hopping Infrastructure provides monitoring capabilities for ambulatory patients within a wide coverage area. The Patient Monitors and Smart-hopping Infrastructure operate on the 1.4 GHz US Wireless Medical Telemetry Service (WMTS) band or on the 2.4 GHz Industrial Scientific and Medical (ISM) band.

Patient Monitors exchange data with the Information Center (bidirectional communication) for monitoring, analysis, alarms, data storage and recording.

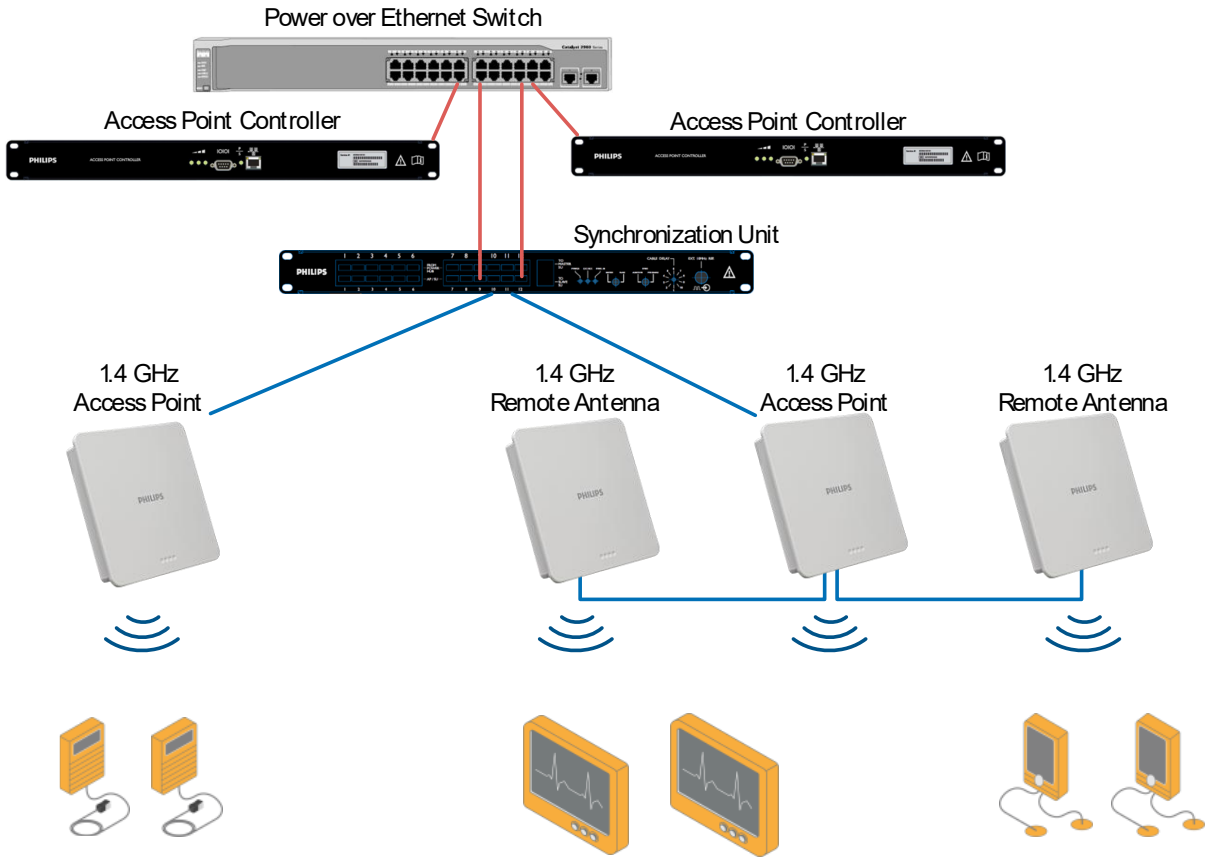


Figure 2: *Smart-hopping Infrastructure*

You can configure the Access Point Controller to communicate with 1.4 or 2.4-GHz Smart-hopping Access Points (APs). 1.4-GHz APs can only communicate with 1.4 GHz Patient Monitors. Likewise, 2.4-GHz APs can only communicate with 2.4 GHz Patient Monitors. You cannot mix 1.4 GHz and 2.4 GHz Patient Monitors at a given installation site.

Smart-hopping technology utilizes a cognitive radio that senses the RF environment and adapts to it. Dynamic wireless channel allocation ensures best use of available wireless spectrum. When configured to operate in the 2.4- GHz spectrum, the Smart-hopping Infrastructure is designed to co-exist with 802.11 wireless deployments.

2.4 Smart-hopping network components

The Smart-hopping Network consists of an Ethernet LAN that can include LAN switches and routers, and is used to interconnect multiple Access Points to one or more Philips Access Point Controllers (APC).

The key function of the Smart-hopping Network is to transport data over a wireless LAN-based infrastructure (part of the IntelliVue Network) between the Patient Monitors and Information Center servers, where the data can be recorded or used to alert clinical operators as to a change in monitored parameters.

Five major components comprise the Philips Smart-hopping Infrastructure:

- 1.4 GHz or 2.4-GHz Smart-hopping Access Points
- Access Point Controller
- Synchronization Unit
- Power over Ethernet Switch
- Uninterruptible Power Supply

2.4.1 Smart-hopping Access Points

The Smart-hopping Infrastructure supports three types of Smart-hopping Access Points:

- Model ITS867216A (P/N 867216) Smart-hopping 2.0 Access Point 1.4 GHz
- Model ITS4843C (P/N 866394) Access Point for 1.4-GHz Smart-hopping Infrastructure
- Model ITS4852A (P/N 989803171221) AP for 2.4-GHz Smart-hopping Infrastructure

2.4.2 1.4 GHz Smart-hopping infrastructure core Access Points

The Smart-hopping 2.0 Access Point (AP), Model ITS867216A (P/N 867216), (Figure 3) provides an air-link to transmit and receive data between wireless clients and the Philips Information Center via the Smart-hopping Network.

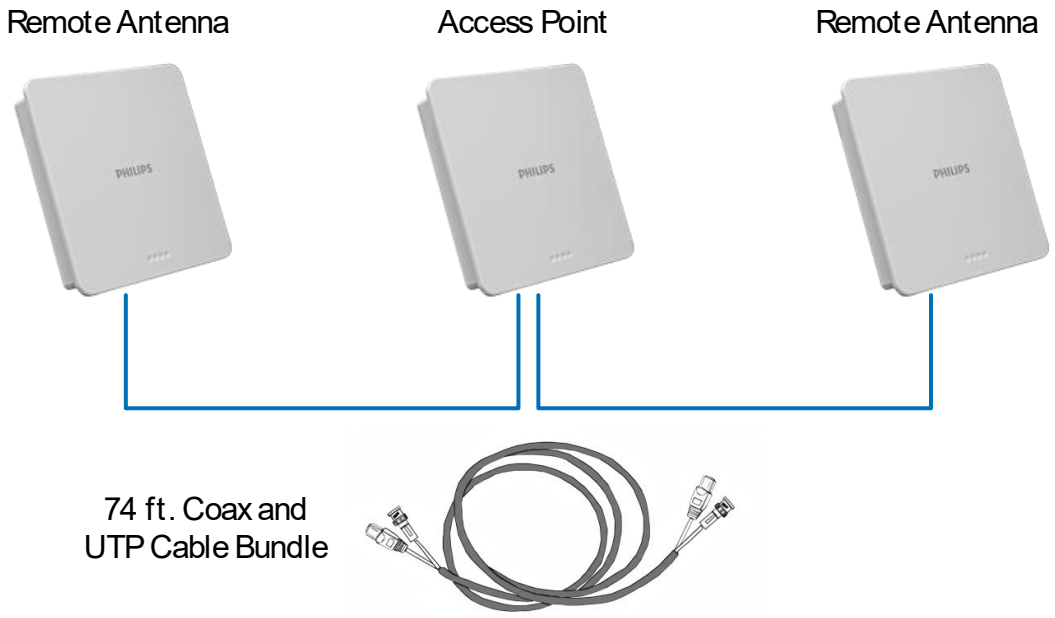


Figure 3: 1.4-GHz Smart-hopping Infrastructure Core Access Point

The AP supports a connection of up to two connected Model ITS4846A Remote Antennas (RAs). A 74-foot (22.6 m) coaxial and unshielded twisted pair (UTP) cable bundle connects a Remote Antenna to an Access Point.

The effective range of the Access Point and of each Remote Antenna is typically 32 feet. The Access Point always supports a maximum of 18 wireless clients regardless of its component configuration. An Access Point alone supports 18 wireless clients. When used with a single RA, the Access Point supports nine wireless clients and its connected RA supports nine wireless clients (9+9=18). When used with two RAs, the Access Point supports six wireless clients and each connected RA supports six wireless clients (6+6+6=18).

When monitored patients are ambulatory, data roams seamlessly between the other Smart-hopping Access Points in the coverage area. The Access Point and each RA are always used with their two supplied antennas installed. Refer to the Smart-hopping 1.4 GHz Access Points Installation Guide for more details.

2.4.3 2.4 GHz Smart-hopping Access Points

The Smart-hopping Access Point (AP), Model ITS4852A (P/N 989803171221) (Figure 1-4), provides an air-link to transmit and receive data between wireless clients and the Philips Information Center via the Smart-hopping network.

Figure 4: *2.4 GHz Smart-hopping Access Point*

The Smart-hopping 2.4 GHz AP supports up to 18 wireless clients and has a 9.8 m (32 ft.) Radius-of-Coverage. Refer to the Smart-hopping 2.4 GHz Access Point Installation Guide for more details.

2.4.4 Access Point Controller

The Philips Access Point Controller (APC) centralizes the management and security features of the Smart-hopping network. Working with the Philips Smart-hopping Network, the APC provides a gateway between the Smart-hopping Access Points (APs) and the Philips Information Center.

The Smart-hopping APC can be configured for the 1.4 GHz or 2.4-GHz Smart-hopping APs. Up to nine APCs can be installed on the network to support the data throughput from the connected Smart-hopping APs.

Refer to the *Smart-hopping Access Point Controller Installation Guide* for more details.

Figure 5: Access Point Controller

2.4.5 Synchronization unit

The Philips Synchronization Unit ITS4844A (866212) provides a necessary common clock signal to synchronize all the Smart-hopping Access Points in the system. Access Points must synchronize, as the patients move around the hospital, they are able to maintain and hand over connections between the Access Points seamlessly.

Each Sync Unit provides synchronization for up to 12 Access Points. The maximum cable length between a Switch/ PoE Unit/Sync Unit/Access Point is 100 m (328 ft.).

Figure 6: *ITS4844A (866212) Synchronization Unit*

2.4.6 Power over ethernet switch

You use a PoE switch to provide power to the Access Points and remote antennas.

Figure 7: *Power over Ethernet Switch*

2.4.7 Uninterruptible power supply

The Smart-hopping infrastructure has several components that must be powered from an Uninterruptible Power Supply (UPS), including the APC, the PoE switch, the Sync Unit, and network switches and routers. The UPS supplies backup power to protect against hospital generator changeover interruptions and short power line transients.

The Philips UPS can be rack mounted (recommended) or placed free standing on a desktop.
Refer to Table 2-5 to when connecting Smart-hopping infrastructure devices to the UPS to ensure that you do not exceed the UPS' backup power capacity.

2.5 Network data flow

Data sent from the Patient Monitor to the Patient Information Center traverses the Smart-hopping network as follows:

1. The Patient Monitor sends its ECG data over the wireless link to a Smart-hopping Access Point.
2. The AP then "wraps" the ECG data into another message packet, with its destination as the Access Point Controller that is assigned to handle the management activities for that AP.
3. The wired network then treats the packet like a message to the APC.
4. The APC receives the packet, "unwraps" it and puts the message on the network.
5. The network forwards it on to the destination address of the Patient Information Center.

Data sent from the Patient Information Center to an Patient Monitor traverses the Smart-hopping network as follows:

1. The Information Center sends a message to the Patient Monitor IP address. The network "sees" the location of the Patient Monitor IP address as the location of the APC, and sends the message there.
2. The APC then looks at the message, determines which Smart-hopping Access Point is connected to the Patient Monitor it needs to send the message to, "wraps" the message into a packet and forwards the packet on to the appropriate Smart-hopping Access Point.
3. The network handles the packet as a message for the Smart-hopping Access Point.

4. When the packet arrives at the Smart-hopping Access Point, the Access Point “unwraps” the message, determines which Patient Monitor the message is intended for, and sends the message on to the Patient Monitor over the wireless link.

2.6 Defined bandwidth

The Patient Monitors and Smart-hopping infrastructure operate on the 1.4 GHz US Wireless Medical Telemetry Service (WMTS) band or on the 2.4 GHz band.

2.6.1 GHz bandwidth

In the United States, the Federal Communications Commission (FCC) has established the Wireless Medical Telemetry Service (WMTS) to promote interference-free operation of medical telemetry systems.
The Philips Smart-hopping network operates in the WMTS radio bands of 1395 – 1400 MHz and 1427 – 1432 MHz.

2.6.1.1 Standard WMTS channels

Generally, WMTS operations are accorded primary status over non-medical telemetry operations in 1395-1400 MHz and 1427-1429.5 MHz bands but are treated as secondary to non-medical telemetry operations in the 1429.5-1432 MHz band. Table 1 lists the standard primary and secondary 1.4GHz WMTS frequencies.

WMTS channel frequencies in the band 1395 to 1400MHz		
Channel 1	1395.9MHz	Primary WMTS Channel
Channel 2	1397.5MHz	Primary WMTS Channel
Channel 3	1399.1MHz	Primary WMTS Channel
Channel 4	1427.9MHz	Primary WMTS Channel
Channel 5	1429.5MHz	Secondary Channel, available only if not in use
Channel 6	1431.1MHz	Secondary Channel, available only if not in use

Table 1: Standard WMTS frequencies

2.6.1.2 Carved-out regions

The FCC has carved the following metropolitan regions out of the standard WMTS spectrum to protect operation of critical RF devices (e.g., radar, military and government communications, etc.):

- Pittsburgh, PA
- Metro Washington D.C.
- Richmond/Norfolk, VA
- Austin/Georgetown, TX
- Battle Creek, MI
- Detroit, MI
- Spokane, WA

In these seven areas, in contrast to the rest of the US, the FCC has specified that for WMTS and non-medical telemetry devices operating in the 1427 - 1432 MHz range the band be “flipped” as to which device type enjoys primary status.

Figure 8 illustrates the use of the 1427 - 1432 MHz band for the US and the designated carved out regions.

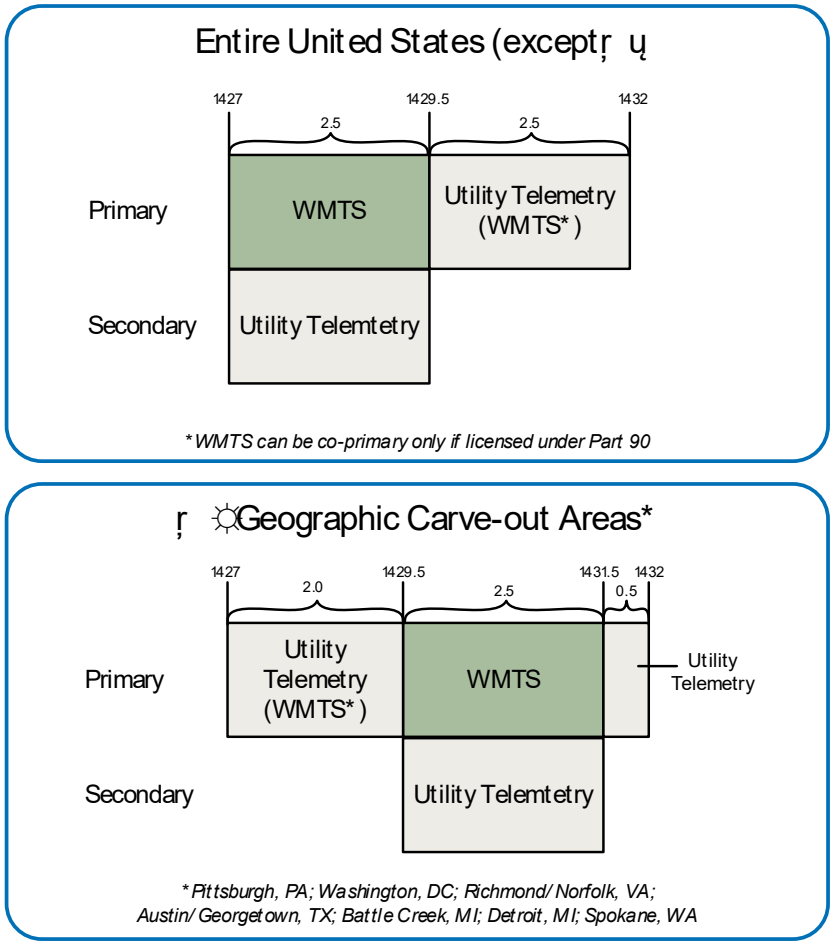


Figure 8: *Designated Use of WMTS Frequencies in the 1427 - 1432 MHz Band*

Table 2 lists the 1.4GHz WMTS channels available for use in “carved-out” regions.

WMTS Channel Frequencies in the Band 1395 to 1400MHz		
Channel 1	1395.9MHz	Primary WMTS Channel
Channel 2	1397.5MHz	Primary WMTS Channel
Channel 3	1399.1MHz	Primary WMTS Channel
WMTS Channel Frequencies in the Band 1427 to 1432MHz		
Channel 4*	1427.9MHz	Secondary Channel, only available if not in use
Channel 4a	1430.24MHz	Primary WMTS Channel

Table 2: WMTS frquencies in 'carved out' regions

*Channel 4 is not available when special “Carved-out” geographic area is selected as part of the APC configuration.

2.6.1.3 Required FCC registration

The FCC[1] requires that all wireless medical telemetry devices operation in the designated WMTS bands be registered prior to use.

As a convenience to our customers, Philips offers WMTS services to register wireless medical telemetry devices with the American Society for Healthcare Engineering (ASHE) on the customers behalf using the WMTS database administered by Comsearch.

2.6.1.4 Regulatory information

Description	Philips part#:	FCC ID:	Model#
1.4 GHz Smart-hopping Access Point	989803171211	PQC-4843B	ITS4843B
1.4 GHz Smart-hopping Access Point	989803171211	PQC-4843C	ITS4843C

Table 3: Smart-hopping 1.4 GHz Access Point regulatory information

2.6.2 2.4 GHz bandwidth

Outside the United States, the Smart-hopping network operates in the 2.4 GHz frequency space across 48 radio channels assigned from 2401.066 MHz to 2482.272 MHz, with a channel spacing of 1.728 MHz. Table 4 lists the 2.4 GHz channels.

2.4 GHz channel (for advanced selection)	Center frequency (GHz)	Approximate start frequency	Approximate stop frequency
0	2.401056	2.4002	2.4019
1	2.402784	2.4019	2.4036
2	2.404512	2.4036	2.4054
3	2.406240	2.4054	2.4071
4	2.407968	2.4071	2.4088
5	2.409696	2.4088	2.4106
6	2.411424	2.4106	2.4123
7	2.413152	2.4123	2.4140
8	2.414880	2.4140	2.4157
9	2.416608	2.4157	2.4175
10	2.418336	2.4175	2.4192
11	2.420064	2.4192	2.4209
12	2.421792	2.4209	2.4227
13	2.423520	2.4227	2.4244
14	2.425248	2.4244	2.4261
15	2.426976	2.4261	2.4278
16	2.428704	2.4278	2.4296
17	2.430432	2.4296	2.4313
18	2.432160	2.4313	2.4330
19	2.433888	2.4330	2.4348

[1] FCC regulations, Title 47: Telecommunications, Part 95: Personal Radio Services, Subpart H: Wireless Medical Telemetry Service (WMTS), Sections 95.1101-95.1129 (Frequency Coordination).

2.4 GHz channel (for advanced selection)	Center frequency (GHz)	Approximate start frequency	Approximate stop frequency
20	2.435616	2.4348	2.4365
21	2.437344	2.4365	2.4382
22	2.439072	2.4382	2.4399
23	2.440800	2.4399	2.4417
24	2.442528	2.4417	2.4434
25	2.444256	2.4434	2.4451
26	2.445984	2.4451	2.4468
27	2.447712	2.4468	2.4486
28	2.449440	2.4486	2.4503
29	2.451168	2.4503	2.4520
30	2.452896	2.4520	2.4538
31	2.454624	2.4538	2.4555
32	2.456352	2.4555	2.4572
33	2.458080	2.4572	2.4589
34	2.459808	2.4589	2.4607
35	2.461536	2.4607	2.4624
36	2.463264	2.4624	2.4641
37	2.464992	2.4641	2.4659
38	2.466720	2.4659	2.4676
39	2.468448	2.4676	2.4693
40	2.470176	2.4693	2.4710
41	2.471904	2.4710	2.4728
42	2.473632	2.4728	2.4745
43	2.475360	2.4745	2.4762
44	2.477088	2.4762	2.4780
45	2.478816	2.4780	2.4797
46	2.480544	2.4797	2.4814
47	2.482272	2.4814	2.4831

Table 4: 2.4 GHz channels

The 2.4 GHz channels available at a given installation site vary by geographic region as determined by the regulatory domain for that region. Table 5 lists the available 2.4 GHz channels and regulatory domain by geographic region.

Country/Region	Regulatory rule	Allowed ROW channels	Max Power EIRP from Antenna, dBm
Europe	ETSI	1-46	10 dBm
North America	FCC, RS-210	0-47	20 dBm
South America	ETSI	1-46	10 dBm
Japan	JAPAN, ARIB	1-47	12.14 dBm, Max Antenna gain is 2.14dB
Taiwan, Singapore, Hong Kong	FCC	0-47	20 dBm
Asia	ETSI	1-46	10 dBm
Australia/New Zealand	AUS/NZ	1-46	10 dBm
Africa	ETSI	1-46	10 dBm

Table 5: Available 2.4 GHz channels by geographic region

2.7 Supported topologies and system limits

Refer to the latest edition of the Network Design and Deployment Guide for detailed information about all supported IntelliVue Network topologies.

As an alternative to installing the Philips Smart-hopping infrastructure on a Philips-supplied network (PSN), you may install the Philips Smart-hopping infrastructure on customer-supplied network (CSN) infrastructure as described in “Deploying the Smart-hopping infrastructure on a Customer-supplied Network” on page 31.

2.7.1 Installing the smart-hopping infrastructure within a non-routed topology

In a non-routed Smart-hopping Network configuration, the Smart-hopping Network functions as an independent network. Figure 9 represents a Smart-hopping infrastructure installed in a non-routed configuration.

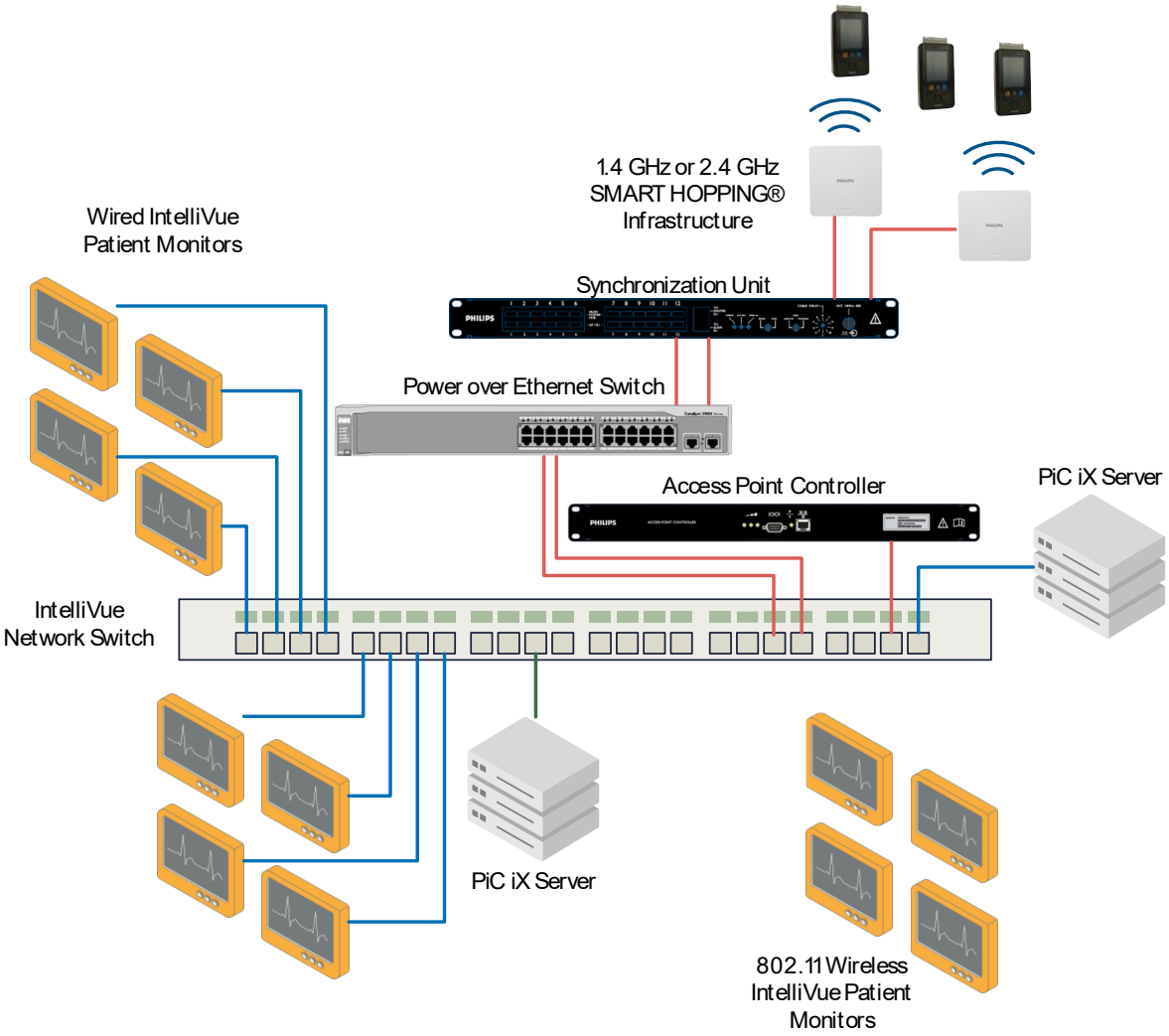


Figure 9: *Smart-hopping infrastructure Installed within a Non-routed Topology*

Note the following guidelines for installing the Smart-hopping infrastructure within a non-routed Smart-hopping Network topology:

- All Patient Monitors must reside on the network where the Smart-hopping infrastructure is installed.
- Up to 48 Smart-hopping Standard or Core Access Points may be installed on a non-routed Smart-hopping Network topology.
- Multiple Smart-hopping systems at a single hospital are supported only if the topology, configuration, and the Sync Network requirements listed in Appendix A are met.

Figure 10 illustrates supported and non-supported Smart-hopping infrastructure installations within a non-routed IntelliVue Network topology.

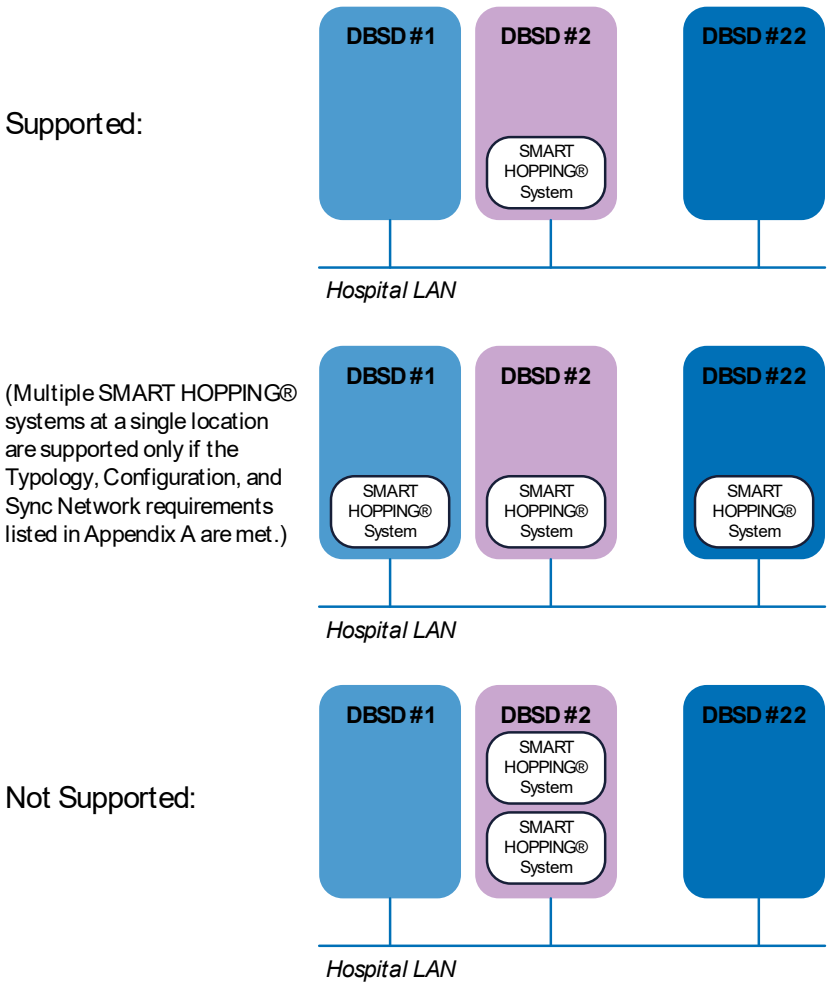


Figure 10: *Supported and Non-Supported Smart-hopping infrastructures for Non- routed IntelliVue Network Installations*

Refer to table 6 for a list of the device IP address assignments used in a non-routed IntelliVue Network configuration where the Smart-hopping infrastructure is installed on the IntelliVue Network subnet. Note the following regarding table 6:

- "n" represents the network number and starts at 0 for single IntelliVue Network deployments. This variable increments by 8 for each additional IntelliVue Network deployment. For example, for subnet 2, "n" equals 8, for subnet 3, "n" equals 16, and so on.

Device types (with non-routed subnet)	IP addresses subnet mask: 255.255.248.0	Default gateway
Network Subnet Address	172.31.n.0	Left Blank (0.0.0.0)
Reserved for Routed Solution	172.31.n.1 - 3	
Reserved for Service PC	172.31.n.4 - 9	IP Address of DBS or M3150 Information Center
Network Switches and Remote Client Infrastructure (i.e., Remote Client Router)	172.31.n.10 - 102	IP Address of DBS or M3150 Information Center
Reserved for Future Use	172.31.n.103 - 255	

Device types (with non-routed subnet)	IP addresses subnet mask: 255.255.248.0	Default gateway
1.4/2.4 GHz Smart-hopping APCs and IntelliVue 802.11 Devices	172.31.(n+1).0 - 63	IP Address of DBS or M3150 Information Center
IntelliVue 802.11 Devices	172.31.(n+1).64 - 127	
Reserved for Future Use	172.31.(n+1).128 - 255	
1.4/2.4GHz AP Static Range	172.31.(n+2).0 - 127	IP Address of DBS or M3150 Information Center
Bootp/DHCP Server Range 2 for Smart-hopping APs (configured in APC)	172.31.(n+2).128 - 255	IP Address of DBS or M3150 Information Center
Database server (NIC 1)	172.31.(n+3).0	
Application Server (NIC 1)	172.31.(n+3).16 - 31	IP Address of DBS or M3150 Information Center
Information Centers (NIC 1)	172.31.(n+3).32 - 63	IP Address of DBS or M3150 Information Center
Information Center Clients	172.31.(n+3).64 - 95	IP Address of DBS or M3150 Information Center
Printers (Set by BootP in DBS)	172.31.(n+3). 96 - 127	IP Address of DBS or M3150 Information Center
Reserved for Future Use	172.31.(n+3).128 - 255	
Patient Monitors/Devices (Wired & ISM 2.4 GHz Wireless)	172.31.(n+4).0 - 255	IP Address of DBS or M3150 Information Center
Reserved for Future Use	172.31.(n+5).0 - 255	
Bootp/DHCP Server Range 1 for 1.4/2.4 GHz Smart-hopping IPMs (config in APC)	172.31.(n+6).0 - 255	IP Address of DBS or M3150 Information Center
IntelliVue XDS PC	172.31.(n+7).0 - 254	
Network broadcast address	172.31.(n+7).255	

Table 6: IP address assignments for non-routed IntelliVue network subnet

Note the following guidelines for installing the Smart-hopping infrastructure within a routed ring topology:

- A Smart-hopping infrastructure subnet can be connected up to 22 IntelliVue Network subnets using routers.
- Up to 320 Smart-hopping Standard Access Points may be installed on a routed IntelliVue Network topology. Up to 600 Smart-hopping Standard Access Points may be installed with APC D.0 or greater.
- Up to 600 Smart-hopping Core Access Points and up to 1200 Remote Antennas (i.e., two per Access Point) may be installed on a routed IntelliVue Network topology for a total of 1800 cells with APC D.0 or greater. The limit of 320 Smart-hopping Access Points applied to older software versions.
- Smart-hopping Standard and Access Points may exist together on a routed IntelliVue Network topology so long as the maximum number of APs does not exceed 600.
- You may install the 1.4 GHz or 2.4 GHz Smart-hopping infrastructure within a routed IntelliVue Network topology.

Refer to table 7 for a list of the device IP address assignments used in a routed IntelliVue Network configuration where the Smart-hopping infrastructure is installed as a separate subnet to which up to 22 subnets have access using routers.

Note the following regarding table 7:

- "n" represents the network number and starts at 0 for single IntelliVue Network subnets. This variable increments by 8 from there for additional IntelliVue Networks. For example, for subnet 2, "n" equals 8, for subnet 3, "n" equals 16, and so on.

- Route statements are generated (in instances with a Router) at the completion of the Config Wizard.

Device types (with routed subnet)	IntelliVue Network Subnet IPs Mask: 255.255.248.0	Default Gateway	Smart-hopping Wireless Subnet IPs Mask: 255.255.240.0	Smart-hopping Default Gateway
Network Subnet Address (Used in Config Wizard for Router)	172.31.n.0		172.31.240.0	
Gateway Address	172.31.n.1		172.31.240.1	
Router A – <used for Wireless Subnet Router>	172.31.n.2		172.31.240.2	172.31.240.1
Router B – <used for Wireless Subnet Router>	172.31.n.3		172.31.240.3	172.31.240.1
Reserved for Service PC	172.31.n.4 - 9	172.31.n.1	172.31.240.4-9	172.31.240.1
Network Switches and Remote Client Infrastructure	172.31.n.10 - 102	172.31.n.1	172.31.240.10 – 20	172.31.240.1
Reserved for Future Use	172.31.n.103 - 255		172.31.240.21 – 172.31.240. 255	
Smart-hopping APCs			172.31.241.0 – 127	172.31.240.1
IntelliVue 802.11 Devices	172.31.(n+1).0 - 63	172.31.n.1		
IntelliVue 802.11 Devices and legacy Proxim (RangeLAN2/Harmony) APs. te: Proxim devices are not supported on PIC Release J (or higher).	172.31.(n+1).64 - 127	172.31.n.1		
Reserved for Future Use	172.31.(n+1).128 - 255		172.31.241.128 - 255	
Smart-hopping AP Static Range (1.4/2.4 GHz)			172.31.242.0 – 172.31.244.127	172.31.240.1
Smart-hopping APC Bootp/DHCP Server Range 2 for 1.4/2.4 GHz APs			172.31.244.128 - 172.31.246.255	172.31.240.1
Database Server (NIC 1)	172.31.(n+3).0 - 15	Default blank		
Application Server (NIC 1)	172.31.(n+3).16 - 31	172.31.n.1		
Information Centers (NIC 1)	172.31.(n+3).32 - 63	172.31.n.1		
Information Center Clients	172.31.(n+3).64 - 95	172.31.n.1		
Printers (Set by BootP)	172.31.(n+3). 96 - 127			
Reserved for Future Use	172.31.(n+3).128 - 255		172.31.247.0 - 255	

APs /Devices (Wired & ISM 2.4GHz) (Set By BootP)	172.31.(n+4).0 - 255			
Reserved for Future Use	172.31.(n+5).0 - 255			
Smart-hopping APC Bootp/DHCP Server Range 1 for IPMs			172.31.248.0 – 172.31.253.255	172.31.240.1
IntelliVue XDS PC	172.31.(n+7).0 - 254		172.31.254.0 – 172.31.255.254	
Network Broadcast Address	172.31.(n+7).255		172.31.255.255	

Table 7: Routed ring topology subnet and Smart-hopping infrastructure wireless subnet device IP addresses

2.7.2 System limits

Note the following important Smart-hopping system limits.

Smart-hopping infrastructure Device	Maximum Supported Rev. D.0 or later	Maximum Supported Rev. B.00 or C.00
Access Point Controllers	9 (includes one for redundancy)	9 (includes one for redundancy)
Access Points	600 (routed IntelliVue Network topology) 48 (non-routed IntelliVue Network topology)	320 (routed IntelliVue Network topology) 48 (non-routed IntelliVue Network topology)
Remote Antennas (Applies to 1.4 GHz only)	1200 (routed IntelliVue Network topology) 96 (non-routed IntelliVue Network topology)	640 (routed IntelliVue Network topology) 96 (non-routed IntelliVue Network topology)
Smart-hopping Wireless Clients (Patient Monitors)	1024 (routed IntelliVue Network topology) 128 (non-routed IntelliVue Network topology)	1024 (routed IntelliVue Network topology) 128 (non-routed IntelliVue Network topology)

Table 8: Maximum Smart-hopping infrastructure capacities

2.7.3 Deploying the Smart-hopping infrastructure on a customer-supplied network

If you will be deploying the Philips IntelliVue Telemetry System on customer-supplied network infrastructure, then you must follow all the requirements and specifications listed in the latest revision of the Philips IntelliVue Network Specification document, available on the Philips InCenter web site.

You must use a Philips supplied PoE Switch when deploying the Smart-hopping infrastructure with Smart-hopping Access Points.

Additionally, you should be aware of the requirements for assigning IP addresses to 1.4GHz or 2.4 GHz Smart-hopping Access Points on a customer-supplied clinical network.

Caution The device location value within a Smart-hopping infrastructure is based on an Smart-hopping AP IP address and is limited to the last ten bits. If an AP IP address is used whereby the 11th bit changes, unstable system behavior could occur. We recommend that you define the Smart-hopping subnet to be 255.255.240.0 for a routed network.

2.8 Smart-hopping infrastructure specifications

This section lists power, radio, and regulatory compliance specifications for the Smart-hopping infrastructure.

2.8.1 Power requirements

Device/ Component	Input Voltage	Manual Switching Required	Input Frequency (Hz)	Dissipated Power (Max)
Standard or Core Access Point	48 VDC Nominal (44 -52) VDC 287 mA (PoE standard - auto sensing PoE that is IEEE 802.3af compliant)	No	DC	≤ 13.8W
SYNC Unit	88-264 VAC	No	47-63	≤ 10W/18VA
Access Point Controller	88-264 VAC	No	47-63	≤ 10W/40VA

Table 9: Smart-hopping infrastructure component power requirements

UPS Requirements	Parameter Specification	
Input Voltage	1.4 GHz	2.4 GHz
	120VAC +/-10%	100, 120, 127, 220, 240 VAC ± 10%
Input Frequency	60Hz +/-3Hz minimum	50, 60Hz +/-3Hz
UPS AC Input Port	100, 120VAC model: one NEMA 5-15P plug. 230 VAC model: one IEC 320 C14 plug.	
Number of UPS AC output ports	100, 120VAC model: 3 minimum (NEMA 5-15R output receptacles), desirable to have 5 ports or greater. 230V model: 3 minimum (IEC 320 C13 output receptacles), desirable to have 5 ports or greater.	
Power delivery	UPS shall provide at least 225Watts for > 90 seconds to power connected equipment.	
Power Fail Transition	UPS must be responsive to power fail conditions such that the Smart- hopping system does not experience reboot due to transition to temporary battery backup power.	
Power Fail Alert	UPS shall provide local auditory response to power fail conditions.	
EMI Filtering	Provide AC line EMI filtering over 100KHz to 30MHz on UPS ports.	
EMC	FCC part 15 class A or B certification, CE Mark: CISPR 22/ EN 55022, and CISPR 24/EN 55024.	
Safety	UL certification, EN 62040 (Low Voltage Directive).	
Mounting	Rack Mounting is preferred.	

Table 10: UPS specifications

2.8.2 Safety regulatory compliance

Safety Specification	Compliant Device/Component
Information Technology Equipment - Safety UL 60950-1	1.4 GHz Access Points, 2.4 GHz Access Points, APC, and Sync Unit, PoE Unit, Switches, Routers, UPS.
Fire Safety	1.4 GHz Core Access Points, 1.4 GHz Remote Antennas, and 2.4 Access Points, are Listed for use within “Other Spaces Used for Environmental Air (Plenum)” per NFPA70: 2011, Article 300.22. Note: The term “plenum” as used in Article 300.22 Section C correlates with the use of the term “plenum” in NFPA 90A-2009, Standard for the Installation of Air- Conditioning and Ventilating Systems, and other mechanical codes where the plenum is used for return air purposes, as well as some other air-handling spaces. The area above dropped ceilings is an example of plenum space.
Standard for Uninterruptible Power Supply Equipment UL 1778	UPS.

Table 11: Smart-hopping infrastructure safety standard compliance

2.8.3 Environmental specifications

For EMC purposes component parts of the system conform to the requirements of EN60601-1-2.

In general, the Smart-hopping infrastructure is designed for use in an indoor environment and operates over an ambient temperature range of 0° to 55° C, excluding the Patient Monitor.

The Access Point, Sync Unit, APC, and Power over Ethernet Unit, and switches are all classified as Information Technology Equipment (ITE) devices.

Environmental Test	Test Type & Limits	Applicable System Element
Operating Temperature	0° to 55° C	Standard and Access Points, Remote Antennas, Sync Unit, APC
Operating Humidity	< 95% RH at 40°C (104°F)/ non-condensing	Standard and Access Points, Remote Antennas, Sync Unit, APC
Storage Temperature	-40° C to 60° C	Standard and Access Points, Remote Antennas, Sync Unit, APC
Storage Humidity	< 90% RH at 60° C	Standard and Access Points, Remote Antennas, Sync Unit, APC

Environmental Test	Test Type & Limits	Applicable System Element
Altitude (Operating and Non-operating)	3,048 meters (10,000 ft)	Standard and Access Points, Remote Antennas, Sync Unit, APC

Table 12: Smart-hopping infrastructure environmental specifications

2.9 Smart-hopping infrastructure product numbers

Table 13 lists the key product numbers associated with the Smart-hopping infrastructure.

Device/Option	Product Number/ Option Number
Model ITS3171A Access Point Controller	865346
ITS4844A Synchronization Unit	866212
Model ITS4843B/C 1.4 GHz Core Smart-hopping Access Point	989803171211 866394
Model ITS4846A IntelliVue Remote Antenna	865052 867151 (compatible with the Smart-hopping 2.0 Access Point)
Model ITS4852A 2.4 GHz Smart-hopping Access Point	989803171221
Smart-hopping 2.0 Access Point 1.4 GHz	867216
Firestop Putty Discs (package of 32 discs)	453564931011

Table 13: Smart-hopping infrastructure product numbers

2.10 New Smart-hopping hardware features

2.10.1 Smart-hopping 2.0 Access Points

Philips now offers the Smart-hopping 2.0 Access Point (part number 867216) as a replacement to the 866394 Smart-hopping 1.4 GHz Access Point.

2.10.2 Firestop putty discs (optional)

Philips offers firestop putty discs to use when installing Access Points and Remote Antenna ceiling mounting kits. These discs wrap around a cable or antenna whip and adhere to a ceiling tile, preventing smoke from penetrating the holes in the tile created during installation.

Figure 11: Firestop putty disc

Refer to the Smart-hopping 2.0 Access Point Installation guide (available on the Philips InCenter web site) for instructions on installing the Firestop putty discs.

2.10.3 Remote Antennas (for 1.4 GHz core Access Points)

A new 1.4GHz Remote Antenna is now available (part number 867151). You can find installation and service information on this remote antenna in a new manual, the Smart-hopping 1.4 GHz Remote Antenna Installation Guide. This manual is also part of the Smart-hopping infrastructure documentation portfolio.

2.11 New Smart-hopping software features

2.11.1 Smart-hopping 2.0 upgrade tool

The Smart-hopping 2.0 Upgrade Tool is software used to upgrade Smart-hopping 2.0 Access Points and Access Point Controllers. Philips plans to replace the current Upgrade Tool with this version once all of the Smart-hopping infrastructure upgrades are complete.

2.11.2 Updates to APC revision D.02 software

APC software revision D.02 adds or updates the following features and components:

- Security Enhancements and Vulnerability Fixes-
    - APC serial port is password protected
    - APC web browser interface is password protected
    - Web Communication Protocol can be set for HTTP or HTTPS

- Backup Primary APC Priority Level (0, 2) - this is located under the Static TCP/IP and APC Priority Settings main menu option. This feature allows you to configure a primary APC server and a backup primary APC to ensure continuous AP operation upon fail-over of the primary APC to backup primary APC (requires compatible APs).

2.11.3 Updates to APC revision D.01 software

These additional features have been added in Revision D.01:

- There is a new item under the main menu item, Static TCP/IP and APC Priority Settings:
    - Check APC network interface periodically - Ping the Gateway at one minute intervals and report an error after 5 minutes of continuous failure.

    - Serial based logging - Print out all log messages through the serial port.

    - Network based logging - This is a reserved feature for future debugging purposes. Use this to setup the IP address of a remote system to send APC log messages.

    - Flash based Error logging - Log task monitoring error messages to the APC flash.

    - Display Flash based Error logs - Read and display task monitoring error messages from the APC flash.

    - BACKUP this APC config files - Back up the APC configuration files to a backup directory.

    - RESTORE this APC config files - Restore the APC configuration files from a backup directory.

    - Network Logging IP Address - This is to setup a remote logging PC's IP address. This is a reserved feature for future debugging purposes.

2.11.4 Updates to revision D.00 software

These additional features have been added in Revision D.00:

- Client CI MULTICAST Spoof - This option allows configuration of the Smart-hopping wireless client CI (Connect Indication) Multicast address to either 224.0.23.63 or 224.0.23.173 (Philips registered Multicast IP address).
- APC MULTICAST Layer 3 - This option enables or disables the Layer 3 option.
- APC Client Gratuitous ARP - Enabling this option allows the Primary APC to generate Gratuitous ARP for clients during DHCP requests. The default setting is disabled. Disabling the option will prevent the Primary APC from providing Gratuitous ARP for clients during DHCP requests.
- Acquire GATEWAY Physical Address (MAC) - This option forces the APC to acquire a Gateway MAC address, which is needed for Layer 3, if the APC was set up prior to the network set up or if the physical Gateway changes.

Note Although the following items appear in the APC serial menu, they are not supported at this time:

- This APC for Mastership Contention - Any APC is allowed to contend for Mastership by default. This option disables Mastership Contention on an APC.
- APC Service Mode - This option minimizes the impact to live monitoring when rebooting or working on the Primary APC by redirecting traffic to the Secondary APCs.
- Snapshot Primary APC current running config - This option saves a copy of the current configuration of the Primary APC. A reboot of the Primary will not disrupt the system. The snapshot does not persist after rebooting.
- SAFE Reset Primary Access Point Controller - This option performs the same function as Snapshot Primary APC current running config and then reboots the Primary APC.

3 Planning your deployment

Locating the Smart-hopping Access Points and supporting infrastructure to assure full coverage for all wireless clients requires careful site planning.

This chapter provides information and procedures that must be followed to ensure a successful IntelliVue 1.4 GHz or 2.4 GHz Smart-hopping infrastructure deployment including:

- General Smart-hopping infrastructure Site Planning Guidelines
- Performing a Physical Space Assessment
- Planning the Sync Network Layout
- Planning Your AP Groupings
- Performing an RF Frequency Survey
- Assigning 2.4 GHz Smart-hopping infrastructure Channels
- Completing Installation Worksheets

3.1 General Smart-hopping infrastructure site planning guidelines

Patient Monitors with a wireless network connection have their advantages, however the flexibility the wireless link offers is not without its challenges. The reliability and quality of the wireless signal transmission through the air and hospital walls are governed by a number of variables that can be difficult to control. A wireless network connection is not as dependable as a wired network connection.

The effect of low signal strength and interference on the display of the patient information from a wireless Patient Monitor at the Philips Information Center server can range from a momentary data loss to a lengthy period of data loss. Monitoring continues local to the IntelliVue monitor in cases where a wireless network signal is disconnected between the IntelliVue monitor and the Philips Information Center server.

Before installing the Smart-hopping infrastructure as part of an IntelliVue Network deployment, you must complete the following site planning tasks:

- Establish a coverage area agreement.
    - Define the desired coverage area within the hospital.

- Perform a physical site assessment and consider building materials and construction which can affect RF properties.
    - Determine how many Patient Monitors are required.
    - Apply radius-of-coverage circles to the site floor plan to define optimal AP installation locations.
    - Add additional APs to cover other high-density wireless client areas if needed.
    - Determine the number of Access Point Controllers required to support the installation.
    - Evaluate the availability and location of equipment rooms and possible locations for PoE Switches, APCs, and Sync Units.
    - Specify the cable runs between Smart-hopping infrastructure devices.

- Define the number of Uninterruptible Power Supplies required to support the Smart-hopping infrastructure installation.

- Define the Sync Unit Network required to support the number of APs to be installed. If there are multiple Smart-hopping systems in the hospital, then they may need to synchronized together. See “Installing Multiple Smart-hopping systems at a Single Hospital Site” for details.

- Plan your AP Groupings.

- On a Philips-supplied network with redundant Core routers and Distribution Layer switches, and primary APC is connected to the Philips Supplied Network Distribution A switch, a flooding situation can occur on the network, causing an increase in broadcast network traffic. In this network state,

when Upgrader.exe is run the APs may become unresponsive to the upgrade command and either do not upgrade or take many retries to complete. To prevent this situation, install all APCs on the Distribution Layer switch B or on any Access Layer switch and make sure all APs are assigned to AP groups and that AP groups are associated with a specific APC. Make sure no APs are part of the Smart-hopping AP group.

- If you are installing the 2.4 GHz Smart-hopping infrastructure or IntelliVue short-range radio, perform an RF frequency survey.
    - Understand RF co-existence issues in the hospital environment.
    - Determine available channels. Use a spectrum analyzer tool to identify RF channels in use and possible interference. Capture and store the spectrum analysis data.
    - Assign channels to APs to avoid interference.

3.2 Performing a physical space assessment

Prior to designing an infrastructure for your deployment, you must first determine the coverage area. Assessing the physical space at the Smart-hopping infrastructure deployment site requires that you:

- understand the radius of coverage provided by 1.4 GHz and 2.4 GHz Access Points
- determine the number of Patient Monitors to be deployed
- determine optimal AP installation locations
- determine the number of APCs required to support the APs to be deployed
- locate IT equipment closets
- plan cable runs between Smart-hopping infrastructure devices
- determine the number of UPS units required to support the Smart-hopping infrastructure deployment

3.2.1 Understanding the radius of coverage (RoC) metric

The radius of coverage (RoC) is the area for which a given access point can provide RF coverage. Graphically, this is represented as a circle with the AP at its center. In reality, the actual area of acceptable coverage has been demonstrated to be an irregular shape, formed in large part by site structure such as walls, elevator shafts and other materials that affect RF coverage. However as a starting point, a simple circle can often be effectively used to represent coverage for a given AP.

The Smart-hopping infrastructure design goal is to blanket the desired coverage area such that wireless clients might move and be used throughout this area without losing network connectivity. The actual usable radius of coverage value depends on the building layout and construction techniques. Table 14 lists the RoC values for Smart-hopping Access Points and Remote Antennas.

Site Layout Type	Example	Radius of Coverage Values to Use for Site Planning and Design	
		1.4 GHz Standard AP, Access Point, or Remote Antenna, and 2.4 GHz AP (ETSI, ARIB, or AS/NZ Mode)	2.4 GHz AP (FCC or RSS-210 Mode)
Typical Patient Room Area	Hospital wing area with concentrated patient rooms and newer building construction. The RoC values listed at right are conservative values that apply to typical deployment sites.	32 feet (9.8 m)	60 feet (18.3 m)

Dense, congested area/RF impermeable materials	Sites built with materials known to absorb RF energy require that a smaller RoC be used for design. Experience has found that older hospitals with more block, brick, metal lathe and plaster and/or tile construction do not allow RF signals to penetrate walls as well as those with newer drywall and metal stud construction. Also, sites in earthquake prone areas with more reinforced concrete wall construction also absorb more RF energy and need a smaller RoC used for design. Large metal objects (LMOs) also degrade RF signal propagation. These could be in an area with elevator shafts or lead lined walls such as found in X-Ray imaging areas.	30 feet (9.1 m)	50 feet (15.2 m)
Open air/LOS	Open “line of sight” (LOS) environment such as a long hallway corridor or open ward with no walls. Note that when installing Access Points, an Access Point alone (without connected Remote Antennas) will generally provide sufficient coverage for a LOS area.	60 feet (18.3 m)	100 feet (30.5 m)

Table 14: Radius of coverage values for Smart-hopping Access Points

3.2.2 Determining the number of wireless clients to be supported

The number of wireless clients to be used in the desired coverage area will have an impact on the overall system design. Sites will use as many IPMs as there are beds in the coverage area, or some number fewer than that.

Note We recommend that you use an Access Point alone (without connected RAs) to provide coverage to a Radius-of-Coverage cell that has a high density of wireless IPMs. Add additional Access Points to cover other high-density wireless IPM areas if needed.

Note these limits when determining the number of wireless IPMs to be supported.

Smart-hopping infrastructure device	Maximum Supported
Total Number 1.4 GHz or 2.4 GHz Smart-hopping infrastructure wireless clients	128 (non-routed IntelliVue Network topology) 1024 (routed IntelliVue Network topology)
Device Density: Maximum wireless clients per AP	Each Standard 1.4/2.4 GHz AP supports up to 18 wireless clients. An Access Point alone supports 18 wireless clients. When used with a single RA, the Access Point supports nine wireless clients and its connected RA supports nine wireless clients (9+9=18). When used with two RAs, the Access Point supports six wireless clients and its connected RAs each support six wireless clients (6+6+6=18).

Table 15: Maximum numbers of wireless clients supported

3.2.3 Determining AP installation locations

The Smart-hopping infrastructure design goal is to blanket the coverage area with overlapping coverage cells such that Patient Monitors might move and be used throughout this area without losing network connectivity.

When determining where to install the APs, give priority to the areas where patients spend the majority of their time.

Use an up-to-date hospital floor plan to determine the desired coverage areas taking into consideration any past coverage issues with existing equipment, areas with rooms deeper than 28 feet or hallways wider than 8 feet and construction issues which can affect wireless signals.

In the ideal system, the number of walls that the RF signal must penetrate should be minimized. Since wall penetration is a requirement in all covered areas, the AP should be placed on the side of the wall where the patient (and Patient Monitor) spends the majority of the time. At the same time, the AP installation location should maximize the amount of covered area. These objectives are sometimes diametrically opposed. A rule of thumb to designing an optimal system is to limit the wall penetrations for any given AP-to-IPM connection to one. The following sections describe the best employment of this approach for two common types of patient room layouts.

3.2.3.1 Seamless roaming

To provide seamless roaming, adjacent Access Points must be positioned close enough to each other such that the coverage area of Access Points overlaps.

This overlapping area has two very important attributes. Any IPM situated in the overlapping area can associate and communicate with either Access Point; and any IPM can move seamlessly through the overlapping coverage areas without losing its network connection. This attribute is called seamless roaming.

3.2.3.2 Traditional hallway patient room layout

In Figure 12, patient rooms lie on either side of the hallway. With traditional corridor widths of approximately 10 to 12 feet (3 to 3.6 m), and patient room depths of 12 to 18 feet (3.6 to 5.5 m), covering a wing side-to-side with APs placed along the hallway centerline appears feasible (for a 32-foot (9.8 m) RoC). In many cases, this method has been employed successfully, but not in every case. Sites with dense wall construction (typically older hospitals, high rise hospitals and/or hospitals built to earthquake codes) often do not perform well using this method, especially if there are bathrooms located in the outside edges of the patient rooms. As RF penetration decreases at these types of sites, the typical method to achieve coverage is to reduce the AP spacing in the hallway and add more APs. This sometimes works, but places the concentration of APs in an area where the patient will not spend much time, the hallway.

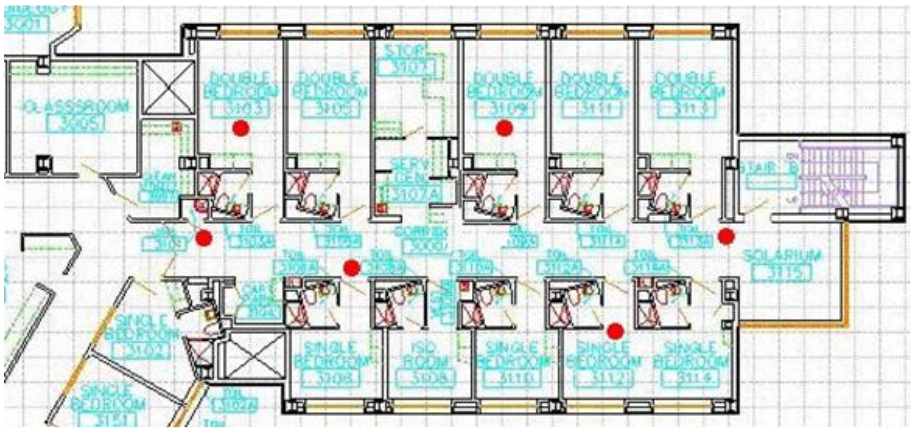


Figure 12: AP placement for a traditional room layout

The analysis of coverage for hallway-placed APs is quantized quite simply to how many pairs of rooms one AP can cover. Two to three pairs (4 to 6 rooms) is typical. In cases where only one pair can be covered, you may want to consider placing APs in every other room alternating side-to-side along the corridor.

3.2.3.3 Non-linear patient room layout

More common in newer hospital designs, are layouts where the patient rooms are placed along the outside of the structure, and non-clinical, administrative areas are clustered in the central areas. This creates an asymmetry in the floor plan relative to the location of the hallways and the patient rooms. In these cases, placing the APs in the hallway becomes far less desirable as there is no advantage to covering multiple patient rooms from an AP placed outside of the patient rooms. The “one wall” rule would dictate placing the APs in the patient rooms in this type of layout.

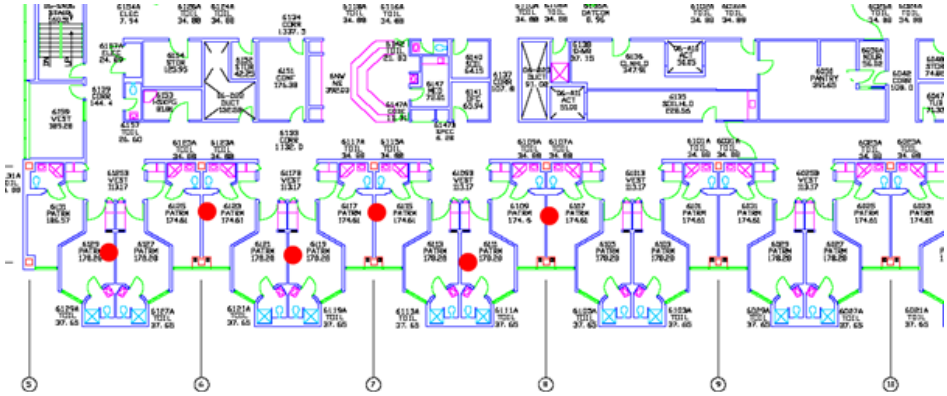


Figure 13: AP *Placement for a Non-linear Room Layout*

The “one wall” rule as applied to this layout would allow for AP coverage in hallways where the patients ambulate as well.

3.2.3.4 Placing RoC cells on a floorplan

Figure 14 shows an example of how 1.4 GHz Smart-hopping infrastructure AP installation locations were determined by placing Radius-of-Coverage circles and a Line-of-Sight circle on a floor-plan to blanket the coverage area with overlapping coverage cells such that Patient Monitors might roam throughout this area without losing network connectivity.

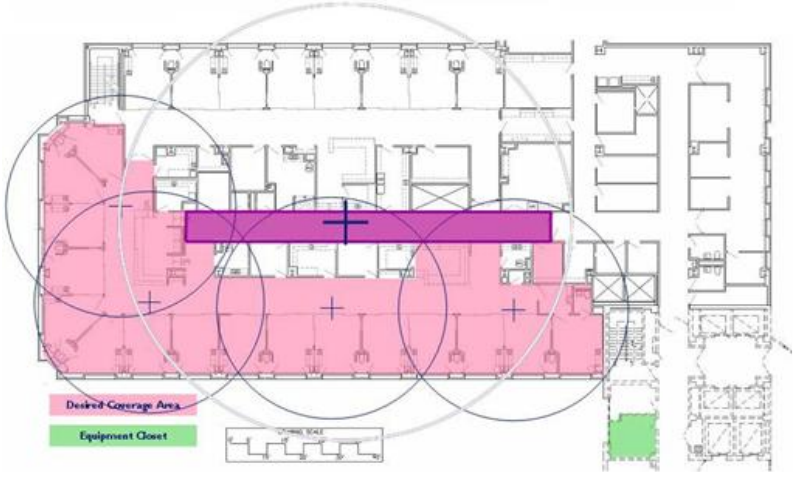


Figure 14: *Placing RoC Coverage Circles on a Floor Plan*

For the example shown in Figure 14, a 32 ft. RoC was used for the Access Points that provided coverage to patient rooms, and a 60 ft. LoS was used for the AP providing coverage to the hallway.

3.2.3.5 Access Point placements

Smart-hopping Access Point implementations differ minimally from standard AP implementations. The primary difference is rather than an individual “home run” UTP cable from each standard AP, only one UTP run is made for each Access Point—from the Access Point to the supporting POE/Sync infrastructure. The Remote Antennas connect directly to the Access Point via a 74-foot (22.6m) coaxial and unshielded twisted pair (UTP) cable bundle.

Spacing between the Access Point and Remote Antennas is limited to the length of the UTP/coax cable bundle—74 feet (22.6m). The cable assembly, is pre-terminated when manufactured and cannot be shortened. The actual Access Point-to-Remote Antenna spacing will vary depending on the dimensions of the area to be covered at a given installation site.

The Access Point can be deployed using two installation methods, linear or interleaved. Regardless of which installation method you use, you must manage the Remote Antenna port assignments on each Access Point such that RAs with the same Access Point port assignment are not installed adjacent to each other. This restriction must be considered in both two (i.e., Access Points installed on the same floor) and three (i.e., Access Points installed on adjacent floors) dimensions. This restriction exists to ensure proper time slot allocation. In the following figures, the port assignment for each RA is listed.
In linear deployments, the component Access Point devices are laid end to end while maintaining an even spacing between devices.

Figure 15: *A Linear Access Point Deployment*

In interleaved deployments, the RAs are located in between an adjacent Remote Antenna and its Access Point, resulting in an “overlap” of the Access Points. An interleaved design builds in some fault tolerance/redundancy to the RF coverage area.

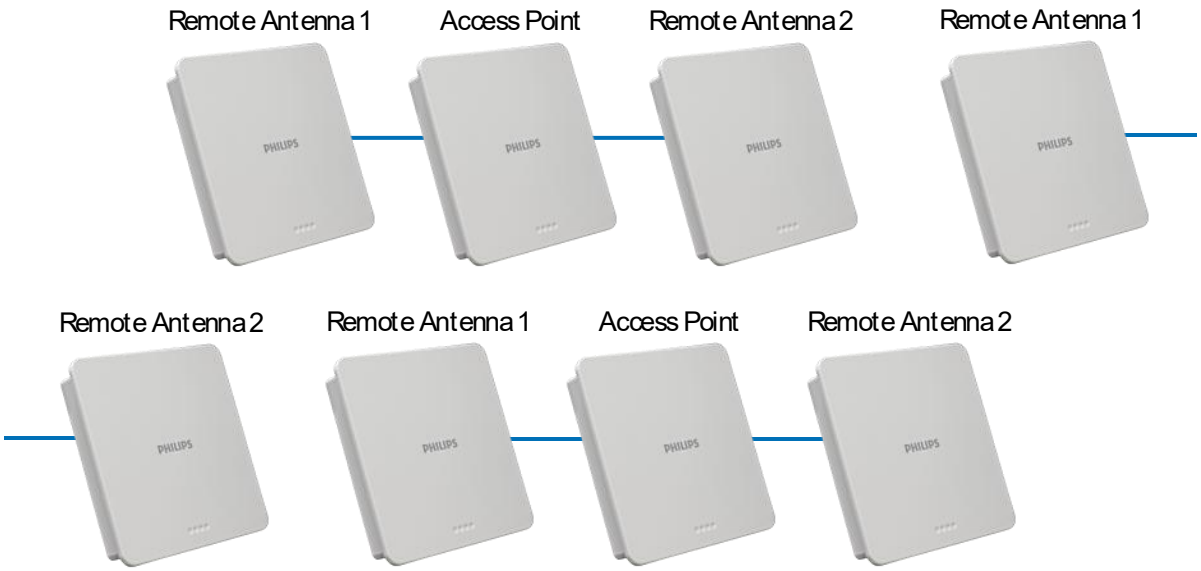


Figure 16: An Interleaved Access Point Deployment

The following figures represent various possible Access Point deployments.

Figure 17 shows a single Access Point deployment. This deployment may be made with either none, one, or two remote Antennas.

Figure 17: A Single Access Point Deployment

Figure 18 shows a multiple, linear Access Point deployment.

Figure 18: Linear Multiple Access Point Deployment

Figure 19 shows a multiple, interleaved Access Point deployment.

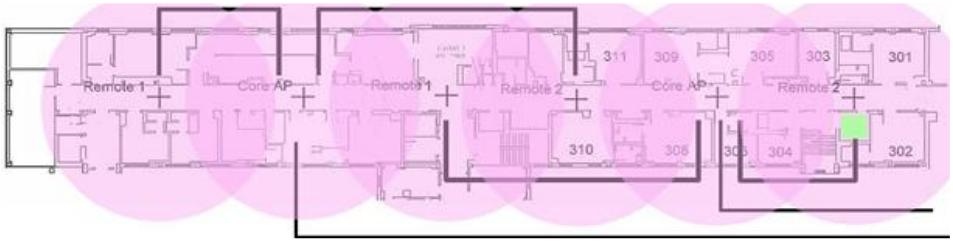


Figure 19: Interleaved Multiple Access Point Deployment

Figure 20 shows 1.4 GHz Smart-hopping infrastructure Standard APs and Access Points deployed together.

Figure 20: Mixed Standard and Access Point Deployment

3.2.3.6 Access Point placement guidelines

Note the following important guidelines when locating Smart-hopping Access Points:

- AP antennas must be more than four inches (10 cm) away from metal structures. If the antennas are too close to the structure, antenna performance can be degraded.
- Each Smart-hopping Standard Access Point can handle communication with up to 18 wireless clients.
- An Access Point alone supports 18 wireless clients. When used with a single RA, the Access Point supports nine wireless clients and its connected RA supports nine wireless clients (9+9=18). When used with two RAs, the Access Point supports six wireless clients and its connected RAs each support

six wireless clients (6+6+6=18).

- We recommend that you use an Access Point alone (without connected RAs) to provide coverage to a Radius-of-Coverage cell that has a high density of wireless clients. Add additional Access Points to cover other high-density IPM areas if needed.
- APs or Remote Antennas shall not be placed closer than three feet (1 m) together to prevent signal overload conditions.
- Smart-hopping Access Points require a 100 Mbps/Full Duplex switch port connection.
- Try to avoid placing APs and RAs close to other electrical devices (exit lights, light fixtures, speakers, etc.). Things like florescent light ballasts can create a significant amount of interference that can impact system performance.
- Locate Smart-hopping Access Points a minimum of six feet (1.8m) from 802.11 APs.
- Locate APs at least 6 ft (1.8 m) from phone base stations.
- Locate APs at least 20 ft (6 m) from microwave ovens.
- Orient the antennas on Smart-hopping 1.0 APs so that they are straight and perpendicular to the floor.
- Smart-hopping 2.0 Access Points utilize internal antennas that are located under the face of the AP. For optimal performance, use one of the approved mounting alternatives (for more information on mounting options, see the Smart-hopping 2.0 Access Point 1.4 GHz Installation Guide, available on the Philips InCenter web site) to mount the AP to the wall, below the ceiling or flush with the ceiling.

3.2.4 Determining the required number of APCs

Once the number of required Access Points is known, calculate the number of Access Point Controllers needed and determine their location. When determining the number of APCs required, follow these guidelines:

- No more than 40 APs should be supported by a single APC for systems running APC Release B.00 or C.00.
- No more than 75 APs should be supported by a single APC for systems running APC Release D.00 or later.
- No more than 9 APCs should be installed in a system (i.e., 8 APCs fully loaded and 1 APC for redundancy) when installing the Smart-hopping infrastructure.
- We REQUIRE redundancy (this applies to APC redundancy and network redundancy) if the Smart-hopping infrastructure:
    - has greater than 32 IPMs in operation, or
    - has greater than sixteen 32 ft. (9.8m) cells of coverage, or
    - has greater than eight 60 ft. (18.3m) cells of coverage.

If any of these three conditions exist, the Smart-hopping infrastructure should be designed such that a single point of failure will not result in more than 32 Smart-hopping patients losing monitoring.

Refer to table 16 and table 17 for guidance in determining the number of APCs required for your system.

With Redundancy: REQUIRED if: Total Number of IPMs > 32 OR Number of 32 ft. (9.8m) Cells of Coverage > 16 OR Number of 60 ft. (18.3m) Cells of Coverage > 8 OR Using Routed Network Topology

Number of Access Points for APCs running B.00 or C.00	Number of Access Points for APCs running D.00 and later	Minimum Number of APCs	Minimum Number of APCs for Backup Primary APC Feature (Requires Version D.02 or Higher)	Maximum Number of APCs
1 to 40	1-75	2	3	9
41 to 80	76-150	3	4	9
81 to 120	151-225	4	5	9
121 to 160	226-300	5	6	9
161 to 200	301-375	6	7	9
201 to 240	376--450	7	8	9
241 to 280	451-525	8	9	9
281 to 320	526-600	9	9	9

Table 16: Required number of APCs in redundant system

APC software version D.02 offers a new feature for APC redundancy and fail-over - configuring APCs as primary, backup primary, or secondary units. In the event of the failure of the primary APC, the backup primary APC takes over without disrupting operation of APs that it manages, or APs managed by secondary APCs. This feature requires at least three APCs that operate with software version D.02 to implement.

You can configure whether the APC is a primary, backup primary, or secondary using the APC serial console menu.

From the console menu, the Backup APC Priority Level for the Primary APC and the Backup Primary APC is set to 0. Set the Backup APC Priority Level value for all secondary APCs is to 2.

Additionally, the Backup Primary APC feature requires the following compatible AP hardware and software:

- 1.4GHz AP 2nd Generation Hardware and A.00.30 software
- 1.4GHz AP 3rd Generation Hardware and D.02.31 software
- 1.4GHz AP 4th Generation Hardware and E.00.XX software
- 2.4GHz AP 2nd Generation Hardware and D.02.31 software

Note First generation APs (both 1.4GHz and 2.4GHz) do not support the Backup Primary APC feature.

NO Redundancy: Allowed if: Total Number of IPMs <= 32 AND Number of 32 ft. (9.8m) Cells of Coverage <= 16 AND Number of 60 ft. (18.3m) Cells of Coverage < 8 AND Using Non-routed Topology	
Cells of Coverage	Minimum Number of APCs
1 to 16 (32ft. (9.8m)) Cells	1
1 to 8 (60 ft. (18.3m)) Cells	1

Table 17: Non-redundant system guidelines

3.2.5 Locating equipment closets

As part of the RF coverage assessment, you must locate the available IT equipment closets at the Smart-hopping infrastructure installation site.

The location of equipment closets is a relevant consideration as these closets will be used to house the supporting AP and IntelliVue Network infrastructure. For this reason, equipment closets must be located within 328 feet (100 meters) cable length of each Smart-hopping AP to be installed.

Equipment closets must house the IntelliVue Network switches, APCs, PoE Switches, and Sync Units. You should assess the needed or available rack space within each equipment closet at this time.

3.2.6 Planning cable runs

Smart-hopping APs require Power over Ethernet (PoE) network switches and Sync Units to support data connection, RF synchronization, and DC power. Note that in Figure 2-10, the maximum total cable length between the AP and switch is 100m (328 ft.). The devices are connected as shown in Figure 21.

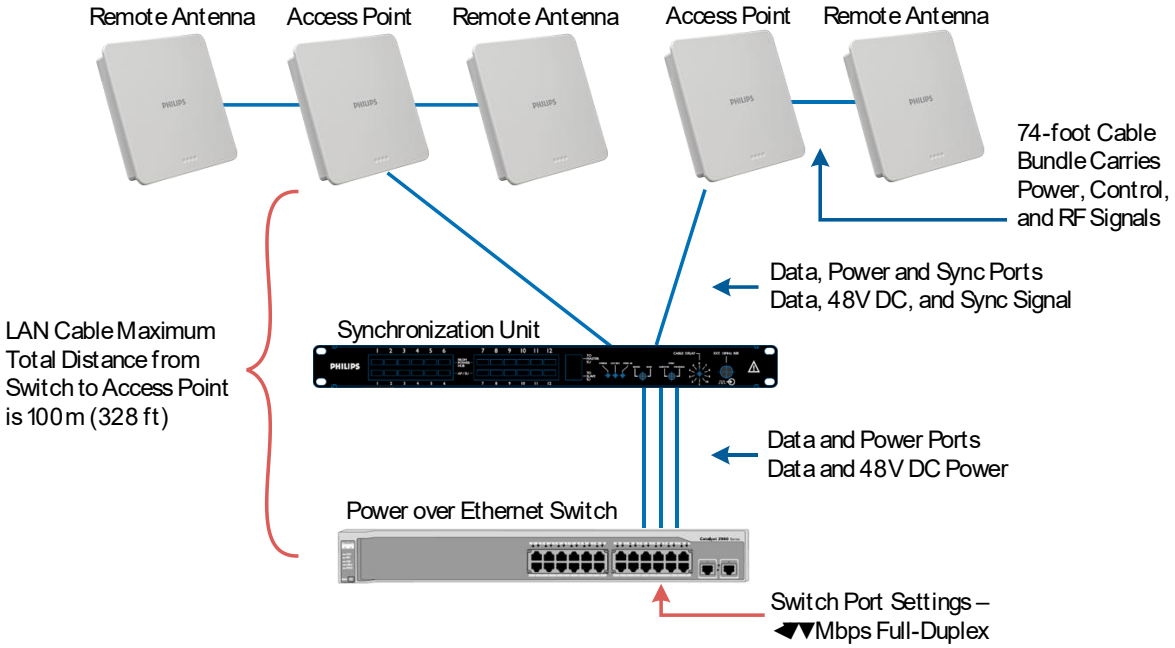


Figure 21: Maximum AP to Switch Cable Length

From a design perspective, careful analysis of the site layout, wire run options and equipment closet locations dictate the optimal Smart-hopping infrastructure layout. Ideally, each Sync Unit supports 12 APs, as each has 12 ports available on it. For this to be the case, the APs must all be located within 328 ft (100m) of the network switch to which they are connected, as the Ethernet wire run limitation for data cables applies. The Sync Units do not buffer and re- drive the data signals like other network devices.

3.2.7 Defining the UPS deployment

Because a reset of any of the Smart-hopping infrastructure devices can result in the loss of patient waveforms for several minutes, we require that the following Smart-hopping infrastructure devices be connected to an Uninterruptible Power Supply (UPS) and also be on emergency hospital power:

- Routers
- Network Switches
- Sync Units
- Access Point Controllers

When determining the number of UPS units required to support your planned Smart-hopping infrastructure deployment, consider the Smart-hopping infrastructure device power draws listed in Table 2-5.

Product Number	Device	Power in Watts
866212	Sync Unit	10 Watts
865346	APC	10 Watts

Table 18: Smart-hopping infrastructure device power draws

3.3 Planning the sync network layout

Design of a “Sync Network” is required for any site using more than one Sync Unit. A site may need more than one Sync Unit if:

- more than 12 APs are needed
- the geographical dispersion and/or location of available equipment closets dictate this
- multiple Smart-hopping systems are installed at a hospital (See “Installing Multiple Smart- hopping systems at a Single Hospital Site” for details)

The Sync Network is imperative to ensure that all RF channels are driven in Synchronization and no “drifting” occurs. While these connections are made using UTP/CAT5e (or greater) cabling like the other network connections, these are non-data connections that can be run up to 500 meters (1640 feet). Note that even Smart-hopping networks that support non-contiguous RF coverage areas must be synchronized if they are located at the same hospital site.

A Sync Unit can support up to 12 APs and can be configured as a Primary or a Secondary using its front-panel. It is also possible for a Sync Unit to act as a Primary to feed up to 13 Secondary Sync Units.The Primary Sync Unit is the unit at the head of the chain, or center of the topology and is used to generate the synchronization signal format to other Secondary Sync Units. Secondary Units act as regenerators to further distribute the signal if needed.

Note that there must be only one Sync Unit designated as a Primary, all others must be Secondary. Also, note that an Access Point cannot be operated from the ‘TO Secondary SU’ output on the Sync Unit. APs should only be connected to an “AP/SU” port that sources sync signal, power, and data.

The maximum number of Sync Units that may be linked in a single daisy-chain is 4 (including the Primary Sync Unit). Larger installations requiring more than four Sync Units will use a Star Sync Network that typically has the Primary Sync Unit located in the middle. Arms of the Star may each have chains of up to four Sync Units total.

There are three main Sync network layouts:

- Daisy-chained Sync Network
- Star Sync Network
- Hybrid Sync Network

3.3.1 Daisy-chained sync network

Figure 22 below shows one example of how PoE/Sync Unit/Network Switch stacks might be deployed using the daisy-chain method. Each PoE/Sync Unit/Network Switch stack could support up to 12 APs. The stack Sync Units are all connected by the Primary/Secondary Sync signal ports on their front panels, the uppermost stack containing the Primary Sync Unit.

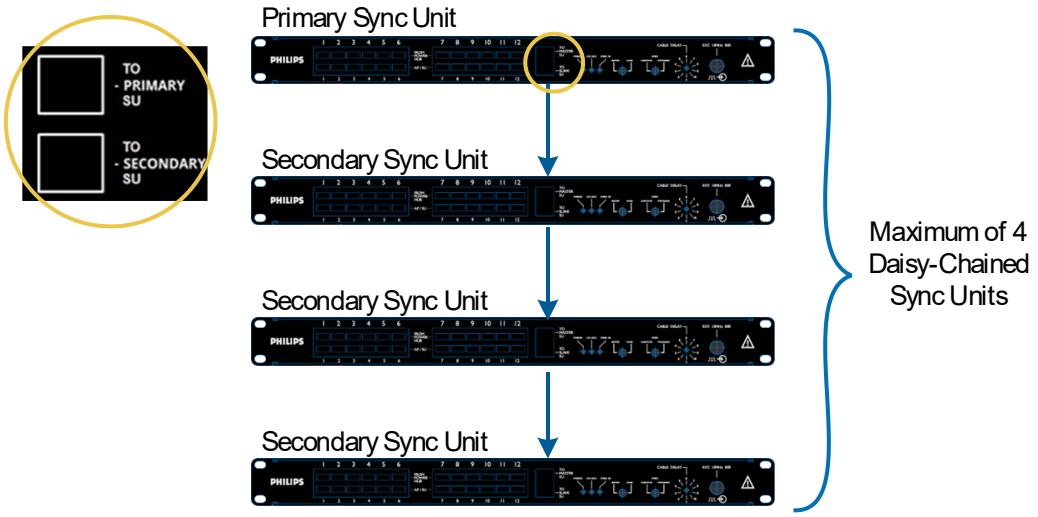


Figure 22: Daisy-chained Sync Network

3.3.2 Star sync network

In some cases, the daisy-chain topology of interconnecting AP infrastructures may not be desirable. If the best candidate for the Primary Sync Unit is centrally located and the Secondary Syncs are located radially around it, using a “star” topology approach to wiring Primary/Secondary Sync Units may be preferable.

In this methodology, the Primary Sync Unit supplies its signal out of its “AP/SU” ports to as many Secondary Sync Units as needed. The total number of Sync Units that can be driven by one Sync Unit is 13. The Sync cable connects to the “AP/SU” port of the Primary and to the “To Primary SU” port on the front panel of the Secondary Sync Unit.

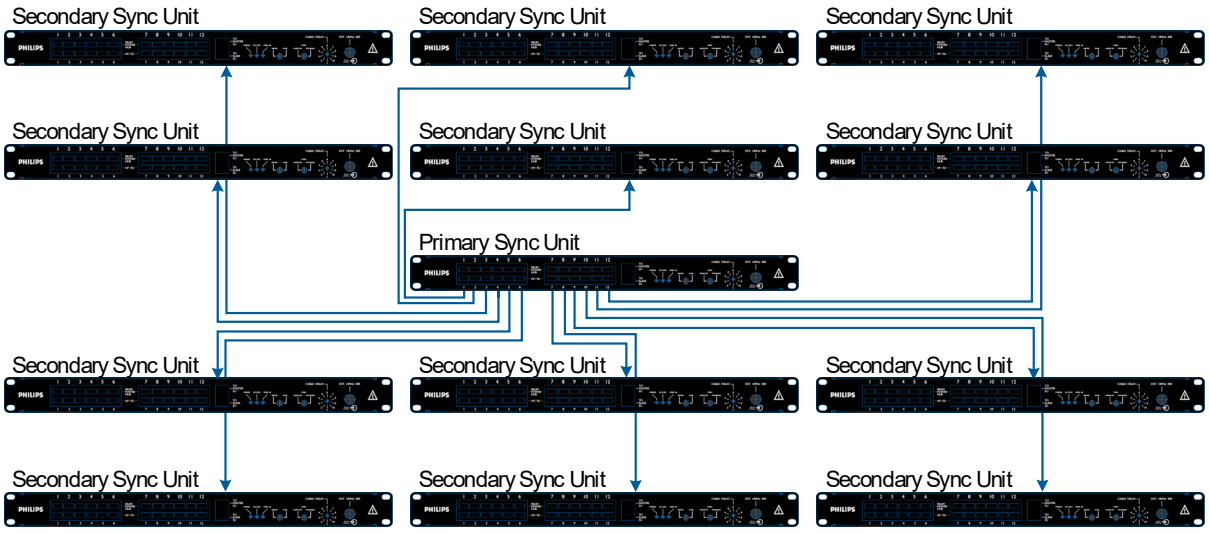


Figure 23: Star Sync Network

This topology, however, decreases the number of available ports on the Primary Sync Unit that may be used for APs. ‘AP/SU’ ports used to drive Secondary Sync Units may not be used for APs. Any combination of Secondary Sync Unit and Access Point connections can be made to these ports, up to the maximum of 13 (i.e., 12 Sync

Units connected to the AP/SU Ports and one connected to the “To Secondary SU” port), from any one Sync Unit.
Note also that in this “star” topology, the 'AP/SU' ports on the Primary Sync Unit must have their corresponding PoE ports connected to a PoE switch, or the synchronization signal will not be propagated to the Secondary Sync Unit. Also, the cable delay switch should be properly set for each Secondary Sync Unit.

3.3.3 Hybrid sync network

If you need more than the 144 AP connections provided by the star topology, then you can create a hybrid of the daisy- chain and star topologies (Figure 24).

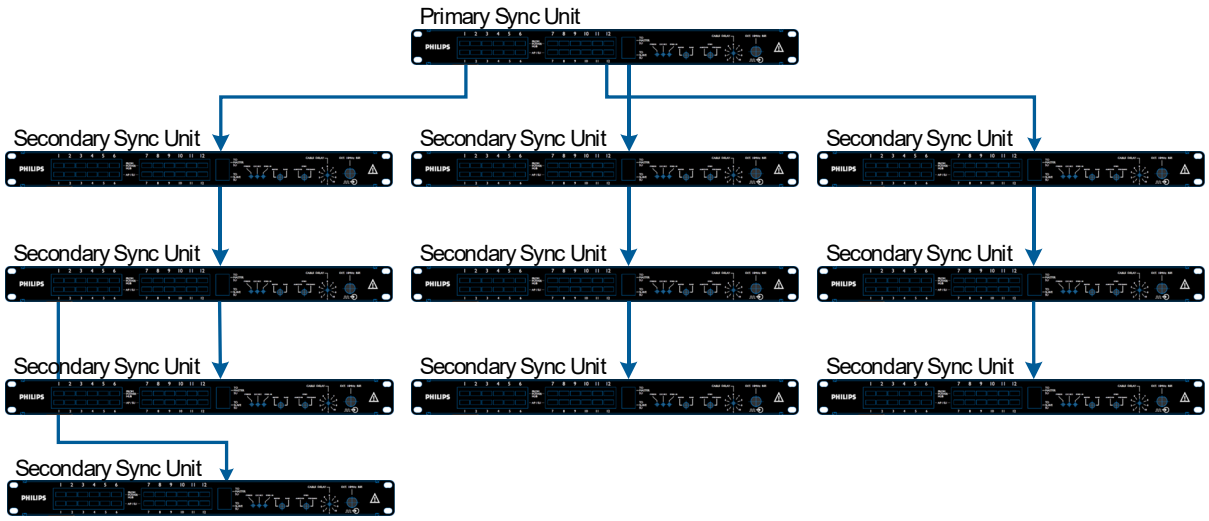


Figure 24: Hybrid Sync Network Topology

3.4 Sync toggle switch settings

Always on is only used on the Primary Sync Unit when it is only driving other Sync Units from the AP/SU ports. In this single configuration, it is not necessary to connect the corresponding From Power Hub ports to a POE switch.

If any of the AP/SU ports on the Primary Sync Unit are connected to an AP, then the Sync toggle switch is set to POE Enable, and for any port used to drive a downstream AP or Sync Unit, it is necessary to connect all of the corresponding *From Power Hub* ports to a POE switch.

On the Secondary Sync Units, the toggle switch is set to POE Enable, and for any port used to drive a downstream AP or Sync Unit, it is necessary to connect all of the corresponding From Power Hub ports to a POE switch.

3.5 Cable delay rotary switch settings

You must select a delay setting on the front panel of the Sync Unit using the Cable Delay rotary switch. The switch setting must correspond to the length of the cable connected the Sync Unit To Primary SU port (its Sync source may be the system Primary, or another Secondary Sync Unit in a daisy-chain implementation).

The delay switch setting on a Primary Sync Unit does not affect Smart-hopping infrastructure operation, but for consistency, always set it to 1. Set the Delay Switch on Secondary Sync Units as listed in table 19.

Cable Length	Sync Unit - Cable Delay Rotary Switch Position
0 to 50 meters (0 to 164 ft.)	1
>50 to 100 meters (164 to 328 ft.)	2
>100 to 150 meters (328 to 492 ft.)	3
>150 to 200 meters (492 to 656 ft.)	4
>200 to 250 meters (656 to 820 ft.)	5
>250 to 300 meters (821to 984 ft.)	6
>300 to 350 meters (984 to 1148 ft.)	7
>350 to 400 meters (1148 to 1312 ft.)	8
>400 to 450 meters (1312 to 1476 ft.)	9
>450 to 500 meters (1476 to 1640 ft.)	10

Table 19: Sync unit cable delay rotary switch settings

If the delay setting is not set correctly, the APs will not be synchronized properly resulting in an intermittent loss of connectivity.

3.6 Planning your AP groupings

“Groups” as defined for the Smart-hopping network have more than one meaning and must be carefully thought out prior to configuration. They are also defined in two places on the system and care must be taken to ensure that the definitions are not in conflict.

For improved network stability and roaming Philips recommends that all APs on one floor are partnered to the same APC.

If possible, avoid assigning AP Groups to the Primary APC. This can make upgrades and the process of synchronization of the APC configurations more efficient.

When enabling the Backup Primary APC feature, avoid assigning AP Groups to both the Primary APC and to the Backup Primary APC for the best performance. For systems with greater than 525 APs this is not possible. In these situations, the Backup Primary APC should manage APs in less critical areas.

3.6.1 Configuring AP groups

APs are assigned to groups once they are defined in the Smart-hopping Infrastructure configuration. The reasons for creating AP groups are:

- Groups of APs can be individually targeted for upgrades without affecting the APs in the other groups.
- Each defined group can have a different destination IP address for its alerts. The destination IP address correlates to a server IP address. The server can be either the Information Center server or the Focal Point server. The relevance of the destination IP address is:
    - The server accumulates all alerts for those APs and builds an alert database from them
    - The server sends out notifications to the required Information Centers (Wireless Monitoring Loss - Contact Service system messages), or service personnel.

- Each AP Group is assigned a Partnered APC. This APC manages an AP during normal operation. However, if the assigned APC fails, the APs partner with any available APC.

Take care when defining AP groups. APs that are not physically located within a care area must still be given a home group for equipment management purposes. This includes APs in transport areas, as well as APs in procedure areas (such as X-ray or Dialysis) that may be used by patients in more than one care group (such as ICU and CCU).

3.7 Performing an RF frequency survey

The Smart-hopping infrastructure operates on the 1.4 GHz US Wireless Medical Telemetry Service (WMTS) band or on the 2.4 GHz band.

In the USA, you must have a minimum of three available channels to deploy the 1.4 GHz Smart-hopping infrastructure successfully. In general, this should not be a problem as the WMTS band is a reserved, protected spectrum in the USA.

You must have a minimum of three available channels (six available channels is recommended) to deploy the 2.4 GHz Smart-hopping infrastructure successfully. As there are many devices (especially 802.11 b/g devices) that use the 2.4 GHz spectrum, it is imperative that you perform an RF frequency survey before installing the 2.4 GHz Smart- hopping infrastructure.

3.7.1 Understanding RF coexistence issues in the 2.4 GHz spectrum

There are several devices that may be encountered in the hospital environment that radiate 2.4GHz RF energy and may potentially cause interference. An understanding of their existence and power levels is key to a successful Smart-hopping infrastructure deployment.

3.7.2 Transient noise in the 2.4 GHz spectrum

Transient noise is RF energy that is not constant, but rather spurious and intermittent. Transient noise may sometimes only be observed by analyzing RF spectra over a longer period of time, or it may not be seen at all of it occurs outside the time that the data is taken.

3.7.2.1 Microwave ovens

The pulse of most consumer grade microwave ovens (typically 700-1300 watts) generally falls in the middle of the 2.4 GHz band. The pulse is very broad and will often affect at least half of the usable 2.4 to 2.5 GHz spectra but may not always be in the same place. Most consumer grade microwaves are single magnetron tube devices and the RF radiation of these varies by manufacturer.

While microwave ovens are typically only used periodically, their location should be known and steps should be taken to minimize their potential interference.

To avoid interference, position Smart-hopping Access Points a minimum of 20 feet (6 m) from consumer-grade microwave ovens. Ensure that there is not a microwave oven located between an Access Point and IPMs.

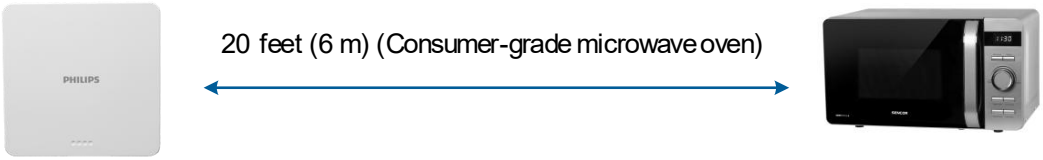


Figure 25: Recommended Minimum AP Distance from Microwave Ovens

Avoidance: Physical separation of at least 20 feet. Microwave level at 2.4 GHz Smart-hopping infrastructure AP shall be < -25dBm. Use the insufficient spectrum alert on the APC web interface to determine if a microwave source will be a problem at the selected AP location. Microwaves that operate on ½ sine wave can be avoided by the 2.4 GHz Smart- hopping infrastructure with its frequency agility & retry mechanism. If an IPM is in close proximity to a microwave source, then data loss > 90sec/day may be experienced.

3.7.2.2 Bluetooth devices

Although originally designed and deployed for short distance, low power Personal Area Network (PAN) deployments, full power (100mW) devices are now being produced and deployed.

A Bluetooth device may operate as a frequency hopper or as a device emitting energy on several narrow band channels. Fortunately, Bluetooth devices are usually very low powered and have interference avoidance algorithms built into them. When a Bluetooth device encounters a fixed channel system like the 2.4 GHz Smart-hopping infrastructure, it should avoid conflict. Unfortunately, Bluetooth devices are typically non-hospital owned “walk-in” devices and thus are difficult to control. For this reason, they are treated as transient noise sources.

Avoidance: Possibly none needed. Provide physical separation if possible. Refer to hospital policy on Bluetooth use in care areas. 2.4 GHz Smart-hopping infrastructure can tolerate Bluetooth piconet systems with seven Bluetooth 2.0 devices communicating.

3.7.2.3 Other transient devices

Increasingly, the 2.4GHz space is being used for other non-communication or non-computer related devices. Various remote controls and children's toys are using 2.4GHz radios. Be sure to consider these as possible interference sources. If persistent, a noise source like this would be discovered by a spectrum analysis, typically appearing as a narrow band, continuous emitter with nearly a 100% duty cycle.
Avoidance: Physical separation.

3.7.3 Continuous noise in the 2.4 GHz spectrum

We refer to “Continuous” RF emitters as devices that emit energy constantly, although seldom at a 100% duty cycle. Devices which “beacon” when in low use may not be thought of as continuous noise sources, but because they often appear in short-term (5 to 20 minute) spectra captures, they are treated as such.

3.7.3.1 802.11/Wi-Fi devices

Noise attributed to 802.11 devices will vary in duration/duty cycle. It can range from short, intermittent “beaconing” bursts to near steady state, broad spectrum energy from heavily loaded, systems. Fortunately, device keep-alive and beaconing schemes make them generally detectable anytime that they are turned on, and therefore are treated as steady state noise sources.

While many 802.11 systems are fixed channel, many newer systems are dynamic and may change channels as other RF spectra changes take place. Predictable, coexistence with 2.4 GHz Smart-hopping infrastructure is possible only if both the Smart-hopping infrastructure and the Wi-Fi device are configured for static, fixed channelization.

The 2.4 GHz Smart-hopping infrastructure has pre-set configurations that are designed to “fit” channels in between commonly used 802.11b/g channels. See “Avoiding Wi-Fi Interference” on page 54 for more details.

Avoidance: Collaboration with hospital IT administrators to achieve a fixed 802.11 channel configuration that avoids the 2.4GHz Smart-hopping infrastructure channel configuration. Use 2.4 GHz Smart-hopping infrastructure channel assignment to avoid these 802.11 b/g channels: 1, 6, 11 or 1, 7, 13. Locate 2.4 GHz Smart-hopping infrastructure APs and Remote Antennas at least 6 ft (2 m) from 802.11 Wi- Fi APs.

3.7.3.2 Cordless phones and headsets

2.4GHz cordless phones and wireless headsets are prevalent and have been shown to interfere with 2.4GHz systems when in very close proximity. These devices are generally DECT-based frequency hoppers and populate the spectrum with moving RF “spikes.” When enough devices are present, they may fill the whole spectrum with narrow-band, spike activity. The duty cycle however is typically very low.

Note that many cordless phones/headsets will emit “beacon” pulses even when not being used. Do not assume that such devices can only interfere when in use. For this reason, they are being dealt with here as a “Continuous” interferer. Some of the higher end versions of these devices are capable of detecting like-channel interference and avoiding it. These systems may simply “stay away” from the 2.4 GHz Smart-hopping infrastructure, with fixed channelization, however this cannot be assumed.

Avoidance: Typically, no avoidance measures are needed. Provide physical separation if required. The 2.4 GHz Smart- hopping infrastructure can tolerate up to 12 (2.4GHz) phones.

3.7.3.3 Wireless security devices

X10 cameras, wireless baby monitors and other devices dominate bandwidth on a constant, streaming basis. Duty cycle is typically 100%, however the spectrum usage is narrow.

Avoidance: Collaboration of configurations with system IT or administrators. Fixed channelization and 2.4 GHz avoidance configuration (channelization).

3.7.3.4 ZigBee devices

ZigBee is a published specification set of high level communication protocols designed to use small, low power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). This essentially means that implementations (and therefore RF "footprints") will vary widely, more so than with other technologies. ZigBee is aimed at applications with low data rates and low power consumption and the technology is designed to be simpler and cheaper than other WPANs such as Bluetooth.

Avoidance: Implement proper ZigBee channel management. Limit channels used by ZigBee to ensure that at least three 2.4 GHz channels are available for the Smart-hopping network.

3.7.4 RF analysis guidelines

RF analysis is required for all sites to validate the viability of usable RF spectrum for the 2.4 GHz Smart-hopping infrastructure. The result of the RF analysis will be a picture of the available spectra at the site into which the Smart- hopping network may be configured.

Once the RF analysis is done, you should use the survey data as the basis for selecting the channels used by the 2.4 GHz Smart-hopping infrastructure.

3.7.4.1 Survey objectives

The premise of steady-state or continuous RF interference is that while its source may not be known, it is more or less continuously in the environment and taking a measurement of RF energy for a duration of as little as five minutes will capture it. Short duration tests are intended to capture this type of interference.

It is also acknowledged that in many cases, interference will be experienced intermittently at a given location either because the source is an intermittent radiator (or intermittently used by hospital personnel), or that it is a moving radiator that is experienced in a given location only as it moves through that area.

Capturing and measuring intermittent interference is difficult. Even if measurement tools are left on to "listen" for hours and even days, they may still miss an "event" that would cause interference with the 2.4GHz ITS. A monitoring/ measurement system should be left on as long as time permits to have the best chance to capture all possible steady and intermittent interference sources.

3.7.4.2 Using the spectrum analyzer tool

A spectrum analyzer tool should be used to assess and capture the steady-state RF profiles. The data capture feature of this tool will be used to capture and create .ccf files for each test location. Note that data files for a five-minute capture are approximately 1.6Mb in size and those for a two-hour capture are approximately 37Mb.

The spectrum analyzer allows you to specify the duration of the capture in advance such that when the time limit is reached, recording automatically stops.

Note In most cases, screen shot captures of spectrum analyzer displays are most effective when the tool is not moved during the data gathering. "Roaming" type tests can be useful sometimes, but trying to annotate the captured data such that another person looking at it later will know exactly how the tool was moved during the capture is difficult, if not impossible. Taking separate captures at fixed

locations and annotating on a floor plan where each capture was a taken usually achieves a better overall analysis of the environment.

3.7.4.3 Determining measurement locations

Floor plans should be procured for the test sites and patient care areas identified. Survey locations can be identified in advance on the floor plans and given location designations.

Short term captures (to detect steady state RF energy) should be taken at several such locations in the patient care areas, as well as on floors above and below, and adjacent areas as time and access permit. The objective is to take measurements in patient care areas, and the surrounding areas, where wireless monitoring of any kind might be employed.

In a typical hospital unit, short term (five-minute) measurements should be taken in rooms along one side of the building, but not in every room. It is expected that any unit-wide RF activity would be found in all rooms that were geographically and architecturally similar. Preference should be given for patient care areas that have windows which face other buildings, parking lots or areas of significant activity. Additionally, patient care areas which are adjacent to common public areas such as lobbies, main corridors or waiting areas should be considered as a test location. Surveys should also be taken at planned AP locations.

Also, “long-term” site-surveys should be executed when possible (especially for “critical” sites where implementation to a high degree of thoroughness is warranted). Long-term captures should be taken in at least one location in the patient care area for a minimum period of two hours. The test period should be during a time of maximum hospital activity (i.e., not overnight) to try and capture all intermittent RF sources. Generally, overnight testing is not recommended, as it does not present a realistic picture of spectra use.

3.8 Assigning 2.4 GHz Smart-hopping infrastructure channels

When installing the 2.4 GHz Smart-hopping infrastructure, you must configure 3-6 channels for the system to use. To have a successful deployment, the channels must be located in RF spectra where they are least likely to experience interference. Choosing appropriate channels after reviewing the spectrum analyzer data is critical.

3.8.1 Avoiding Wi-Fi interference

In hospitals, 802.11 systems are the most likely source of interference in the 2.4 GHz space. The following sections describe how to choose the appropriate channels to avoid interference from Wi-Fi systems as well as from other sources of interference.

Figure 26 shows the relationship between available 2.4 GHz Smart-hopping infrastructure channels and 802.11b/g channels.

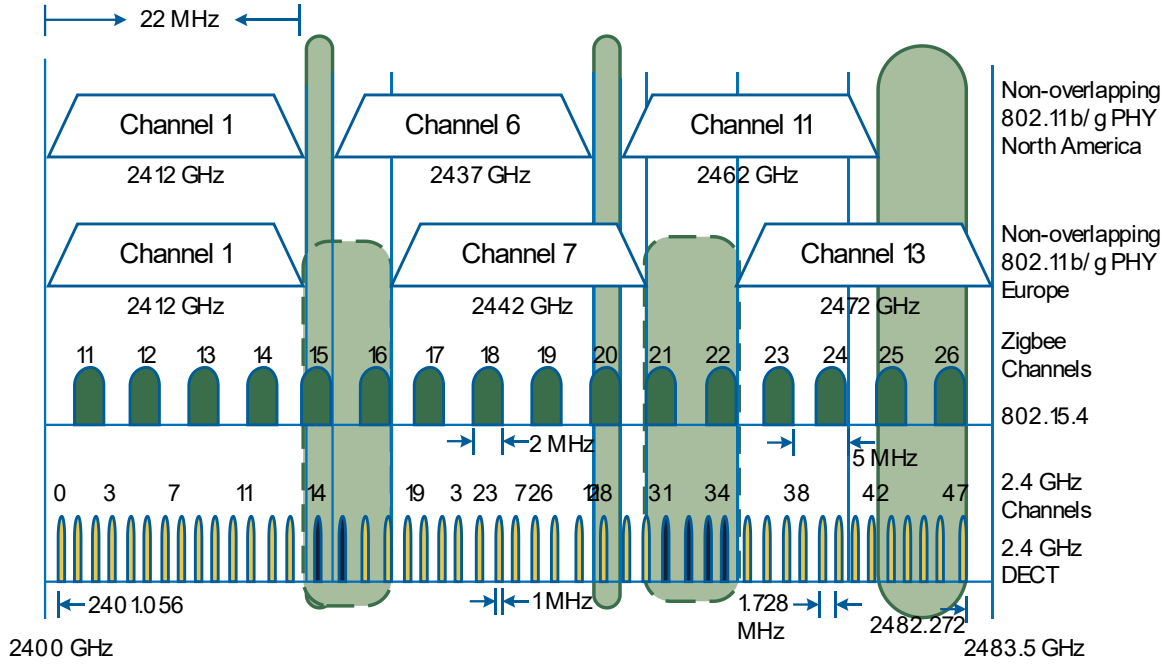


Figure 26: 2.4 GHz Smart-hopping infrastructure Channels vs. 802.11b/g Channels

3.8.2 2.4 GHz Smart-hopping infrastructure frequency plans

The 2.4 GHz Smart-hopping infrastructure provides for simple configuration amid common 802.11 deployments. Configured in this way, the system automatically configures itself for the channels in the “holes” left by the specified 802.11 configuration. Graphical examples are shown below.

3.8.2.1 Frequency plan 1,6,11

Where channels 1-11 are available for 802.11 deployments, channels 1,6,11 offer orthogonality in a three-channel design. When channels 1,6, and 11 are used for Wi-Fi, configure channels 14,28 and 44-47 for use by the 2.4 GHz Smart-hopping infrastructure.

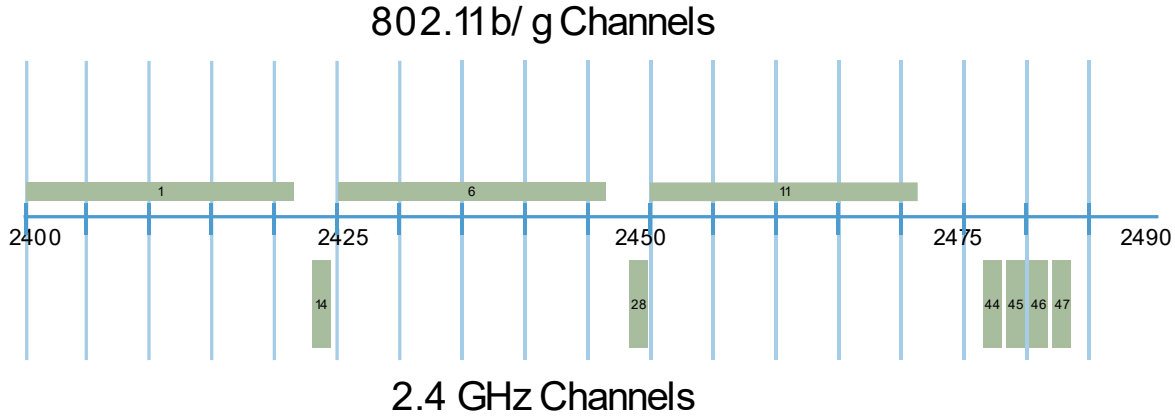


Figure 27: Free 2.4 GHz Smart-hopping infrastructure Channels in a 1, 6, 11 Wi-Fi Configuration

3.8.2.2 Frequency plan 1,7,13

In Europe, where channels 1-13 are available for 802.11 deployments, channels 1,7,13 offer good orthogonality in a three-channel design. When channels 1,7,and 13 are used for Wi-Fi, configure channels 14-16 and 31-33 for use by the 2.4 GHz Smart-hopping infrastructure.

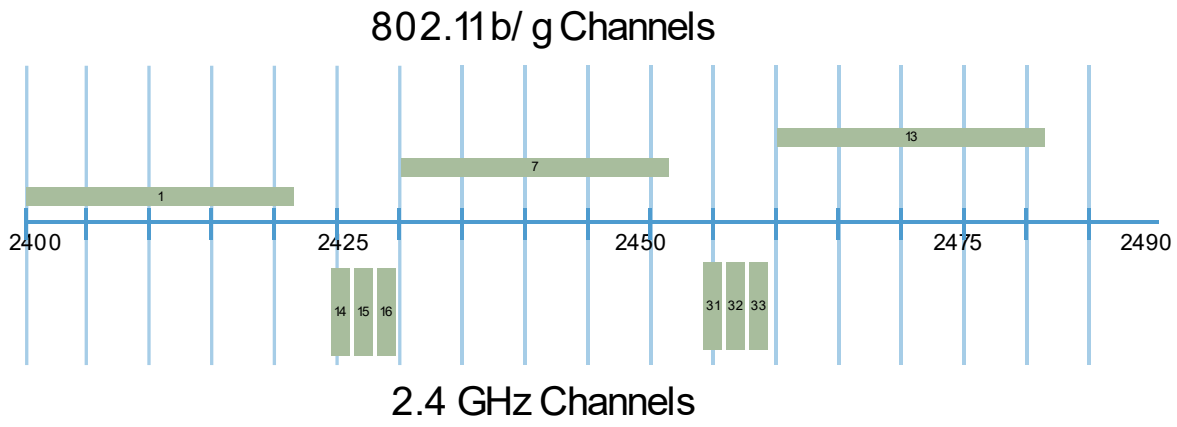


Figure 28: Free 2.4 GHz Channels in a 1, 7, 13 Wi-Fi Configuration

3.8.3 Using 'advanced' 2.4 GHz channel configurations

In cases where an 802.11 deployment with channels 1,6 and 11, or 1, 7 and 13 are not the predominant source of interference to be avoided, specific, individual channel configuration is warranted. Site situations will vary, but the RF Spectrum Analysis should show visually where the best location to configure the 2.4 GHz channels are.

For example, if DECT phones are present at the site and occupy only the upper ¾ of the available spectra, choosing channels on the low end (1-9) of the available range is best.

If the spectra is clean other than a nearby microwave that the spectrum analysis shows radiates in the low end of the spectrum, you should select channels in the upper end of the spectrum for the 2.4 GHz Smart-hopping infrastructure.

3.9 Using the layer 3 option

The International Organization for Standardization (ISO) created the Open Systems Interconnection (OSI) reference model (ISO/IEC 7498-1) which defines seven layers in a network environment to facilitate communication between different systems made by different vendors.

The Smart-hopping Infrastructure by default uses Layer 2, the data link layer, for communication on an IntelliVue Network.

Layer 3, the network layer, is supported; however, it must be configured first.

IntelliVue Networks which rely on customer supplied equipment may choose to use Layer 3 to align their CSCN more closely with the standards used by those vendors to provide more flexibility in the configuration of the IntelliVue Network.

The benefits of using Layer 3 include the ability to use an existing network infrastructure, allowing the Smart-hopping network to span multiple VLANs, and to enable routing to the edge of a network.

The commands used for configuring the Layer 3 option are all available in the serial menu. To set up Layer 3 you will need a service PC with an available RS-232 serial port and a terminal emulation program. Do not power off or disconnect the Primary APC prior to connecting the service PC to the Primary APC to configure the Layer 3 option.

3.9.1 Prerequisites for layer 3

- The Layer 3 option is only available on Customer-supplied Clinical Networks with PIC iX.
- All APCs must be on a single subnet or VLAN. You must configure this subnet to use IGMP (Internet Group Management Protocol) version 3.
- You must configure all subnets or VLANs on which APs reside to use IGMP version1.
- There must be two unique multicast addresses; one for the Primary APC and one for the Secondary APCs
- All APCs must be using release D.x or later.
- A customer-supplied DHCP server is required by the Access Points for Layer 3 operation. Refer to Appendix F, DHCP Option 43 for more information.
- It is required that the lower ten bits of each Access Point IP address is unique. The most efficient way of managing this is with a contiguous block of IP addresses.
    - The recommended IP address lease time for each AP is 8 weeks, but not less than 8 hours.
    - If an AP loses its IP address it will need to be rescanned into the PIC iX configuration to ensure that the device location is populated properly.
- Smart-hopping Layer 3 installation is supported for multi-zone environments. Refer to Appendix A, Multi-Smart-hopping systems for more information.

3.10 Completing installation worksheets

As part of the planning process for your deployment and prior to installing any components, be sure to complete[1] the following installation worksheets:

Note Copies of these worksheets are available in the Smart-hopping Learning Products Documentation Portfolio, available on the Philips InCenter site.

- Smart-hopping infrastructure Equipment Summary (page 57)
- Smart-hopping 1.4 GHz Access Point Equipment Summary (page 57)
- Smart-hopping 2.4 GHz Access Point Equipment Summary (page 57)
- Layer 2 Smart-hopping APC Configuration Worksheets (page 59)
- Layer 3 Smart-hopping APC Configuration Worksheets (page 63)
- 1.4 GHz Default AP Configuration Worksheet (page 66)
- 2.4 GHz Default AP Configuration Worksheet (page 67)
- AP Group Configuration Worksheets (page 69)

3.10.1 Smart-hopping infrastructure equipment summary

Note the location, IP address, etc. of Smart-hopping infrastructure devices (network switches, PoE Units, APCs, etc.) before you physically install them using table 20.

Device Type	Device Name	Physical Location	IP Address	Subnet Mask

Device Type	Device Name	Physical Location	IP Address	Subnet Mask

Table 20: Smart-hopping infrastructure equipment summary

Note the location, IP address, MAC, etc. of Smart-hopping Access Points before you physically install them using table 21 and table 22.

AP Name	RF ID	Group Membership	IP Address	MAC Address	Physical Location	Partnered APC	Connected to Switch	Connected to Switch Port	UTP Cable Run ID

Table 21: Smart-hopping 1.4 GHz Access Point equipment summary

AP Name	RF ID	Group Membership	IP Address	MAC Address	Physical Location	Partnered APC	Connected to Switch	Connected to Switch Port	UTP Cable Run ID	2.4 GHz Frequency plan	2.4 GHz Radio regulations

Table 22: Smart-hopping 2.4 GHz Access Point equipment summary

3.11 Layer 2 Smart-hopping APC configuration worksheets

(leave items in grayed boxes as is, do not change values)

3.11.1 Setting description

Refer to the following setting descriptions when completing the Access Point Controller Configuration Worksheet.

Separate blank templates for standard Layer 2 Smart-hopping deployments for both non-routed and routed IntelliVue Network topologies are provided on the following pages.

APC Configurations - In the worksheet provided, fill in the following information for each APC to be added to the wireless subnet:

- APC Name - Assigned name of this APC within the system.
- APC MAC - MAC Address documented on product label (physical address).
- APC IP Address - IP address for the APC within the wireless subnet.
- Subnet Mask - Set to subnet mask of the Smart-hopping wireless subnet. This will be 255.255.240.0 for Routed IntelliVue Network topologies, and 255.255.248.0 for Non-Routed IntelliVue Network topologies.
- Default Gateway - Typically this will be 172.31.240.1 for Routed IntelliVue Network topologies, and 172.31 (n + 3).0 for Non-Routed IntelliVue Network topologies.
- Multicast Address - For each Smart-hopping wireless network, two unique multicast addresses are required for communication between the APCs and APs.
    - Primary APC Multicast Address - Defaults to 239.255.254.1 but can be configured to be any unique multicast address.
    - Secondary APC Multicast Address - Defaults to 239.255.254.2 but can be configured to any unique multicast address.

- APC Priority Level - This entry allows you to set an APC to be a primary, backup primary, or secondary. If the Primary APC is disabled or stops working, the backup primary becomes the primary. To enable the Backup Primary APC feature, set the Backup APC Priority Level for the Primary APC and the Backup Primary APC to 0. The Backup APC Priority Level value for all secondary APCs is set to 2. If you do not wish to use the Backup Primary APC feature, set all APCs Backup APC Priority Level to 0.

- System Type - Select the appropriate option (1.4 GHz or 2.4 GHz) for the type of Smart-hopping deployment (1.4 or 2.4 GHz).

- Client CI Multicast Spoof - If the system uses the Philips registered multicast IP address of 224.0.23.173 for the CI message enable the Client CI Multicast Spoof feature.

- Advanced Configuration - This entry allows you to change the user ID and password the web browser-based connection to the APC uses.

- Layer 3 Multicast Address Information - Not applicable for Layer 2 Smart-hopping Deployments.

- Security and Advanced Parameters - This feature allows you to configure the web browser session to use HTTP or HTTPS.

3.11.2 Worksheets

(leave items in grayed boxes as is, do not change values)

IP Address	Subnet Mask	Default Gateway

Table 23: Service PC IP address information

APC Name	MAC Address	IP Address	Subnet Mask	Default Gateway	Priority Level 0 or 2

Table 24: APC static TCP/IP address and priority level configuration

	Default Multicast Address	Multicast Address
Primary APC Multicast Address	239.255.254.1	N/A
Secondary APC Multicast Address	239.255.254.2	N/A

Table 25: Layer 3 multicast address information - not applicable for layer 2 Smart-hopping deployments

System Name	Philips - (default - do not change)	
System Type	1.4 GHz Smart-hopping (default)	2.4 GHz Smart-hopping

Table 26: System type - enable 1.4 or 2.4 GHz Smart-hopping

Client CI Multicast Spoof		
	Disabled (default)	Uses Client Current CI Multicast Address: 224.0.23.63
	Enabled	Uses Client New CI Multicast Address: 224.0.23.173

Table 27: Client CI multicast spoof: CI (connection indication) address

Web Configuration	
Web Access	Enabled (default - do not change)
Browser User Name	
Browser Password	
Web Server Port Number (HTTP Only)	80 (default - do not change)
Console Password	

Table 28: Advanced configuration: web browser and console passwords

APC Multicast Layer 3		
X	Disabled (default)	Operates in Smart-hopping Layer 2 mode (APCs, Wireless Clients and APs in same subnet)
	Enabled	Operates in Smart-hopping Layer 3 mode (APCs and Wireless Clients in same subnet, APs in different subnets)

Table 29: APC multicast layer 3

Security and Advanced Parameters		
	Disabled (default)	Cannot view current Secure Communication via SSL menu option
	Enabled	Enable to view current Secure Communication via SSL setting
Secure Communication Using SSL		
	Disabled (default)	Operates in HTTP mode
	Enabled	Operates in HTTPS mode (requires configuration of Browser User Name and Browser Password)

Table 30: Secure communication via SSL: HTTP or HTTPs mode

3.11.3 BOOTP/DHCP server configuration

Non-routed and Routed when used in the BootP/DHCP Server Configuration screen - refers to how data gets from the APCs to the Information Center servers.

- A non-routed system indicates a clinical network that has the APs, APCs, Smart-hopping Wireless Clients and the Information Centers that monitor them on the same subnet. Factory defaults reflect a PIIC Classic system in the ICN 1 subnet (172.31.0.0 / 21).

- A routed system indicates a clinical network where the Smart-hopping devices (APs, APCs and Smart-hopping Wireless Clients) are not on the same subnet as the Information Centers, and therefore data from the Smart-hopping devices must be routed to the Information Center. Factory defaults reflect a system in the Smart-hopping subnet (172.31.240.0 / 20).

3.11.3.1 Non-routed range worksheets

Setting	Factory Default	Site Modification
MAC Address Base	00:09:fb:06:00:00	00:09:fb:06:00:00
MAC Address Mask	ff:ff:ff:0f:00:00	ff:ff:ff:0f:00:00
IP Address Range (Minimum)	172.31.6.0	
IP Address Range (Maximum)	172.31.6.255	
Subnet Mask	255.255.248.0	
Default Gateway	172.31.3.0	
DNS Server IP Address	0.0.0.0	0.0.0.0

Table 31: Non-routed: range 1 - transceivers and wireless bedsides

Setting	Factory Default	Site Modification
MAC Address Base	00:09:fb:05:00:00	00:09:fb:05:00:00
MAC Address Mask	ff:ff:ff:0f:00:00	ff:ff:ff:0f:00:00
IP Address Range (Minimum)	172.31.2.128	
IP Address Range (Maximum)	172.31.2.255	
Subnet Mask	255.255.248.0	
Default Gateway	172.31.3.0	
DNS Server IP Address	0.0.0.0	0.0.0.0

Table 32: Non-routed: range 2 - Access Points

3.11.3.2 Routed range worksheets

Setting	Factory Default	Site Modification
MAC Address Base	00:09:fb:06:00:00	00:09:fb:06:00:00
MAC Address Mask	ff:ff:ff:0f:00:00	ff:ff:ff:0f:00:00
IP Address Range (Minimum)	172.31.248.0	
IP Address Range (Maximum)	172.31.253.255	
Subnet Mask	255.255.240.0	
Default Gateway	172.31.240.1	
DNS Server IP Address	0.0.0.0	0.0.0.0

Table 33: Routed: range 1 - transceiver and wireless bedsides

Setting	Factory Default	Site Modification
MAC Address Base	00:09:fb:05:00:00	00:09:fb:05:00:00
MAC Address Mask	ff:ff:ff:0f:00:00	ff:ff:ff:0f:00:00
IP Address Range (Minimum)	172.31.244.128	
IP Address Range (Maximum)	172.31.246.255	

Subnet Mask	255.255.240.0	
Default Gateway	172.31.240.1	
DNS Server IP Address	0.0.0.0	0.0.0.0

Table 34: Routed: range 2 - Access Points

3.12 Layer 3 Smart-hopping APC configuration worksheets

(leave items in grayed boxes as is, do not change values)

3.12.1 Setting descriptions

Refer to the following setting descriptions when completing the Access Point Controller Configuration Worksheet.

Separate blank templates for standard Layer 3 Smart-hopping deployments for both non-routed and routed IntelliVue Network topologies are provided on the following pages.

- APC Configurations - In the worksheet provided, fill in the following information for each APC to be added to the wireless subnet:
  - APC Name - Assigned name of this APC within the system
  - APC MAC - MAC Address documented on product label (physical address)
  - APC IP Address - IP address for the APC within the wireless subnet
  - Subnet Mask - Set to subnet mask of the Smart-hopping APC/wireless client subnet.
  - Default Gateway - Set to default gateway of the Smart-hopping APC/wireless client subnet.

- CI (Connection Indication) Address Information - The CI multicast address can be configured to be either 224.0.23.63 or 224.0.23.173.

- Multicast Address - For each Smart-hopping wireless network, two unique multicast addresses are required for communication between the APCs and APs.
  - Primary APC Multicast Address - Defaults to 239.255.254.1 but can be configured to be any unique multicast address.
  - Secondary APC Multicast Address - Defaults to 239.255.254.2 but can be configured to any unique multicast address.

- APC Priority Level - This entry allows you to set an APC to be a primary, backup primary, or secondary. If the Primary APC is disabled or stops working, the backup primary becomes the primary. To enable the Backup Primary APC feature, set the Backup APC Priority Level for the Primary APC and the Backup Primary APC to 0. The Backup APC Priority Level value for all secondary APCs is set to 2. If you do not wish to use the Backup Primary APC feature, set all APCs Backup APC Priority Level to 0.

- System Type - Select the appropriate option (1.4 GHz or 2.4 GHz) for the type of Smart-hopping deployment (1.4 or 2.4 GHz).

- Advanced Configuration - This entry allows you to change the user ID and password the web browser-based connection to the APC uses.

- Client CI Multicast Spoof - If the system uses the Philips registered multicast IP address of 224.0.23.173 for the CI message enable the Client CI Multicast Spoof feature.

- APC Multicast Layer 3 - Enable this if your APC part of a Layer 3 deployment.

- Security and Advanced Parameters - This feature allows you to configure the web browser session to use HTTP or HTTPS.

IP Address	Subnet Mask	Default Gateway

Table 35: Service PC IP address information

APC Name	MAC Address	IP Address	Subnet Mask	Default Gateway	Priority Level 0 or 2

Table 36: APC static TCP/IP address and priority level configuration

	Default CI Multicast Address		CI Multicast Address
	224.0.23.63 (default)		224.0.23.173

Table 37: CI (Connection Indication) address information - select one

	Default Multicast Address	Multicast Address
Primary APC Multicast Address	239.255.254.1	
Secondary APC Multicast Address	239.255.254.2	

Table 38: Layer 3 multicast address information - not applicable for layer 2 Smart-hopping deployments

System Name	Philips - (default - do not change)	
System Type	1.4 GHz Smart-hopping (default)	2.4 GHz Smart-hopping

Table 39: Enable 1.4/2.4 GHz Smart-hopping

Web Configuration	
Web Access	Enabled (default - do not change)
Browser User Name	
Browser Password	
Web Server Port Number (HTTP Only)	80 (default - do not change)
Console Password	

Table 40: Advanced configuration: web browser and console passwords

Client CI Multicast Spoof		
	Disabled (default)	Uses Client Current CI Multicast Address: 224.0.23.63
	Enabled	Uses Client New CI Multicast Address: 224.0.23.173

Table 41: Client CI multicast spoof: CI (connection indication) address

APC Multicast Layer 3		
	Disabled (default)	Operates in Smart-hopping Layer 2 mode (APCs, Wireless Clients and APs in same subnet)
X	Enabled	Operates in Smart-hopping Layer 3 mode (APCs and Wireless Clients in same subnet, APs in different subnets)

Table 42: APC multicast layer 3

Security and Advanced Parameters		
	Disabled (default)	Cannot view current Secure Communication via SSL menu option
	Enabled	Enable to view current Secure Communication via SSL setting
Secure Communication Using SSL		
	Disabled (default)	Operates in HTTP mode
	Enabled	Operates in HTTPS mode (requires configuration of Browser User Name and Browser Password)

Table 43: Secure communication via SSL: HTTP or HTTPs mode

3.12.2 BOOTP/DHCP server configuration

Non-routed and Routed when used in the BootP/DHCP Server Configuration screen - refers to how data gets from the APCs to the Information Center servers.

- A non-routed system indicates a clinical network that has the APs, APCs, Smart-hopping Wireless Clients and the Information Centers that monitor them on the same subnet. Factory defaults reflect a PIIC Classic system in the ICN 1 subnet (172.31.0.0 / 21).

- A routed system indicates a clinical network where the Smart-hopping devices (APs, APCs and Smart-hopping Wireless Clients) are not on the same subnet as the Information Centers, and therefore data from the Smart-hopping devices must be routed to the Information Center. Factory defaults reflect a system in the Smart-hopping subnet (172.31.240.0 / 20).

- In a Layer 3 Smart-hopping network, the two NON-ROUTED ranges, and the ROUTED: Range 2 - Access Points range, and RANGE 5 are all unchecked. The Access Points get their IP addresses from the hospital DHCP server, not from the APC.

- In a Layer 3 Smart-hopping network, ROUTED: Range 1 - Transceivers and Wireless Bedsides is checked, and the IP addressing information is configured per the design.

- Non-Routed: Range 1 - Transceivers and Wireless Bedsides
    - Deselect Box - range disabled

- Non-Routed: Range 2 - Access Points
    - Deselect Box - range disabled

- Routed: Range 1

Setting	Factory Default	Site Modification
MAC Address Base	00:09:fb:06:00:00	00:09:fb:06:00:00
MAC Address Mask	ff:ff:ff:0f:00:00	ff:ff:ff:0f:00:00
IP Address Range (Minimum)	172.31.248.0	
IP Address Range (Maximum)	172.31.253.255	
Subnet Mask	255.255.240.0	
Default Gateway	172.31.240.1	
DNS Server IP Address	0.0.0.0	0.0.0.0

Table 44: Routed: range 1 - transceivers and wireless bedsides

- Routed: Range 2 - Access Points
    - Deselect Box - range disabled

Note In a Layer 3 configuration, the APs get their IP address assignments from the hospital DHCP server. This is why the range is disabled.

3.12.3 1.4 GHz default AP configuration worksheet

3.12.3.1 Setting descriptions

Refer to the following setting descriptions when completing the 1.4 GHz Access Point Configuration Worksheet. Use the information you record in this worksheet with the procedure entitled “Configuring the 1.4 GHz Access Point Default Settings” on page 92.

- Partnered APC - “Any”.
- Default Group - Always Smart-hopping.
- WMTS Channels - Circle the WMTS Channel that will be used for this installation. Default range = 1 to 6. Note: Disable channels 4, 5 & 6 when Special Geographic Area is selected - use channels 4a, 1, 2 and 3.
- RF Access Code - Enter number between 1 and 254 to be used as the Access Code for the system (site specific). Do not use 0 or 255, these are reserved for special use. For use of multiple RF Access Codes, refer to Appendix A, Installing Multiple Smart-hopping systems at a Single Hospital Site. For use of multiple RF Access Codes, refer to Appendix A, “Installing Multiple Smart-hopping systems at a Single Hospital Site.”
- IP Addressing: Subnet Mask - Enter the Static Subnet Mask documented for the APC Configuration.
- IP Addressing: Default Gateway - Enter the Static Default Gateway documented for the APC Configuration.

3.12.3.2 Blank template

Settings	Rules	Value
Partnered APC		Any
Default Group		Smart-hopping
WMTS Channels	Circle channels at right.	Standard: 1 2 3 4 5 6 Special: 4a
RF Access Code	Enter any number from 1 to 254 at right. (do not use 0 or 255)	1 (Site Specific)
IP Addressing: Subnet mask	[Copy from APC Configuration]	
IP Addressing: Default gateway	[Copy from APC Configuration]	

Table 45: Blank template

3.12.4 2.4 GHz default AP configuration worksheet

3.12.4.1 Setting description

Refer to the following setting descriptions when completing the 2.4 GHz Access Point Configuration Worksheet. Use the information you record in this worksheet with the procedure entitled “Configuring the 2.4 GHz Access Point Default Settings” on page 92.

- Partnered APC - “Any”.
- Default Group - Always Smart-hopping.
- Radio Regulations - Specify the radio regulations that apply to the country in which you are installing the 2.4 GHz Smart-hopping infrastructure. Possible Radio Regulation choices are:
  - ETSI - Europe, South America, Asia, Asia Pacific, and Africa
  - FCC - Taiwan, Singapore, and Hong Kong
  - RSS-210 - Canada/North America
  - AS/NZ - Australia/New Zealand
  - ARIB – Japan
- Frequency Plan - Specify the 802.11 channel configuration with which the 2.4 GHz Smart- hopping infrastructure will co-exist. Possible Frequency Plan choices are:

Frequency Plan	2.4 GHz Smart-hopping infrastructure Channels Configured for Use	
	FCC, ARIB, RSS-210	ETSI, AS/NZ
Co-exist with 802.11 Channels 1, 6, 11	14, 28, 44, 45, 46, 47[1]	14, 28, 43, 44, 45, 46
Co-exist with 802.11 Channels 1, 7, 13	14, 15,16, 31, 32, 33[2]	14, 15, 16, 31, 32, 33[2]
Advanced	Any set (min 3, max 6) of 2.4 GHz Smart-hopping infrastructure channels from 0 - 47, excluding any that have been disabled by the ZigBee selection.	Any set (min 3, max 6) of 2.4 GHz Smart-hopping infrastructure channels from 1 - 46, excluding any that have been disabled by the ZigBee selection.

- If you select Advanced, then you must specify a minimum of three and a maximum of six channels (six is recommended) for use by the 2.4 GHz Smart-hopping infrastructure.

- ZigBee channel used for medical - Specify the ZigBee channel used for medical purposes at the installation site. Possible selections are channels 11 to 26. Default: None.

- RF Access Code - Enter number between 1 and 254 to be used as the Access Code for the system (site specific). Do not use 0 or 255, these are reserved for special use. For use of multiple RF Access Codes, refer to Appendix A, “Installing Multiple Smart-hopping systems at a Single Hospital Site.”

- IP Addressing: Subnet Mask - Enter the Static Subnet Mask documented for the APC Configuration.

- IP Addressing: Default Gateway - Enter the Static Default Gateway documented for the APC Configuration.

3.12.4.2 Blank template

Settings		Rules	Value
Partnered APC			Any
Default Group			Smart-hopping
Radio Regulations		Specify radio regulations that apply to country in which 2.4 GHz Smart-hopping infrastructure is installed. Circle applicable regulations at right.	ETSI FCC RSS-210 AS/NZ ARIB (Japan)
Frequency Plan		2.4 GHz Must Co-exist with Installed 2.4 GHz 802.11 b/g Systems Circle 802.11 plan at right.	1, 6, 11 1, 7, 13 Advanced - Enter a min. of 3 and a max. of 6 channels for use by the ITS.
ZigBee channel used for medical		Specify the ZigBee channel used for medical purposes at the installation site. Possible selections are channels 11 to 26.	None (Site Specific)
RF Access Code		Enter any number from 1 to 254 at right. (do not use 0 or 255)	1 (or other Site-specific Value)
IP Addressing: Subnet mask		[Copy from APC Configuration]	
IP Addressing: Default gateway		[Copy from APC Configuration]	

Table 46: Blank template

3.12.5 AP group configuration worksheets

3.12.5.1 Setting description

For each AP Group to be established, complete a separate worksheet. The template for this form is provided on the Documentation files available on the Philips InCenter web site. See “Planning Your AP Groupings” on page 50 for information about AP groups and how you may want to configure them. Use the information you record in this worksheet with the procedure entitled “Configuring AP Groups” on page 50.

Group Level Settings:

Document the following settings for each AP group:

- AP Group Name - The name of the AP Group
- AP Group Type - Always Smart-hopping
- AP Group Description - Optional notes regarding this AP Group
- Partnered APC - Copy APC Name from APC Configuration Worksheet for the APC that will be associated with Access Points in this group.
- Alert Destination - IP Address of Focal Point server or Philips Information Center server receiving alerts for this group of APs.

Note You can only set one alert destination for each AP group, in most cases, this would be either a Philips Patient Information Center server or a Focal Point server.

AP Group Members:

Document the following settings for each AP group:

- AP MAC Address - MAC Address as labeled on the Access Point
- AP Name - The name assigned to this AP within the system.
- AP Specific IP Address - Specific IP address to be assigned to this AP. This IP address needs to be the same as the IP address assigned in the Database Server in order for statistics gathering to occur for this AP.

3.12.5.2 Blank template

Group Level Parameters:

Setting	Rules	Value
AP Group Name		
AP Group Type		Smart-hopping
AP Group Description/ Area Covered (optional)		
Partnered APC	Enter APC Name from AP Configuration Worksheet.	
Alert Destination (DBS IP Address)		

Table 47: Blank template

AP Group Members:

AP Group Name:			
No.	AP MAC Address	AP Name	AP Specific IP Address
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

Table 48: Blank template

4 Installing and configuring the Smart-hopping infrastructure

This chapter provides procedures to physically install the Smart-hopping versions 1.0 and 2.0 Infrastructure components and configure the operational settings for use at the installation site, and includes:

- High-level Smart-hopping infrastructure Installation and Configuration Procedure
- Step 1. Complete the Smart-hopping Infrastructure Installation Worksheets
- Step 2. Install the Smart-hopping infrastructure Components
- Step 3. Set Up Your Service PC
- Step 4. Installing the Upgrade Tool
- Step 5. Perform Initial Configuration of the APCs to be Installed
- Step 6. Add the APCs to the Network
- Step 7. Run the Philips Upgrade Tool
- Step 8. Verify and Configure Important Smart-hopping infrastructure Settings via the APC Web Browser Interface
- Step 9. Run the Philips Upgrade Tool Again
- Step 10. Add APs to the Network
- Step 11. Rename Installed APs and Remote Antennas
- Step 12. Run the Philips Upgrade Tool Again
- Step 13. Export the Smart-hopping infrastructure Configuration to a Disk File
- Step 14. Backup the APC Config files
- Step 15. Restore your Service PC to its Original Settings
- Step 16. Perform Network Scan
- Step 17. Install Patient Monitors

4.1 High-level Smart-hopping infrastructure installation and configuration procedure

The following high-level procedure lists the steps you must follow to install and configure the Smart-hopping Infrastructure. Detailed procedures for each of these steps is provided in the sections that follow.

To install and configure the Smart-hopping infrastructure:

1. Complete the Smart-hopping infrastructure Installation Worksheets provided in Chapter 2. (page 57) Note the location, IP address, MAC, etc. of Smart-hopping infrastructure devices before you physically install them. Be sure to complete the APC and AP configuration worksheets prior to attempting to configure the Smart-hopping Access Point Controller.

2. Physically install, but do not power up, the Smart-hopping infrastructure components. (page 71) At this time complete all inter-component cabling connections with the exception of connecting the APs and APCs to the network. Do not connect the APs and APCs to the network until you have configured the APCs.

3. Set up your Service PC so that it may be used to connect to the Wireless Subnet. (page 71)

4. Perform initial configuration of each APC. (page 71)

5. Add the APCs to the network. (page 71)

6. Run the Philips Upgrade Tool (also known as Upgrader.exe or the Upgrader) to verify that the newly installed APCs have the same firmware revision. (page 71)

7. Using the APC web interface, verify and configure these settings: (page 71)
    a. Verify Filters
    b. Verify BootP Address Ranges
    c. Verify AP Defaults
    d. Configure AP Groups
    e. Configure Basic Settings for each Group

f. Configure Alerts for each Group

8. Perform the configuration check and replication procedure using the Philips Upgrade Tool to verify that the APCs have the same firmware revision and proper configuration settings. (page 72)

9. Add each Access Point to the Smart-hopping infrastructure, wait for it to fully power up (typically around 60 seconds), and then configure it via the APC web interface. Ensure that you have connected each Access Point to its installed Remote Antennas before connecting the Access Point to the Smart-hopping infrastructure. (page 72)
   For each Standard and Access Point you will need to:
   a. Configure the AP Name, IP Address and Group membership.
   b. Verify the AP Subnet mask, and Default gateway settings.
   c. Assign descriptive meaningful names to Access Point Remote Antennas.
   d. Save the AP configuration settings.
   e. Verify that the AP moves to Registered APs list.
   f. Disconnect and then reconnect the AP to the network.
   g. Verify that the AP is associated to the correct APC and has its IP address set correctly.

10. Change the names of installed APs and Remote Antennas from their default values to meaningful, user-friendly names. (page 102)

11. Run the Philips Upgrade Tool again to verify that the APCs and APs have the same firmware revision and proper configuration settings. (page 99)

12. Export the Smart-hopping infrastructure configuration to a disk file for archive purposes. (page 103)

13. Backup the APC configuration files (page 103)

14. Restore your service PC to its original settings. (page 71)

15. Perform network scan (page 103)

16. Enter the Smart-hopping infrastructure devices into the Information Center server configuration, and then bring the Patient Monitors online. (page 105)

4.2 Complete the Smart-hopping infrastructure installation worksheets

Photocopy and complete the following Smart-hopping infrastructure installation worksheets provided in Chapter 2 prior to installing any components:

- “Smart-hopping infrastructure Equipment Summary” on page 57
- “Smart-hopping 1.4 GHz Access Point Equipment Summary” on page 58
- “Smart-hopping 2.4 GHz Access Point Equipment Summary” on page 59
- “Layer 2 Smart-hopping APC Configuration Worksheets” on page 59
- “1.4 GHz Default AP Configuration Worksheet” on page 66
- “2.4 GHz Default AP Configuration Worksheet” on page 67
- “AP Group Configuration Worksheets” on page 69

4.3 Install the Smart-hopping infrastructure components

4.3.1 Smart-hopping component installation information

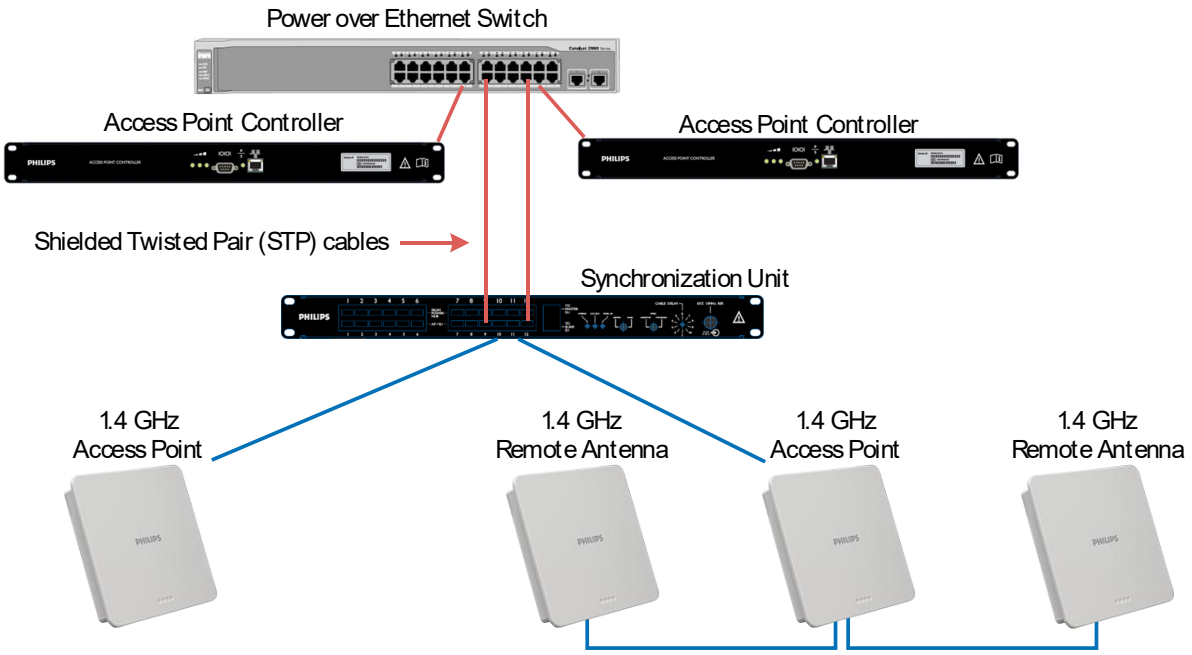


Figure 29: Smart-hopping Network Infrastructure Components

Figure 30 shows the suggested order when rack-mounting Smart-hopping infrastructure components.

4.3.1.1 Required use of shielded twisted-pair (STP) cables

STP cables enable compliance of specific components to EN 60601-1-2:2015 (IEC 60601-1- 2:2014) Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests.

When installing an Smart-hopping network, Philips requires the following LAN cables are Shielded Twisted Pair (STP) network cables (see the cables highlighted in red in Figure 29):

- Cable(s) connecting the switch to the Access Point Controller(s)
- Cable(s) connecting the switch to the Synchronization Unit (that connects to the Access Points)

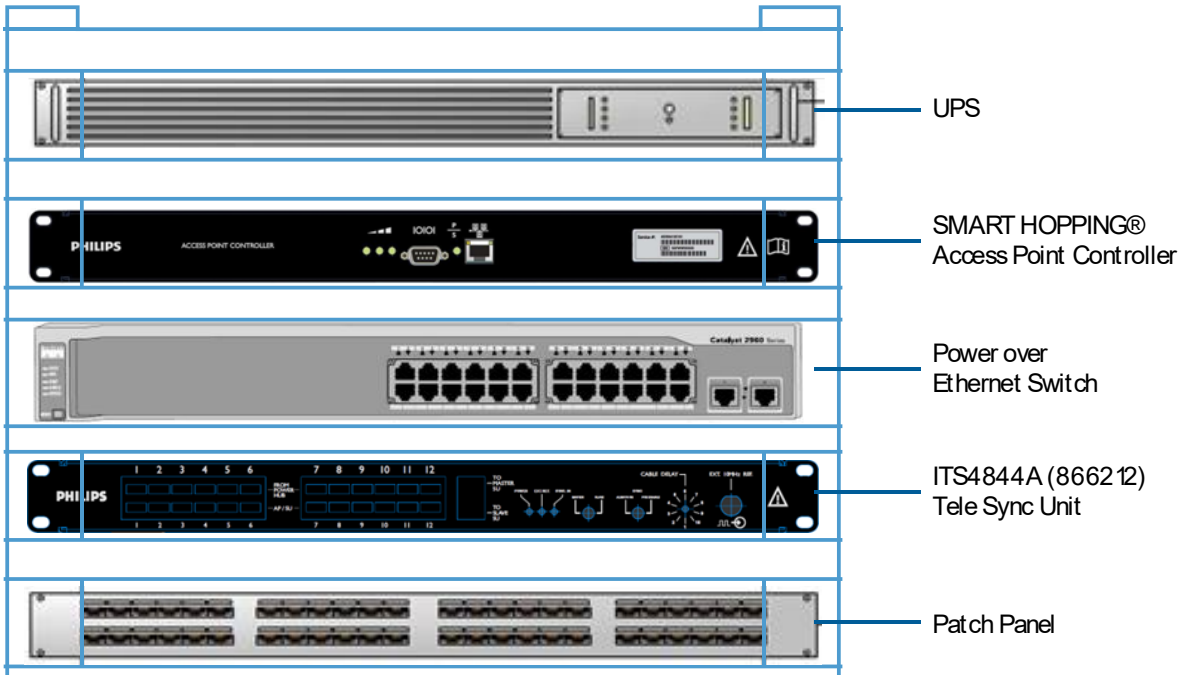


Figure 30: Rack-mounting the Smart-hopping infrastructure Components (PoE Switch)

Note It is extremely important that you power and interconnect the Smart-hopping infrastructure components only in the prescribed order. Do not power up a Smart-hopping infrastructure component or connect it to the network until instructed to do so.

To install, power, and verify operation of the 1.4/2.4 GHz Smart-hopping Infrastructure components:

1. Referring to Figure 30, mount the Smart-hopping infrastructure components in a standard 19- inch equipment rack:
    a. Mount the Smart-hopping Access Point Controller above the IntelliVue Network Switch or PoE Switch.

Note To reduce fast power line transients which can cause data loss in the system, Philips requires that the APCs are powered from a surge-protected UPS and that the APCs are connected to the switch via a shielded LAN patch cable.

    b. Mount the Synchronization Unit beneath the Power over Ethernet switch and above the UPS.

2. Mount the 1.4/2.4 GHz Smart-hopping Access Points and Remote Antennas within the clinic where they can communicate with the Patient Monitors. Note these guidelines when installing the Smart-hopping Access points:
    a. You can mount Smart-hopping Access Points to the ceiling or to a wall. Refer to the Smart-hopping 2.0 Access Point Installation Guide 1.4 GHz or the 2.4 GHz Smart-hopping Access Point Installation Guide for detailed installation procedures.

b. Use category 5e (or higher) Ethernet cable to connect each Smart-hopping Access Point to the Synchronization Unit.

c. The total length of Ethernet cable from the Smart-hopping Access point to the Synchronization Unit to the Power over Ethernet switch to the network switch cannot exceed 328 ft. (100 m).

d. Install 2.4 GHz Smart-hopping infrastructure APs a minimum of six feet (1.8 m) away from 802.11 APs.

3. If you have installed Access Points and Remote Antennas, connect the Access Points to their RAs now using the provided 74-ft. UTP-and-Coaxial cable bundles.

Caution Ensure you do not kink the RA Coax-and-UTP-cable-bundle during installation. You must maintain a minimum 3.0 inch (76-mm) bend radius for the RA Coaxial and UTP cable bundle throughout the installation.

a. Connect the first Remote Antenna to the Access Point using the UTP and Coaxial cable connectors labeled RA 1.
   i. If installing a Smart-hopping 2.0 Access Point, see Figure 31.
   ii. If installing a Smart-hopping 1.0 Access Point, see Figure 32.

b. Connect the second Remote Antenna to the Access Point using the UTP and Coaxial cable connectors labeled RA 2.
   i. If installing a Smart-hopping 2.0 Access Point, see Figure 31.
   ii. If installing a Smart-hopping 1.0 Access Point, see Figure 32.

c. Be sure to label the UTP and the Remote Antennas cable bundles as RA 1 and RA 2 corresponding to the cable connections you made in steps a and b.

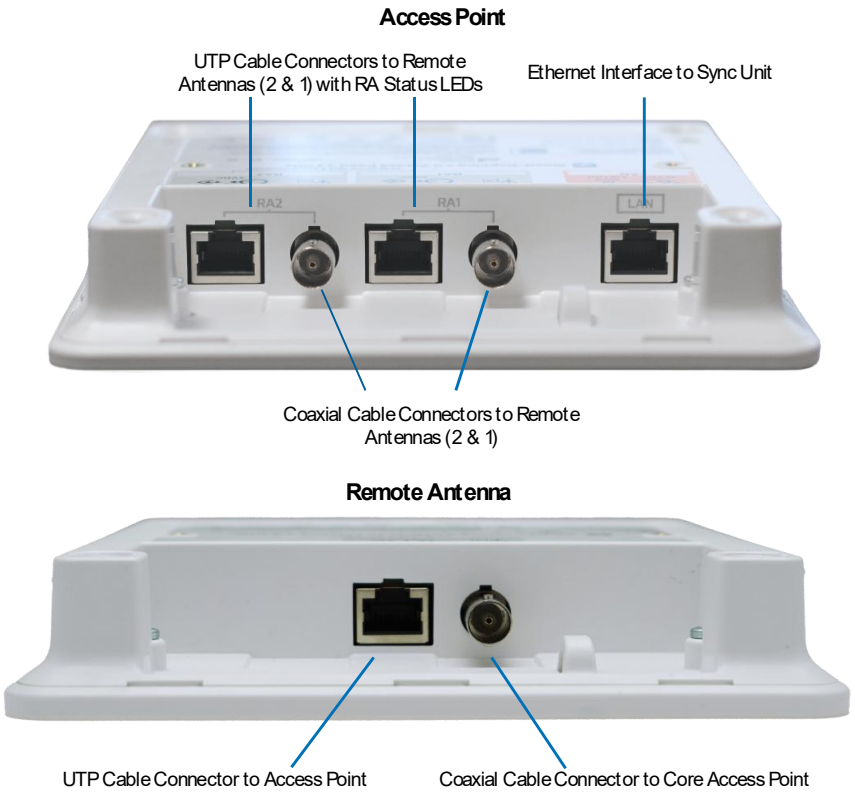


Figure 31: 1.4 GHz Smart-hopping 2.0 Access Point with Remote Antenna Controls and Connectors

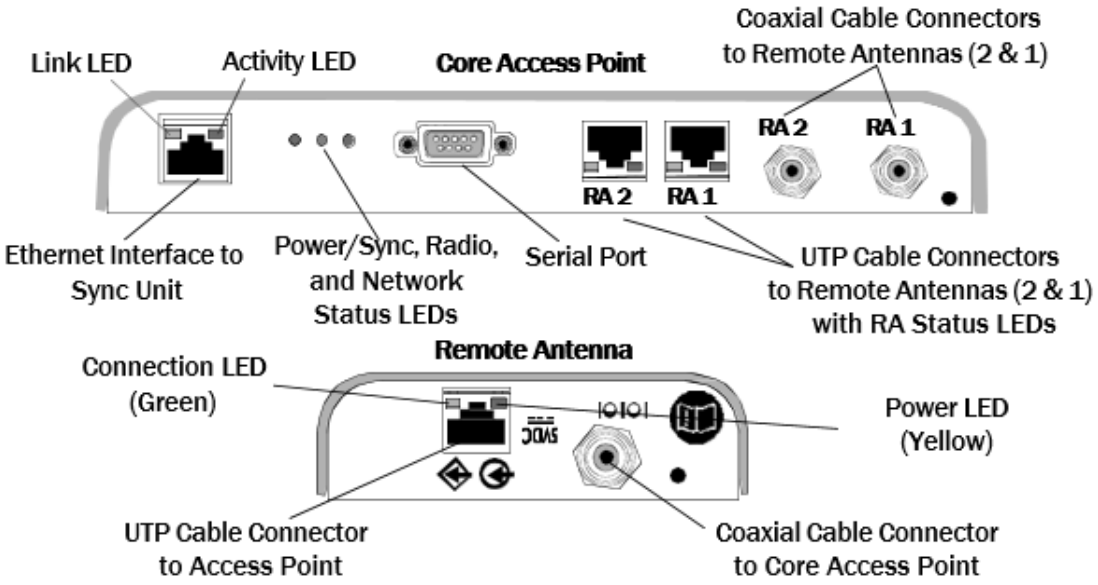


Figure 32: Smart-hopping 1.0 1.4 GHz Access Point with Remote Antenna Controls and Connectors

Figure 33: Smart-hopping 2.4 GHz Access Point

4. Route a Category 5e (or higher) Ethernet cable between each Smart-hopping Access Point and the equipment closet in which the Smart-hopping infrastructure devices are installed. Connect the routed Category 5 UTP cables to the Access Points, but do not connect these cables to the network yet. The Access Points are the last devices to be connected to the network.

Note Only for 2.4 GHz Access Points - Be sure to install a ferrite block within 20 inches (50 cm) of the RJ-45 connector that connects to the Standard or Core Access Point as shown in Figure 34.

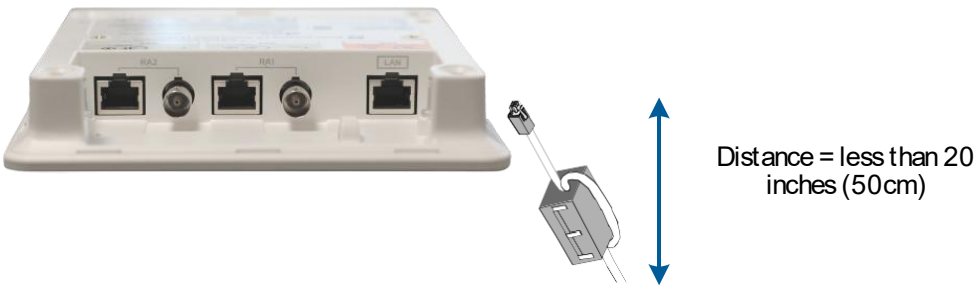


Figure 34: Installing a Ferrite Block on the Smart-hopping 2.4 GHz AP UTP Cable

5. Connect the Uninterruptible Power Supply (UPS) to an AC power source.
6. Connect and power the Power over Ethernet Switch and Synchronization Unit.
    a. For each 1.4/2.4 Access Point you have installed, connect a Category 5e (or higher) STP patch cable between a Data & Power Port on the PoE Switch and a From Hub Port (i.e., top connectors) on the Synchronization Unit.
    b. Connect the PoE Switch power cord to an available power outlet on the back of the UPS.
    c. Verify that Power over Ethernet (PoE) PoE Switch powers up properly and that its power indicator lights green.
    d. Figure 35 shows cable connections between the Power over Ethernet (PoE) switch and the IntelliVue Sync Unit to support connection of two 1.4/2.4 GHz Smart-hopping Access Points.
7. Connect and power the Synchronization Unit.
    a. Verify that for the Primary Synchronization Unit, the Primary/Secondary toggle switch is set to Primary.
    All other Sync Units in the network should have the Primary/Secondary toggle switch set to Secondary. All Secondary Sync units should have their front-panel Cable Delay Switch set as described in Table 2-6.
    b. Set the Always On/POE Enable toggle switch to the proper setting (Always On) if the Sync Unit is the Primary Sync Unit and only drives downstream Sync Units from the AP/SU ports (no APs). Otherwise, set the switch to POE Enable).
    c. Connect the Synchronization Unit power cord to an available power outlet on the back of the UPS.
    d. Verify that the Synchronization Unit powers up properly and that its power indicator lights green.

Figure 35 shows cable connections between the Power over Ethernet switch and the Synchronization Unit to support connection of two 1.4/2.4 GHz Smart-hopping Access Points.

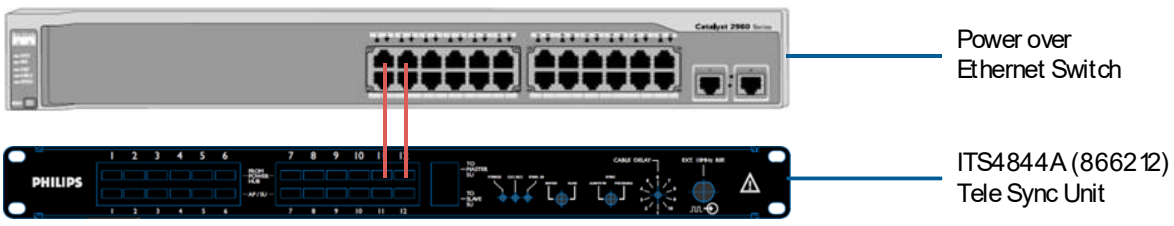


Figure 35: PoE Switch to Synchronization Unit Cable Connections

4.4 Set up your service PC

To prepare your service PC to configure the APCs, you must:

- Configure your PC to connect to the Smart-hopping Wireless Subnet used by the APCs.
- Copy the Philips Upgrade Tool and the latest Smart-hopping APC and AP firmware files to your PC from the Philips Network Infrastructure Tools files available on the Philips InCenter web site.

4.4.1 Configuring a windows PC to connect to the Smart-hopping wireless subnet

Note

The service PC must be equipped with a RS232 serial port and a terminal emulation program (such as PuTTY) to perform the initial configuration of the APCs.

If the service PC does not have an RS232 serial port, you can use a USB-to-RS232 adapter. Windows 10 does not include HyperTerminal.

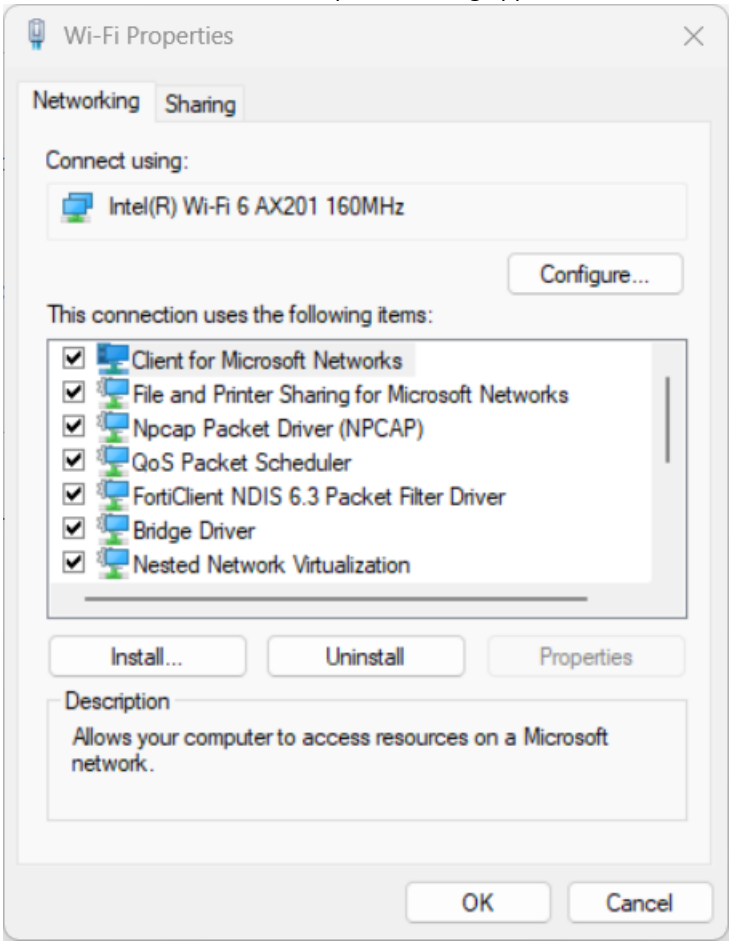
If you use PuTTY as your terminal emulation program, ensure that the backspace setting is set to “CTRL-H” and not “CTRL-?”. Refer to the PuTTY documentation for additional details.

To configure a Windows PC to connect to the Smart-hopping wireless subnet:

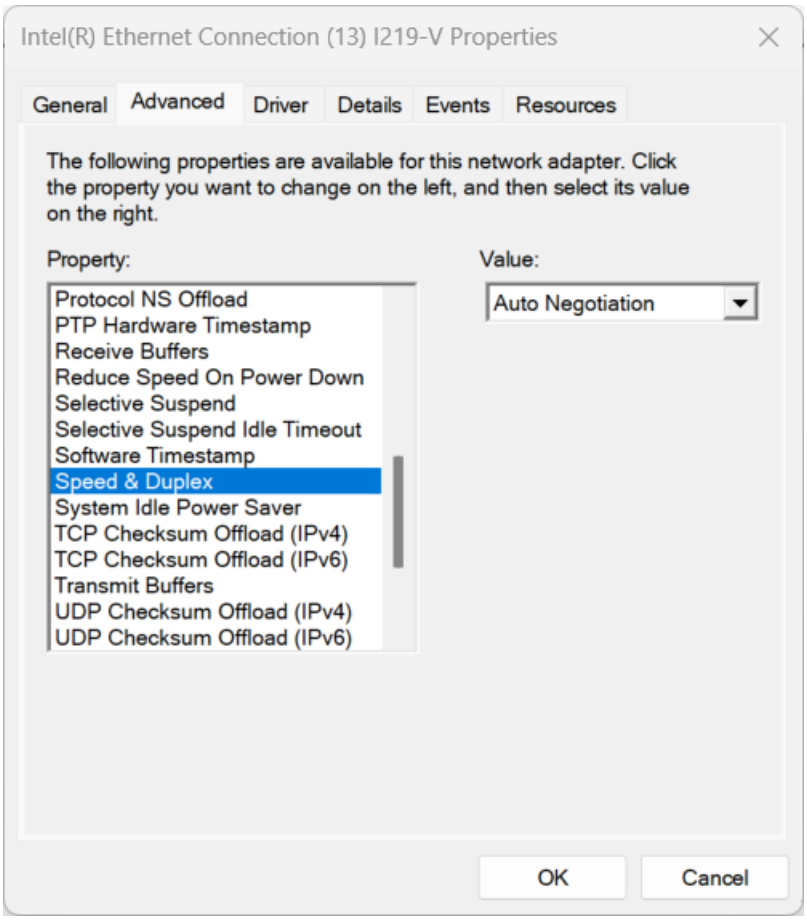
1. Configure your Service PC network adapter for Auto-negotiation (Smart-hopping 2.0 APs) or 100 Mbps, Full-duplex communications (Smart-hopping 1.0 APs), and assign a fixed IP address to your Service PC that falls within the Smart-hopping subnet address space:

Note Make sure the Speed and Duplex settings on your Service PC and the switch port are the same before connecting your Service PC to the Smart-hopping network.

a. Disconnect all network connections from your PC.
b. Select Start/Control Panel/Network and Sharing Center/Change Adapter Settings/Local Area Connection/Change Settings of this Connection.
The Local Area Connection Status dialog appears.
c. Click Properties.
The Local Area Connection Properties dialog appears.



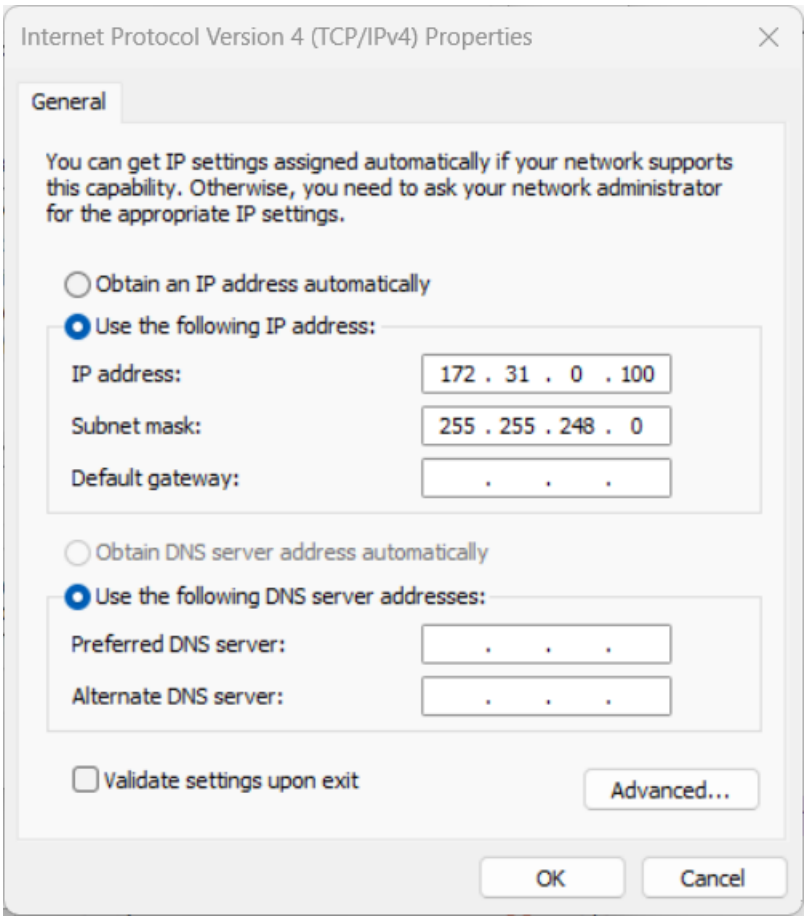
d. Click Configure and then click the Advanced tab in the displayed Properties dialog.
The advanced properties for your PC network adapter are displayed.



e. Select Speed and Duplex, the confirm that the speed and duplex settings match the settings on the switch port to which it connects. Click OK.

f. Select Start/Control Panel/Network and Sharing Center/Change Adapter Settings/Local Area Connection/Change Settings of this Connection.

g. Select Internet Protocol Version 4 (TCP/IPv4) and then click Properties. The Internet Protocol Properties dialog appears.



h. Mark the Use the following IP Address radio button, enter the following Routed or Non-Routed settings, and then click OK:
Non-routed Configuration, where “n” represents the IntelliVue Network subnet number:
   1. IP address - 172.31.(n).4 (.4 to .9 are available for Service PCs)
   2. Subnet mask - 255.255.248.0
   3. Default gateway - 172.31.(n+3).0 (IP address of DBS or M3150 PIC)
   4. Routed configuration
      a. IP address - 172.31.240.4 (.4 to .9 are available for Service PCs)
      b. Subnet mask - 255.255.240.0
      c. Default gateway - 172.31.240.1

i. Click OK at each open dialog to close the dialogs and save the Local Area Connection settings.
j. Connect the Service PC to the Smart-hopping wireless subnet.

4.5 Installing the upgrade tool

Note the following requirements for the PC on which you are running the Upgrade Tool:

- The Upgrade Tool relies on proper network communications between the Support PC on which the Upgrade Tool is run and the Smart-hopping infrastructure. Verify that there are proper connections between the Upgraded host PC and the installed APCs by running the ping command to ping all installed APCs.
- Verify that non-essential network programs are not running on the Upgrade Tool host PC (e.g., network anti-virus, firewalls, etc.). The Upgrade Tool uses TFTP which can be blocked by such non-essential network programs.

Installation instructions for the Smart-hopping device upgrade tool versions 1.0 and 2.0 are available in the Upgrading Smart-hopping Access Point Controllers and Access Points guide, available on the Philips InCenter web site.

4.6 Perform initial configuration of the APCs to be installed

Important For more information on the APC serial menu, see “Using the APC Serial Console” on page 170.

The initial configuration procedure is detailed below. All other configuration settings of the Smart-hopping Infrastructure are configured via the APC web-accessed management screens.The Access Point Controllers are shipped from Philips in a factory default state. Prior to operation on a network, each APC must have the following parameters configured via its serial port interface:

Configuration Parameter	Default Value
Static IP address	172.31.1.0
Static Subnet Mask	255.255.248.0
Static Default Gateway	172.31.3.0
Set APC to control 1.4 GHz or 2.4 GHz Access Points	1.4 GHz Smart-hopping
Select communication method - HTTP or HTTPS	HTTP
Primary APC Multicast Address (Layer 3)	239.255.254.1
Secondary APC Multicast Address (Layer 3)	239.255.254.2
APC Multicast Layer 3 (Layer 3)	Disabled
Client CI Multicast Spoof	Disabled (CI uses 224.0.23.63)
Backup APC Priority Level	0
Web user name and password	Please change passwords before first use and store them in a safe place (such as a password manager)
Serial menu console password	Philips recommends you do not change the serial console password

Table 49: Configuration parameters with default values

Warning When you reset an APC to factory defaults, wait two minutes until attempting to access the APC. The two minutes allows the configuration to save properly.

Refer to your completed APC configuration worksheet (page 59) for your planned and documented APC configurations. Repeat this initial configuration procedure for each APC to be installed and connected to the Smart- hopping wireless subnet.

Note	All Static IP address assignments for Access Point Controllers must be unique within the system. If two or more Access Point Controllers are configured with the same IP address, system behavior is unpredictable and unspecified.

4.6.1 APC configuration procedure

To perform initial configuration of an Access Point Controller:

1. Connect a serial cable between an available COM port on your service PC and the APC serial interface port.

2. Connect a power cable to the APC to power up the APC.

3. Select your terminal emulator to open a serial port session on your computer.

4. Set up your terminal emulator:
   a. Enter a name for the New Connection. Click OK.
   b. Select the COM port chosen in Step 1 from the Connect Using drop-down menu, and then click OK.
   c. Set the serial port settings as follows:
      i. Bits per second: 115200
      ii. Data bits: 8
      iii. Parity: None
      iv. Stop bits: 1
      v. Flow Control: None
   d. Click Apply, then OK.

5. Press Enter twice on the PC and enter the APC console password when prompted. The APC serial interface Main Menu (Figure 36) appears:

```
Philips AP Controller                    Main
Built date: Oct 23 2020 14:15:17.

Selection   Description                              Current Value
---------   -----------                              -------------
1           Static TCP/IP and APC Priority Settings
2           Enable 1.4/2.4GHz Smart Hopping
3           Advanced Configuration
4           APC Error Logging
5           CLIENT CI MULTICAST Spoof                disabled
6           APC MULTICAST Layer 3                    disabled
7           APC Client Gratuitous ARP                disabled
8           This APC for Primary Contention          enabled
9           Security and Advanced Parameters         disabled
10          Check APC network interface periodically disabled
11          BACKUP this APC config files
12          RESTORE this APC config files
13          Reset Configuration to Factory Defaults
14          Reset Access Point Controller
15          Snapshot PRIMARY APC current running config
16          SAFE Reset PRIMARY Access Point Controller

Enter a selection number -> 
```

D.02.23

Check firmware version

Figure 36: APC Serial Interface Main Menu

6. Check the APC firmware version displayed on the APC serial interface Main Menu and verify that the APC is running firmware which is compatible with all components of the system. If the APC is not running a compatible version of the firmware, then:
    a. Enter 1 at the main menu to change the Static TCP/IP and APC Priority Settings. Enter 1, 2, and 3, respectively to change the APC Static IP Address, Static Subnet Mask, and Static Default Gateway Address settings, and then press Enter after changing each setting. Enter Esc to return to the main menu.
    b. Disconnect and exit the console session and disconnect the serial cable from the PC and APC.
    c. Verify that you have configured your service PC with an IP address (see page 77) that will enable it to communicate directly with the APC.
    d. Connect a CAT-5 crossover cable from your service PC directly to the Ethernet In port on the front of the APC.
    e. Run the Philips Upgrade Tool (see page 99) on your service PC to load the firmware onto the APC.
    f. Close the Upgrade Tool and disconnect the CAT-5 crossover cable from your service PC and the APC.
    g. Repeat “Perform Initial Configuration of the APCs to be Installed” on page 82 from the beginning for each APC installed and connected to the Smart-hopping wireless subnet.

7. Enter the option to Reset Configuration to Factory Defaults. The APC reboots after its factory defaults have been set. After the reboot, the APC LEDs display as follows: The Primary APC changes to blinking green, and the Secondary APCs change to blinking orange.

    Warning When you reset an APC to factory defaults, wait two minutes until attempting to access the APC. The two minutes allows the configuration to save properly.

8. Verify that the option for APC Client Gratuitous ARP displayed on the APC serial interface Main Menu has a Current Value of disabled. If APC Client Gratuitous ARP does not have a Current Value of disabled, then:
    a. Enter 7 at the main menu.
    b. Enter 2 to change the Current Value to disabled.
    c. Press Esc to return to the main menu.

9. Enter 1 at the main menu to change the Static TCP/IP and APC Priority Settings. Enter the APC IP Address, Static Subnet Mask, and Default Gateway settings, and then press Esc to return to the main menu.
    a. Enter 1 to modify the APC IP Address and then press Esc.
    b. Enter 2 to modify the Static Subnet Mask and then press Esc.
    c. Enter 3 to modify the Static Default Gateway Address and then press Esc.
    d. Enter 6 to modify the Primary APC Multicast Address (may apply when running in Layer 3 mode) and then press Esc.
    e. Enter 7 to modify the Secondary APC Multicast Address (may apply when running in Layer 3 mode) and then press Esc.
    f. Enter 8 to set the Backup APC Priority Level. Set the value for the Primary APC to 0. Set the value of the Backup Primary APC to 0. Set the value for all secondary APCs to 2.
    Note The Backup Primary APC feature is only available in systems with 3 or more APCs.If all of the APCs in a system are set to a priority level of 0 (factory default), the Backup Primary APC feature is disabled. The system operates like a D.01 or C.00 system.
    g. Press Esc to return to the main menu.

10. Enter 2 at the main menu to access the Enable 1.4/2.4GHz Smart Hopping settings.
    a. Enter 1 to set the System Type to 1.4 GHz Smart-hopping, or enter 2 to set the System Type to 2.4 GHz Smart-hopping.
    b. Press Esc twice to return to the main menu.

11. Select menu option 3 to enter the Advanced Configuration sub-menu.

```
Enter a selection number -> 3


Philips AP Controller           Advanced Configuration                    D.02.23
Built date: Oct 23 2020 14:15:17.

Selection   Description                              Current Value
---------   -----------                              -------------
1           DHCP Subnet TCP/IP Settings
2           Web Configuration
3           DHCP                                     disabled
4           MAC Prefix Forwarding Filter             disabled
5           MAC Prefix Forwarding Entry              00 00 00
6           Console Password

Enter a selection number or <ESC> for previous menu ->
```

Figure 37: Advanced Configuration Menu

Use this menu option to change the configure web access, and to change the console password. Select the option and either manually enter the data or select your choice from the list. Press Enter to commit changes or press Esc to exit without saving an option change or to return to the main menu.

a. Option 1: DHCP Subnet TCP/IP Settings — This option is configured using the web browser. Please leave these settings unchanged.

b. Option 2: Web Configuration — A web server configuration menu appears.

```
Philips AP Controller          Web Configuration                      D.01.02

Selection   Description                              Current Value
---------   -----------                              -------------
1           Web Access                               enabled
2           Browser User Name                        PhilipsBD
3           Browser Password
4           Web server port number                   80

Enter a selection number or <ESC> for previous menu ->
```

   i. Enter 1 to enable Web Access to the APC. Do not change this setting; web access is enabled by default.

   ii. Enter 2 to change the Browser User Name. When prompted, enter a user name (for example, PhilipsBD).

   iii. Enter 3 to change the Browser Password. When prompted, enter a password.

   iv. Option 4 changes the Web Server port number.Philips requires that you leave the port number set to 80. **Note** This option only applies when connecting to the APC web interface over traditional HTTP (not HTTPS).

c. Options 3 - 5: Please leave these values unchanged.

d. Option 6: Console Password — Allows you to set or change the password the APC uses for serial port connections.
   Caution The default APC serial console password is a strong password. If you change the password and do not have the new password, Philips cannot recover the APC. You must then replace the APC, either by purchasing a new APC or replacing it with a spare APC.
   Note The APC has two additional serial console port security features, in addition to the password, to protect unauthorized access:
   The serial port automatically times out after 10 minutes (new feature in D.02 software)
   The APC only supports serial port connections (Telnet and SSH are unsupported) For additional security, Philips recommends placing APCs in locked areas with limited access (such as equipment closets).

e. Press Esc to exit without saving an option change or to return to the main menu.

12. To enable HTTPS communication to the APC using a web browser, enter 9 at the main menu (Security and Advanced Parameters).

a. Enter 1 to enable Security and Advanced Parameters menu items.

b. Press Esc to return to the main menu.

c. Option 10 on the main menu changes to Secure Communication via SSL. To select between HTTP and HTTPS web browser configuration, select option 10 (Secure Communication via SSL).

i. Enter 1 to enable HTTPS web browser communication; enter 2 to revert to HTTP web browser communication.
ii. Press Esc to return to the main menu.

13. If the system will be running in Layer 3 mode, enter 6 at the main menu to enable the APC Multicast Layer 3 feature.
    a. Enter 1 to enable or 2 to disable (default) the Layer 3 option.
    b. Press Esc to return to the main menu.

14. If the system uses the Philips registered multicast IP address of 224.0.23.173 for the CI (Connection Indication) message, enter 5 at the main menu to enable the Client CI Multicast Spoof feature. Enter 1 to enable the Client CI Multicast Spoof option.

15. Disconnect then exit the console session and disconnect the serial cable from the PC and APC.

16. Disconnect the power cable to power off the APC.

We suggest labeling each APC that has been configured with its configured IP address and the name you plan to configure for it via the APC web interface.

Repeat this initial configuration procedure for each APC to be installed.

4.7 Add the APCs to the network

Once you have performed the initial configuration procedure on all of the Access Point Controllers to configure their static IP address and system type (1.4 GHz or 2.4 GHz) settings for either Layer 2 or Layer 3 operation, it is now time to add the first APC to the network.

At this point, we assume that you have already configured the network switches and have identified each port on each switch to which the Access Point Controllers will be connected.

Note All switch ports to which the APCs are connected must be configured for 100 Mbps Full Duplex communications. The automatic speed and duplex configuration is unsupported.

Initially, only one APC is added to the network, and then this APC is configured. Do not add additional Access Point Controllers to the network until instructed to do so. You must power off all APCs before beginning this procedure.

Note Follow the procedure given below only when adding APCs to a new Smart-hopping infrastructure installation. If you are adding an APC to an existing Smart-hopping infrastructure then refer to “Adding APCs to an Existing Smart-hopping infrastructure” on page 113. If you are replacing an APC in an existing Smart-hopping infrastructure then refer to “Replacing an Smart-hopping APC” on page 122.

To add Access Point Controllers to the wireless subnet:

1. Identify the port on the network switch to which you will connect the first APC to be added to the network.
   The switch port must be configured for 100 Mbps Full Duplex communications. The automatic speed and duplex configuration is unsupported.

2. Connect a Shielded Category 5 (or higher) network cable between the switch port and the APC.

3. Connect a power cable to the APC to power up the APC.
   Verify that the APC LED turns flashing green after its self-test (during which the LED is blinking orange). This APC (i.e., the first installed APC) will become the Primary APC within the system. Subsequently installed APCs will be Secondary APCs within the system and will have blinking

orange LEDs post-self-test.

4. Connect to the APC web-based management interface.
   Caution The Upgrader software reports an error for any APC that has a different user ID and password from the Primary APC. Make sure all the APC login credentials match the Primary APC before running the Upgrader software.
   a. Connect your service PC to a network switch on the Smart-hopping wireless subnet.
   b. Open a web browser on the PC.
   c. Enter the static IP address of the APC in the URL field of the browser. The APC web interface appears.
      In the View Devices navigational tree, under System\AP Controllers, observe that the APC you just added to the network is listed and identified with the nomenclature APC-<mac address>.
      Note The UPGRADE button that appears in the APC management screens is not used.

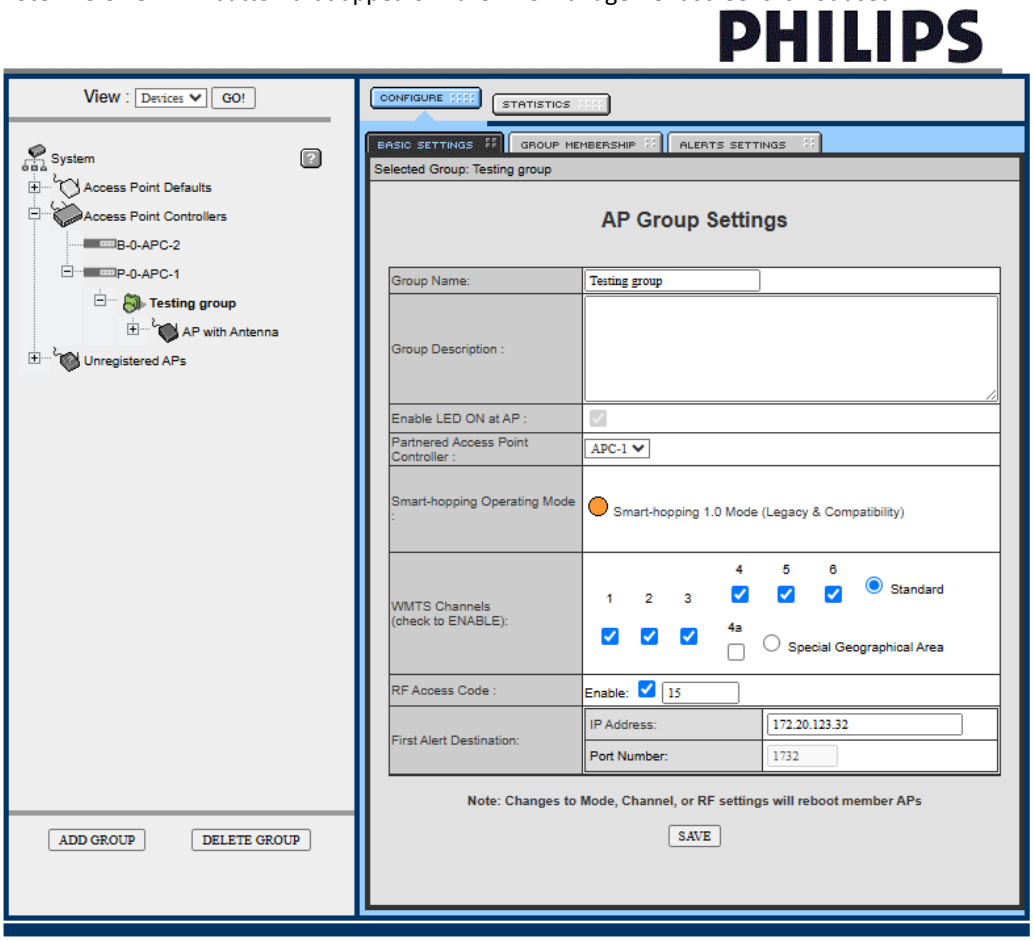


Figure 38: APC Web Interface

Note The APCs appear in the APC web interface with the System ID of Philips. Do not modify this setting.

5. Select the APC in the View Device tree (selected device is displayed green) and then select the Configure tab.
   In the AP Controller Network Configuration screen, configure the following parameters as necessary:
   a. System ID - Verify the setting is Philips. If not, change it to Philips.
   b. AP Controller Name - Enter the APC Name from APC worksheet (page 57).
   c. IP Addressing - Verify that the Specify IP radio button is marked and that the IP Address, Subnet Mask and Default Gateway settings are as expected per APC worksheet (page 57).

If not, change the settings to match the worksheet.

6. Click SAVE, and then verify the settings by selecting the Status tab.

7. At this time, add all other APCs to the network by repeating steps 1, 2, 3, 5, and 6 for each APC.

4.8 Run the Philips upgrade tool

Warning In the Smart-hopping 2.0 Upgrade Tool, clicking the Stop Service button during device upgrades can cause processes to end abruptly. This can cause instability in your device and network infrastructure.

Run the Philips Upgrade Tool to check and verify the APCs you added to the network are running the same version firmware. If any configuration modifications are made, run the Philips Upgrade Tool again.

The Smart-hopping Infrastructure Service Tool is referred to as the Upgrade Tool or Upgrader throughout this document.

The Philips Upgrade Tool has been designed to automate and simplify the upgrade process for Smart-hopping APCs and APs. In addition to upgrading the firmware on these Smart-hopping components, you can use the Upgrade Tool to:

- verify that APCs on your network are configured correctly
- display warning and error messages that you may use to troubleshoot any configuration errors that may exist on your Smart-hopping network

Note The Philips Upgrade Tool requires supported, and compatible AP and APC firmware.

Instructions for running the Smart-hopping device versions 1.0 and 2.0 Upgrade Tools are available in the Upgrading Smart-hopping Access Point Controllers and Access Points guide, available on the Philips InCenter web site.

4.9 Verify and configure important Smart-hopping infrastructure settings via the APC web browser interface

After adding the remaining Access Point Controllers to the wireless subnet, several important Smart-hopping infrastructure settings must be verified and configured via the APC web interface to ensure proper operation of the system. These include:

- Verify Filter Settings
- Verify BootP Address Ranges
- Configure the AP Defaults (for 1.4 GHz or 2.4 GHz APs)
- Configure AP Groups
- Configure Basic Settings for each Group
- Configure Alerts for each Group

Caution Before accessing the APC with a web browser and if you configured SSL encryption, make sure you installed the proper SSL certificate on the system you use to access the APC using a web browser. The certificate is available in the *SSL Certificates* folder in the same directory as the Upgrade Tool.

4.9.1 Verifying the filter settings

To verify the network filter settings:

1. In View Device tree, select System and then select the Filters tab. The Filter Configuration screen (Figure 40) appears.

2. Verify that the following network filter settings are configured as follows:
   Protocol Type Filters:
   a. IP/ARP - UNCHECKED
   b. All others - CHECKED
   Multicast Address Filter:
   c. Enable Multicast Filter – CHECKED.

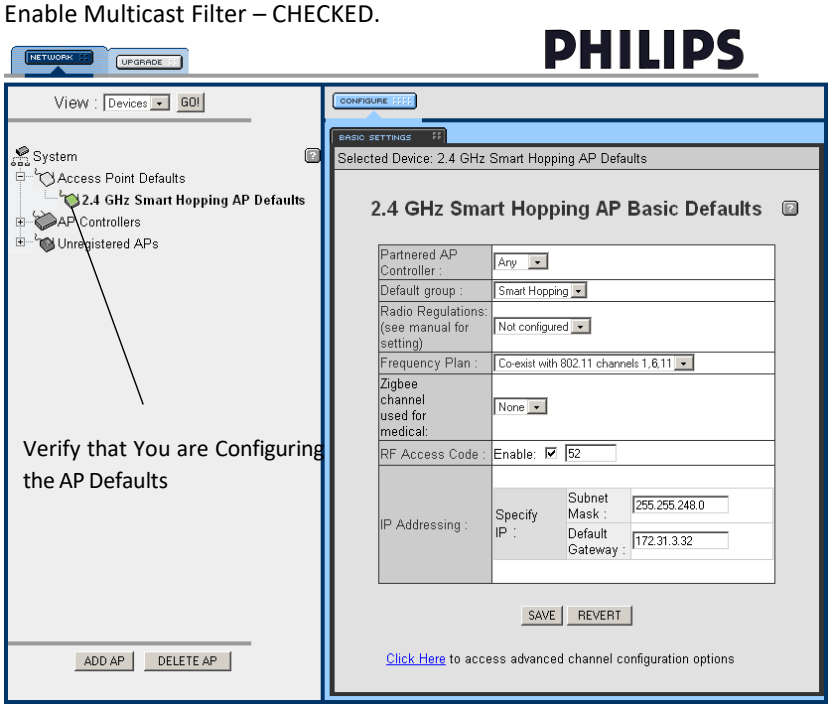


Figure 39: APC Filter Configuration Screen

   d. Multicast Address - 01:00:5E:00:00:00
   e. Multicast Mask - ff:ff:ff:ff:ff:ff
   ARP Filter:
   f. Enable ARP Filter - UNCHECKED
   g. Network IP Address - 0.0.0.0 (N/A)
   h. Network Subnet Mask - 0.0.0.0 (N/A)
   IPX Broadcast Filters:
   i. All filters - CHECKED
   j. Broadcast Bandwidth Allocation - 20%

3. If you made any changes to the Network filter settings, click SAVE and then verify the results.

4.9.2 Verifying the BOOTP/DHCP settings

Note For systems operating in Layer 3 mode, turn off the range for APs and enable routed range for all wireless clients.

To verify the BOOTP/DHCP server settings:

1. In View Device tree, select System and then select the BOOTP/DHCP tab. The BOOTP/DHCP Server Configuration screen (Figure 41) appears.

2. Verify the settings for Range 1 and Range 2 are as follows for IP address ranges for routed and for non-routed systems. Configure the settings as they are documented in your APC Configuration Worksheet (page 57). Typically, any changes to the IP address scheme are made to the following fields:
    a. IP address range minimum
    b. IP address range maximum
    c. Subnet mask
    d. Default gateway

    Non-Routed Range 1 - Patient Monitors

    a. Enabled - CHECKED for non-routed Smart-hopping infrastructure, UNCHECKED for routed Smart-hopping infrastructure
    b. MAC address Base - 00:09:fb:06:00:00
    c. MAC address Mask - ff:ff:ff:0f:00:00
    d. IP address range minimum - 172.31.(n + 6).0
    e. IP address range maximum - 172.31.(n + 6).255
    f. Subnet mask - 255.255.248.0
    g. Default gateway - 172.31. (n + 3).0
    h. DNS server IP address - 0.0.0.0

    Non-Routed Range 2 - Access Points

    a. Enabled - CHECKED for non-routed Smart-hopping infrastructure, UNCHECKED for routed Smart-hopping infrastructure
    b. MAC address Base - 00:09:fb:05:00:00
    c. MAC address Mask - ff:ff:ff:0f:00:00
    d. IP address range minimum - 172.31.(n + 2).128
    e. IP address range maximum - 172.31.(n + 2).255
    f. Subnet mask - 255.255.248.0
    g. Default gateway - 172.31. (n + 3).0
    h. DNS server IP address - 0.0.0.0

    Routed Range 1 - Patient Monitors

    a. Enabled - CHECKED for routed Smart-hopping infrastructure, UNCHECKED for non-routed Smart-hopping infrastructure
    b. MAC address Base - 00:09:fb:06:00:00
    c. MAC address Mask - ff:ff:ff:0f:00:00
    d. IP address range minimum - 172.31.248.0.

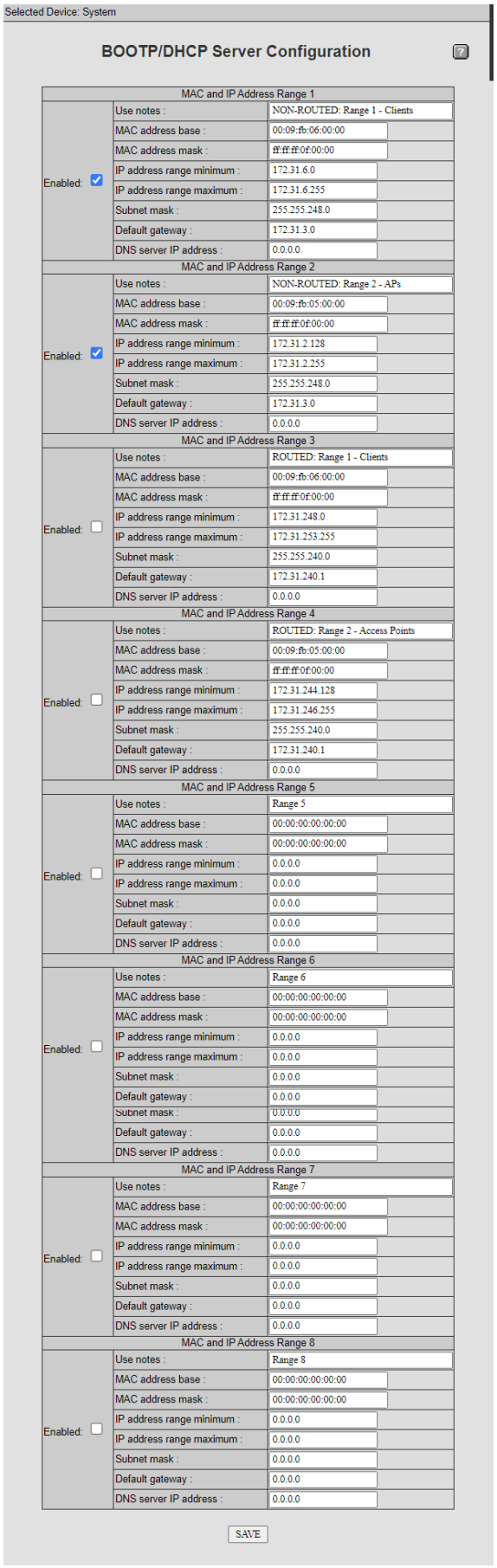


Figure 40: BOOTP/DHCP Server Configuration Screen

e. IP address range maximum - 172.31.253.255
f. Subnet mask - 255.255.240.0
g. Default gateway - 172.31.240.1
h. DNS server IP address - 0.0.0.0

Routed Range 2 - Access Points

a. Enabled - CHECKED for routed Smart-hopping infrastructure, UNCHECKED for non-routed Smart-hopping infrastructure
b. MAC address Base - 00:09:fb:05:00:00
c. MAC address Mask - ff:ff:ff:0f:00:00
d. IP address range minimum - 172.31.244.128
e. IP address range maximum - 172.31.246.255
f. Subnet mask - 255.255.240.0
g. Default gateway - 172.31.240.1
h. DNS server IP address - 0.0.0.0

Range 5

i. Enabled - UNCHECKED (always)
j. If you made any changes to the settings, click SAVE and then verify the results.

4.9.3 Configuring the Access Point Default Settings

You must configure the default Access Point settings for the APs installed at your site, either:

- 1.4 GHz Access Points
- 2.4 GHz Access Points

4.9.3.1 Configuring the 1.4GHz Access Point default settings

The next step is to configure the 1.4 GHz Access Point default settings for this installation. Refer to the information you documented on the 1.4 GHz Access Point Default Configuration Worksheet (page 66) during this step.

The default AP settings you configure here are global settings that will become the base configuration for all 1.4 GHz AP Groups you establish in the next step (refer to “Configuring AP Groups” on page 120).

To configure the 1.4 GHz Smart Hopping Access Point default settings:

1. From within View Device tree, browse to the AP Basic Defaults screen under System/Access Point Defaults/1.4 GHz Smart Hopping AP Defaults.

2. Set the Partnered AP Controller drop down list to “ANY.”

3. Set the Default Group drop-down list to Smart-hopping.

4. Set the WMTS Channels as appropriate for your geography and as documented in the 1.4 GHz Access Point Default Configuration Worksheet.
   The FCC requires that all WMTS transmitters be registered with the American Society for Healthcare Engineering (ASHE). Therefore, to be in compliance with FCC regulations, you must register your intended WMTS channel usage with ASHE prior to Smart-hopping infrastructure deployment. See “Required FCC Registration” on page 24 for details.

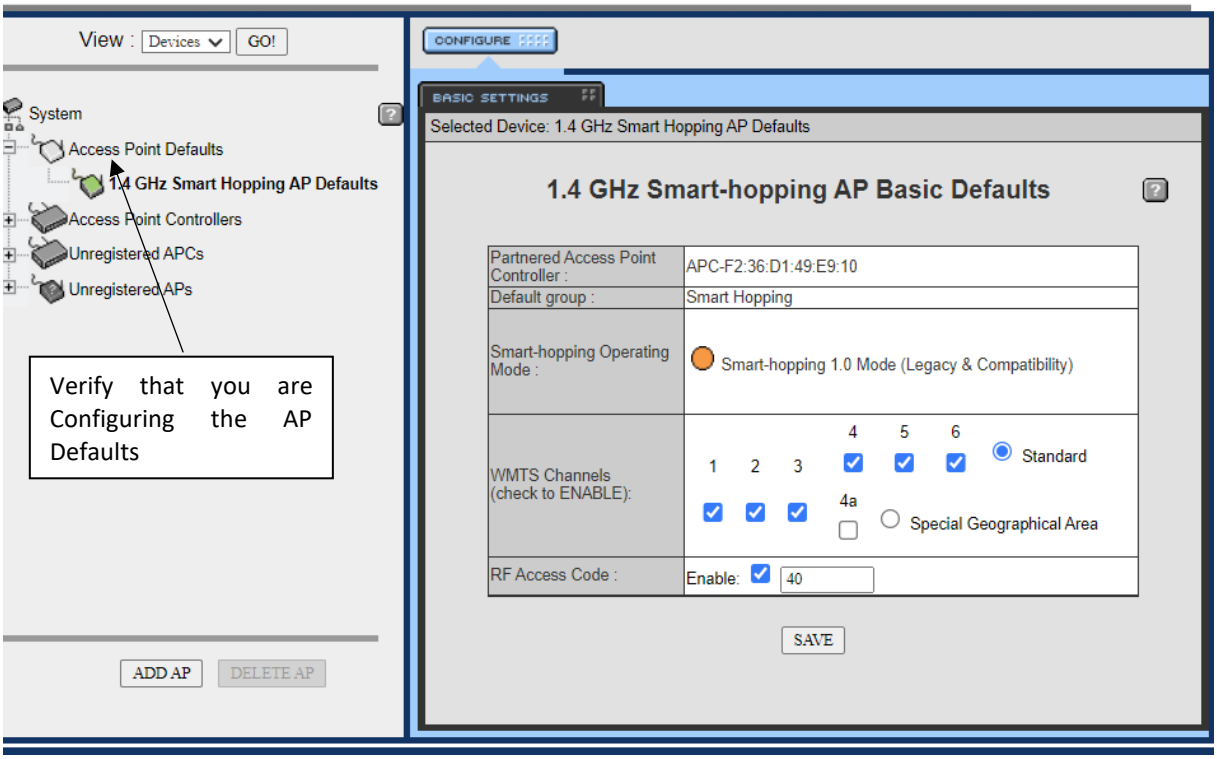


Figure 41: 1.4 GHz Smart Hopping AP Defaults Configuration Screen

Caution If you mark the Special Geographic Area radio button when installing the 1.4 GHz Smart-hopping infrastructure in a "carved-out area," then you must leave channels 4, 5, and 6 unchecked. Checking channels 4, 5, or 6 with the Special Geographic Area radio button marked results in an invalid configuration that may cause APs to continually reboot.

5. Set the RF Access Code field as documented in the 1.4 GHz Access Point Default Configuration Worksheet and set the Enable checkbox to CHECKED.

6. Set the Subnet Mask and Default Gateway fields as documented in the 1.4 GHz Access Point Default Configuration Worksheet.

7. Click SAVE and then verify the results to your expected settings.

4.9.3.2 Configuring the 2.4 GHz Access Point default settings

The next step is to configure the 2.4 GHz Access Point default settings for this installation. Refer to the information you documented on the 2.4 GHz Access Point Default Configuration Worksheet (page 67) during this step.

The default AP settings you configure here are global settings that will become the base configuration for all 2.4 GHz AP Groups you establish in the next step (refer to "Configuring AP Groups" on page 120).

To configure the 2.4 GHz Smart Hopping Access Point default settings:

1. From within View Device tree, browse to the AP Basic Defaults screen under System/Access Point Defaults/2.4 GHz Smart Hopping AP Defaults.

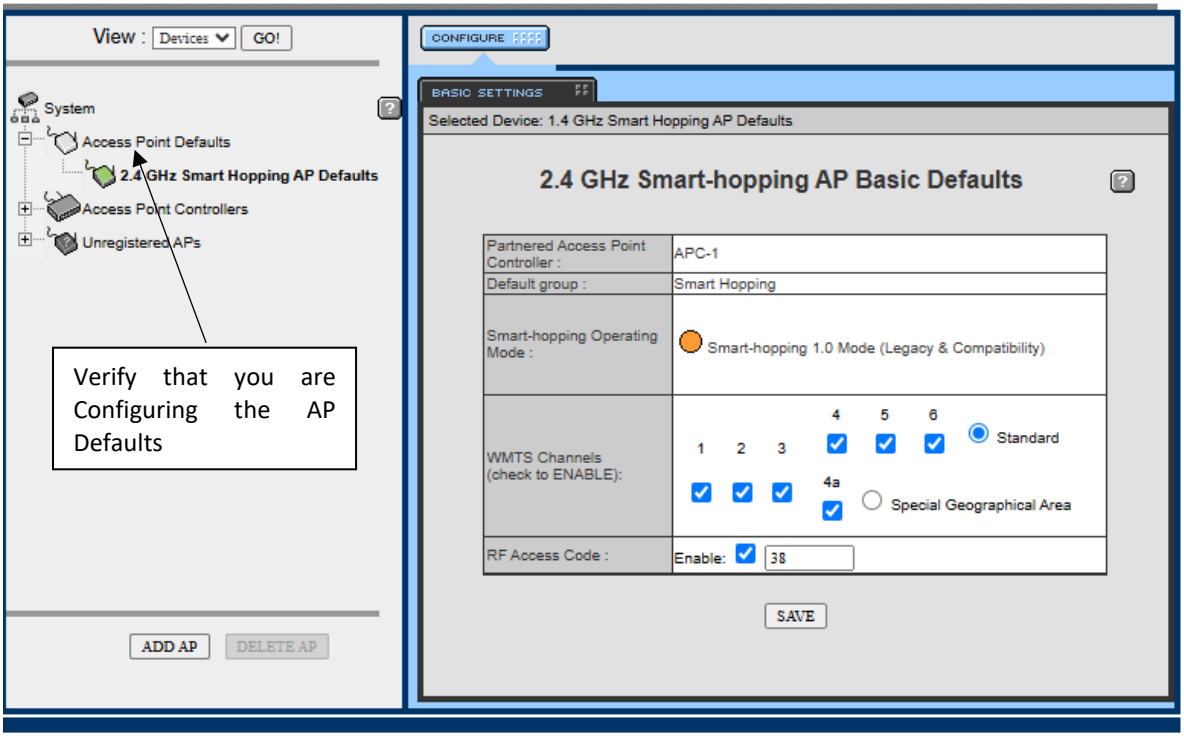


Figure 42: 2.4 GHz Smart Hopping AP Defaults Configuration Screen

2. Set the Partnered AP Controller drop-down list to “ANY.”

3. Set the Default Group drop-down list to Smart-hopping.

4. Select the Radio Regulations from the drop-down list that apply to the country in which you are installing the 2.4 GHz Smart-hopping infrastructure. Possible Radio Regulation choices are:
    a. ETSI - Europe, South America, Asia, Asia Pacific, and Africa
    b. FCC - United States, Taiwan, Singapore, and Hong Kong
    c. AS/NZ - Australia/New Zealand
    d. RSS-210 - Canada/North America
    e. ARIB – Japan

5. Select the Frequency Plan from the drop-down list to specify the 802.11b/g channel configuration with which the 2.4 GHz Smart-hopping infrastructure will co-exist. Possible Frequency Plan choices are:

Frequency Plan	2.4 GHz Smart-hopping infrastructure Channels Configured for Use	
	FCC, ARIB,RSS-210	ETSI, AS/NZ
Co-exist with 802.11 Channels 1, 6, 11	14, 28, 44, 45, 46, 47[2]	14, 28, 43, 44, 45, 46
Co-exist with 802.11 Channels 1, 7, 13	14, 15,16, 31, 32, 33[3]	14, 15, 16, 31, 32, 33
Advanced	Any set (min 3, max 6) of 2.4 GHz Smart-hopping infrastructure channels from 0 - 47, excluding any	Any set (min 3, max 6) of 2.4 GHz Smart-hopping infrastructure channels from 1 - 46, excluding any

[2] If any one of this set of six channels is disabled by the ZigBee channel selection, then channel 43 can be used instead.
[3] If any one of this set of six channels is disabled by the ZigBee channel selection, then channel 34 can be used instead.

	that have been disabled by the ZigBee selection.	that have been disabled by the ZigBee selection

Table 50: 2.4 GHz Smart-Hopping infrastructure frequency plan settings

If you select Advanced, then you must click the Click Here link at the bottom of the page to specify a minimum of three and a maximum of six channels for use by the 2.4 GHz Smart- hopping infrastructure.

6. The ZigBee channel used for medical purposes option is no longer used. The selection should be left to the default of None.
7. Set the RF Access Code field as documented in the 2.4 GHz Access Point Default Configuration Worksheet, and set the Enable checkbox to CHECKED.

8. Set the Subnet Mask and Default Gateway fields as documented in the 2.4 GHz Access Point Default Configuration Worksheet.

9. Click SAVE and then verify the results to your expected settings.

4.9.4 Configuring AP groups

The next step in the process involves establishing the AP Groups for your installation. As described in "Planning Your AP Groupings" on page 50, an AP Group allows for logically associated Access Points within a clinical unit to be given a common set of configurations. These configurations govern everything from AP-to-APC partnership rules, RF Channel and Access Code usage, and Alert Settings.

The AP Groups within the system should logically map to the Clinical Units that have been established for the monitoring network and databases.

Note Any changes you may later make to the Access Point Group settings on an installed Smart-hopping infrastructure will cause a momentary pause in monitoring for all Patient Monitors (and some AP Group setting changes may cause a longer break in monitoring).

Refer to the AP Group Configurations Worksheet on page 69 when configuring AP Groups. Complete the following steps for each AP Group to be created and configured:

1. Select the Groups View in the web interface drop-down menu and then click GO!.

2. Click ADD GROUP at the bottom left of the screen.

3. In the Add New Group screen (Figure 44), configure the following settings:
    a. Group Name - Set as documented in the AP Group Configurations Worksheet (do not use spaces in the group name).
    b. Group Type - Set to Smart-hopping.
    c. Group Description - Optional. Enter a description for this AP Group. Typically, you may want to enter the name of the clinic, unit, or department in which the APS are installed.

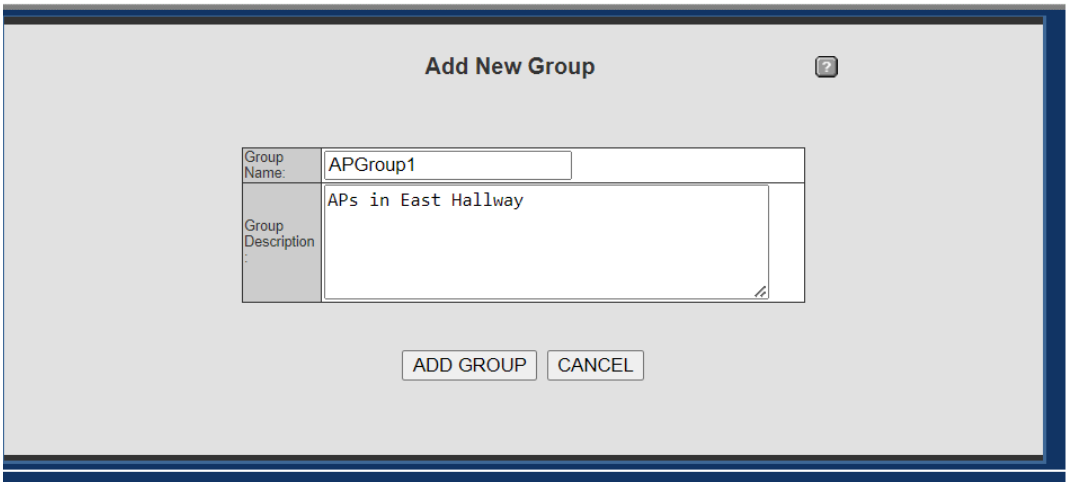


Figure 43: Adding New AP Group

4. Click the ADD GROUP button. Repeat Step 3 for each AP Group being added on this system. When all AP Groups have been added, click the NETWORK button to return to the View Groups tree screen.

For each AP Group that has been added, complete the following steps:

5. In the View Groups tree, select an AP Group that was created and select the BASIC SETTINGS tab.
   In the 1.4 GHz AP Group Configuration Basic Settings screen, set the following configuration for this AP Group:
   a. Select the appropriate APC for this AP group from the Partnered AP Controller drop-down list. Refer to your completed AP Group Configuration Worksheet.

   In the 1.4 GHz AP Group Configuration Basic Settings screen, verify the following configurations for this AP Group. If they are not correct, delete the AP group and then edit the AP default settings (see page 88):
   b. Set the WMTS Channels as appropriate for your geography and as documented in the 1.4 GHz Access Point Default Configuration Worksheet.
   c. Set the RF Access Code field as documented in the 1.4 GHz Access Point Default Configuration Worksheet and set the Enable Box to CHECKED.
   d. Set the Subnet Mask and Default Gateway fields as documented in the 1.4 GHz Access Point Default Configuration Worksheet.

   In the 2.4 GHz AP Group Configuration Basic Settings screen, set the following configurations for this AP Group:
   e. Select the appropriate APC for this AP group from the Partnered AP Controller drop-down list. Refer to your completed AP Group Configuration Worksheet.

   In the 2.4 GHz AP Group Configuration Basic Settings screen, verify the following configurations for this AP Group. If they are not correct, delete the AP group and then edit the AP default settings (see page 88):
   f. Select the Radio Regulations from the drop-down list that apply to the country in which you are installing the 2.4 GHz Smart-hopping infrastructure as documented in the 2.4 GHz AP Default Configuration Worksheet.
   g. Select the Frequency Plan from the drop-down list to specify the 802.11 channel configuration with which the 2.4 GHz Smart-hopping infrastructure will co-exist.
   h. The ZigBee channel used for medical purposes option is no longer used. The selection should be left to the default of None.

i. Set the RF Access Code field as documented in the 2.4 GHz Access Point Default Configuration Worksheet and set the Enable Box to CHECKED.
j. Set the Subnet Mask and Default Gateway fields as documented in the 2.4 GHz Access Point Default Configuration Worksheet.

6. Click SAVE and then verify that the AP Group Basic Configuration settings are correct.

7. Select the ALERTS SETTINGS tab.

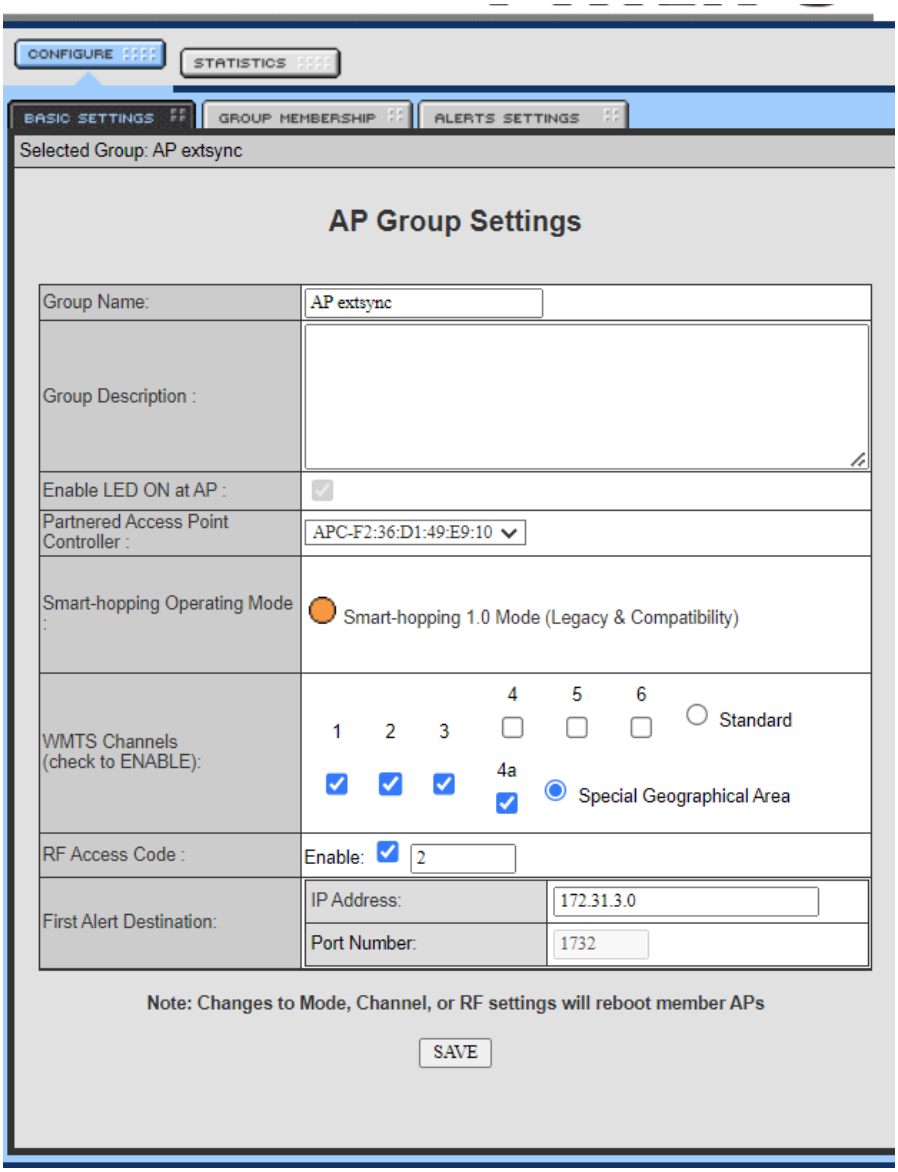
8. 

Figure 44: AP Group Configuration Alert Settings

In the AP Group Configuration Alerts Settings screen, set the following configurations for this AP Group:

- Alert Destination - Set as documented in the AP Group Configuration Worksheet.
- Sync Loss Alert - Verify all boxes are CHECKED.

9. Click SAVE and then verify the AP Group Alerts Configuration settings are correct.
Select the ALERTS SETTINGS tab again. In the AP Group Configuration Alerts Settings screen, click on the Click Here link at the bottom of the screen to display the AP Group Configuration Advanced Alerts Settings screen (Figure 46). and (Figure 47).

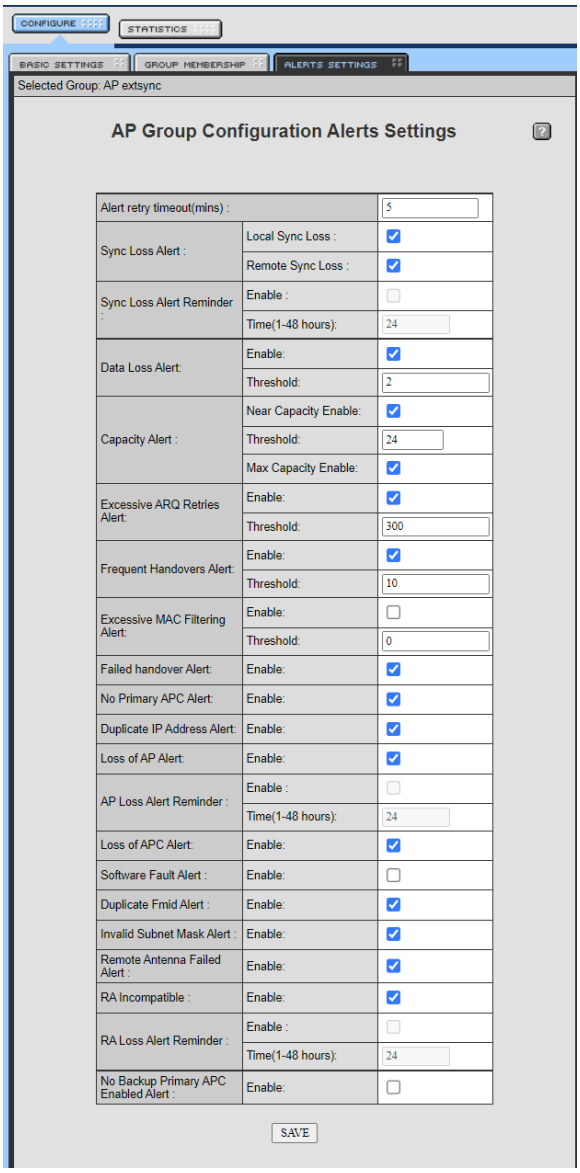


Figure 45: AP Group Configuration Advanced Alert Settings

Figure 46: AP Group Configuration Advanced Alert Settings

NOTE: The Insufficient Spectrum Alert Settings are Only Displayed for and Apply to 2.4 Ghz Access Point

10. Click **SAVE** and then verify the AP Group Configuration Advanced Alerts Results page.

11. Repeat Steps 5 - 10 until you have configured every AP group that you have added to the system.

For the upgrade options in this dialog box, choose these specific options for each respective selection.

4.10 Run the Philips upgrade tool again

Prior to running the Upgrade Tool, close and exit your web browser.

This step is only necessary if there are APCs which still require upgrading.

Run the Philips Upgrade Tool to check and verify the APC configurations, and fix any errors as needed. If any configuration modifications are made, run the Philips Upgrade Tool again.

Instructions for running the Smart-hopping device versions 1.0 and 2.0 Upgrade Tools are available in the Upgrading Smart-hopping Access Point Controllers and Access Points guide, available on the Philips InCenter web site.

4.11 Add APs to the network

Note We recommend that you add your installed APs to the Smart-hopping network in groups of up to 25 APs at a time by following the procedure given in this section. After adding the APs as described here, complete “Rename Installed APs and Remote Antennas” on page 102 and Step 12. Run the Philips Upgrade Tool Again for the newly added APs. Continue to add APs and complete Steps 10 and 11 for the newly added APs until you have added all installed APs to your Smart-hopping network.

After you have run the Philips Upgrade Tool to verify the APC configurations, it is time to add the Access Points to the network. At this point, it is assumed that you have already installed and configured the wired components of the Smart-hopping infrastructure, and you have identified each port on each network switch to which the Access Points will be connected (via the Sync Unit and PoE switch cable connections to the switch described starting on page 57).

- Smart-hopping 1.0 Access Points require a 100 Mbps/Full Duplex switch port connection
- Smart-hopping 2.0 Access Points require the switch port speed and duplex be set to auto- negotiate

Ensure that Access Points are connected to their Remote Antennas when the Access Points are initially added to the Smart-hopping infrastructure.

Upon connection to the Power over Ethernet switch, Access Points (and connected Remote Antennas) will be automatically added to the View Devices tree of the network in the APC management screens. Each Access Point must then be individually configured for proper operation in the system.

Complete the following procedure for each AP to be added to the Smart-hopping infrastructure. To add an Access Point to the Smart-hopping infrastructure:

1. Re-launch your web browser and reconnect to the APC web interface.

2. Route and connect a network patch cable between the Access Point and the Sync switch. (See page 57for illustrations of and instructions for making these cable connections.)
   Wait 60 seconds before proceeding.
   Once power is applied, the Access Point (and Remote Antennas) will take approximately 60 seconds to fully boot and will automatically appear in the View Devices tree of the APC web interface under any AP Controller.
   By default, the Remote Antennas are labeled as AP-1-ID#### (AP-port 1-remote antenna ID) or AP-2-ID#### (AP-port 2-remote antenna ID) where ID#### matches the ID number printed on the Remote Antenna device label.

Press F5 to refresh the APC web interface if the AP is not displayed.
If the AP is still not displayed, click System in the View device tree, click Configure and then select the Advanced tab. Verify that the Allow new APs to be added automatically option is set to True.

3. Find the Access Point and select it in the View Devices tree. It should be named AP- mac_address and be listed under an APC in the list.

4. In the AP Configuration screen for this Access Point, select the Basic Settings tab and then configure the following settings:
   1.4 GHz Smart-hopping AP configuration screen:
   a. Set the AP Name as appropriate for this AP.
   b. Set the Enable AP checkbox to CHECKED.
   c. Verify that the Partnered AP Controller is set to "ANY." The Partnered APC will get set correctly based upon the AP Group membership setting.
   d. Set the Group Membership as appropriate for this AP.
   e. Verify that the WMTS Channels are set as appropriate for your geography. The WMTS Channels are set in the AP default settings.
   f. Verify that the RF Access Code is set correctly. The RF Access Code is set in the AP default settings.

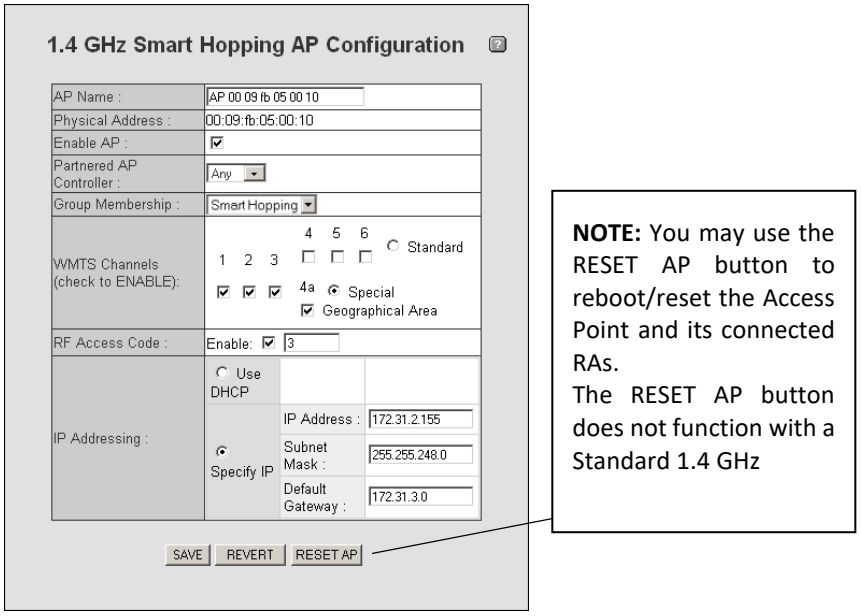


Figure 47: 1.4 GHz Smart Hopping AP Configuration Screen

   g. Set the RF Access Code Enable Box to CHECKED.
   h. Mark the Use DHCP or Specify IP radio button as appropriate for your network. When specifying the IP address, note that the Subnet Mask and Default Gateway fields are populated with the default values set in the AP default settings.
   i. If using Layer 3, you must use DHCP.

2.4 GHz Smart-hopping AP configuration screen:

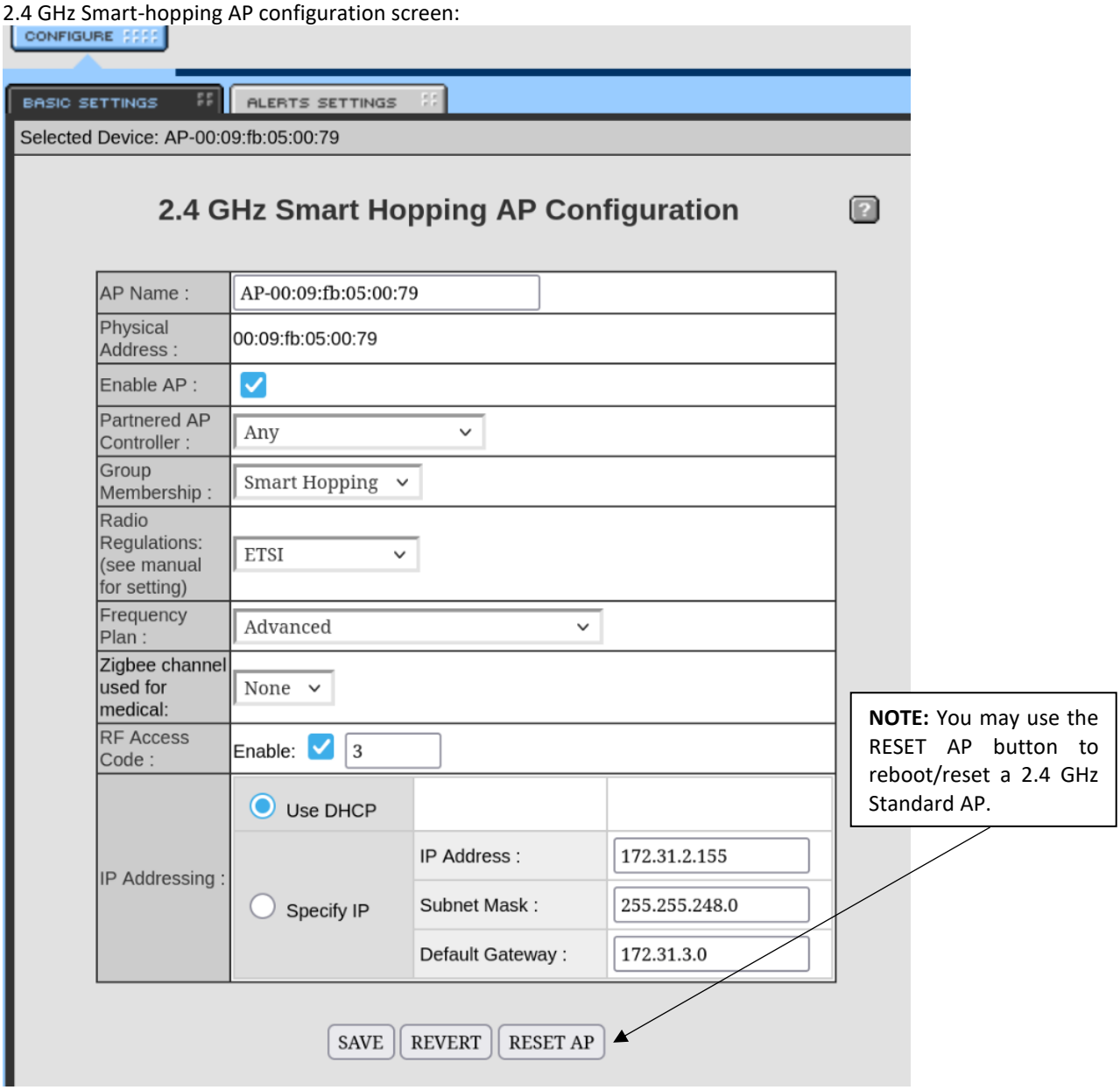


Figure 48: 2.4 GHz Smart Hopping AP Configuration Screen

j. Set the AP Name as appropriate for this AP.
k. Set the Enable AP checkbox to CHECKED.
l. Set the Partnered AP Controller drop-down list to “ANY.” The Partnered APC will get set correctly based upon the AP Group membership setting.
m. Set the Group Membership as appropriate for this AP.
n. Select the Radio Regulations as specified in the 2.4 GHz Default AP Configuration Worksheet.
o. Verify that the Frequency Plan is set correctly for this AP. The Frequency Plan is set as part of the AP default settings.
p. The ZigBee channel used for medical purposes option is no longer used. The selection should be left to the default of None.
q. Verify that the RF Access Code is set correctly. The RF Access Code is set in the AP default settings.
r. Set the RF Access Code Enable Box to CHECKED.
s. Mark the Use DHCP or Specify IP radio button as appropriate for your network. When specifying the IP address, note that the Subnet Mask and Default Gateway fields are populated with the default values set in the AP default settings.
t. If using Layer 3, you must use DHCP.

5. Click SAVE and then verify the AP Configuration settings.

6. Refresh Internet Explorer (by pressing F5), and in the View Devices tree, verify that the AP appears under the correct Access Point Controller.
   This may take several minutes and in the process; the Access Point may appear (for a moment) in the Unregistered List of the View Devices tree. If after five minutes the Access Point remains in the Unregistered List of View Devices tree, select the Access Point in the Unregistered List and click the Delete AP button at the bottom of the page. Remove power to the Access Point and repeat this procedure beginning from Step 1.
7. Disconnect the AP from the Sync Unit, and then reconnect it.
   This will recycle power to the AP and enable the AP to load its configuration properly.
8. Click on the STATUS tab for the newly added AP and verify that the IP shown for that AP is correct. If not, remove power to the AP and then check and verify the status again.
9. Repeat the above steps for all other APs to be added to the Smart-hopping infrastructure.

4.12 Rename installed APs and remote antennas

You can change the names of installed Standard Access Points and Remote Antennas from their default values to more user-friendly names by following these steps:

1. Click on the APC in the APC web interface that is associated with the APs you wish to rename.
2. Click the NAMES tab.
   The AP and Remote Antenna Friendly Name Management screen appears as shown in figure 50.

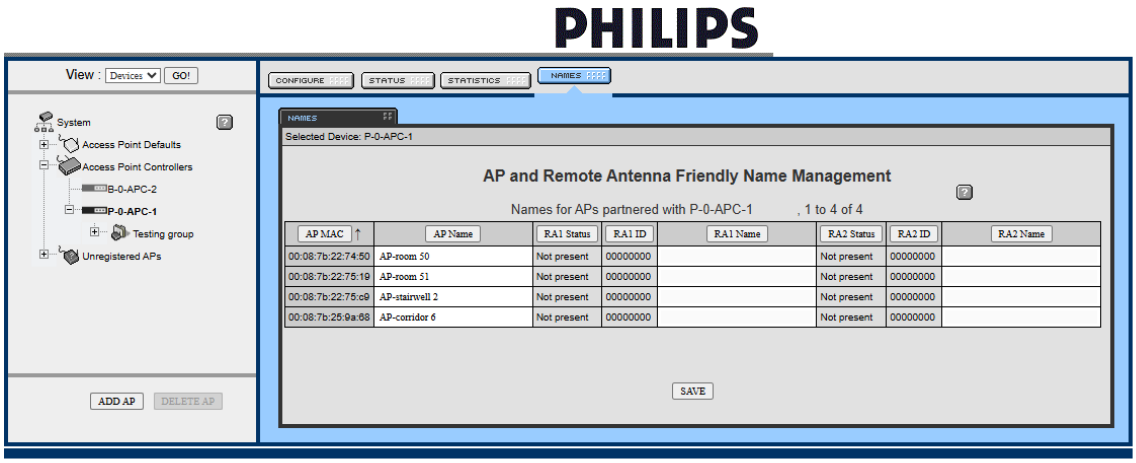


Figure 49: Renaming APs and RAs

3. Enter meaningful, user-friendly names for the installed Standard Access Points and Remote Antennas in the AP Name and RA Name fields.
   a. You may enter a string of up to 32 characters for the name values.
   b. First-generation Access Points display Remote Antennas as Not Present.
   c. Second-generation (and later) Access Points list Remote Antennas and provide the general status of connected Remote Antennas.
4. Click SAVE and then verify the AP Configuration settings.

4.13 Run the Philips upgrade tool again

This step is only necessary if there are APCs and APs which still require upgrading.

Run the Philips Upgrade Tool again to check and verify final APC and AP configurations, and fix any errors as needed. If any configuration modifications are made, run the Philips Upgrade Tool again.

Instructions for running the Smart-hopping device upgrade 1.0 and 2.0 Upgrade Tools are available in the Upgrading Smart-hopping Access Point Controllers and Access Points guide, available on the Philips InCenter web site.

4.14 Export the Smart-hopping infrastructure configuration to a disk file

You can export a system configuration from an Access Point Controller to a disk file and import a previously exported configuration file to an Access Point Controller by running the Upgrade Tool.

Note Before exporting any configuration files, you must run through the Upgrade Tool configuration checking process and correct any errors that are found. If you do not correct errors prior to exporting the configuration, the exported archive will contain errors.

To export the Smart-hopping configuration to a file in both human- and machine-readable formats:

Export a Configuration File (Smart-hopping 2.0)
Run the Smart-hopping 2.0 Upgrader tool to get an export file. From the Service Actions drop-down list, select the APC: Check and Export APC Configuration option.

For more information on the Smart-hopping 2.0 Upgrade Tool, see the Upgrading Smart-hopping 2.0 Access Point Controllers and Access Points guide.

Export a Configuration File (Smart-hopping 1.0)
Run the Smart-hopping 1.0 Upgrader tool to get an export file. For more information on the Smart-hopping 1.0 Upgrade Tool, see the Upgrading Smart-hopping Access Point Controllers and Access Points guide.

4.15 Backup the APC config files

This step applies to Release D.01 or greater APCs.

1. Connect a serial cable between an available COM port on your service PC and the APC serial interface port.

2. Open a Terminal session on your computer.

3. Press Enter twice on the PC and enter the APC console password when prompted. The APC serial interface Main Menu (Figure 36: APC Serial Interface Main Menu) appears:

4. Enter 11 to backup the APC config files.

4.16 Perform network scan

The Network Scan tool in the Philips Information Center server discovers all of the APCs and APs on the system and creates the database entries for them.

When you export files using the Upgrader Tool, the process places the following files and folders into the exports folder (located in the same directory as the upgrader.exe file:

- The APC configuration file (export_YYYYMMDD-HHMMSS.txt)
- An additional file (export_YYYYMMDD-HHMMSS.CSV), an equipment inventory list

- A folder (YYMMDD-HHMMSS), that contains copies of the configuration files (in binary format), used for importing Smart-hopping devices into the PIC iX system Network Scan

Caution Using the Network Scan tool on a live Philips Information Center (PIC) system is not recommended as it requires a reboot of all PIC systems once the scan completes, to reconnect them to the Database server. This can cause data loss.

This does not apply to the PIC iX servers.

Note If your APC is operating using the HTTPS protocol, network scans from the Philips Patient Information Center server fail. To resolve this, do the following:

- If you run PIC iX C.03 you can run the Network Scan using the binary files located in a subdirectory of the exports folder (YYYYMMDD-HHMMSS).
- For other versions of PIC and PIC iX software, use the console serial port menu to disable the HTTPS protocol use, and remove the web user ID and password. This allows the Network Scan feature to operate properly.

Table 51 shows the APC version, PIC or PIC iX software version, and whether they support performing a network scan using HTTP or HTTPS.

APC version and HTTP or HTTPS	PIC classic all versions	PIC iX B.xx, C.02, C.02	PIC iX C.03 (and higher)
APC C.00 - HTTP (no username and password)	Compatible	Compatible	Compatible
APC D.01 - HTTP (no username and password)	Compatible	Compatible	Compatible
APC D.02 - HTTP (no username and password)	Compatible	Compatible	Compatible
APC D.02 - HTTP (using a username and password)	Not Compatible	Not Compatible	Compatible
APC D.02 - HTTPS (using a username and password)	Not Compatible	Not Compatible	Compatible - requires using an APC export file

Table 51: Automatic network scan of APC and AP devices compatibility

1. Before you run the network scan, make sure your HTTP user configuration matches the requirements listed in Table 3-3.
    a. If performing a network scan using PIC iX version C.02 or earlier and you have a web server (HTTP) user name and password set on your APCs, do the following to avoid network scan errors:
        i. If the APC has an existing user name and password, use the console serial port menu to remove the HTTP user ID and password. If the APC has no HTTP login configured, wait until after the network scan to configure it.

2. Obtain the Primary APC IP address information from the APC Web Browser for the Network Scan.

3. Close the APC Web Browser. The APC Web Browser must be closed before starting the Network Scan.

4. From the PIC or PIC iX There should be no APCs present in the Equipment list for this Smart- hopping network.

    Warning Do not run the Upgrader Tool during a network scan or system disruption can occur.

5. In this step, you run the network scan.
    a. If performing a network scan using PIC iX version C.02 or earlier:
        i. From the PIC or PIC iX server, run the network scan. Enter the Primary APC IP address when prompted.
    b. If performing a network scan using PIC iX version C.03 or higher:

i. If running the APC using HTTP - From the PIC or PIC iX server, run the network scan by selecting Scan Device. When prompted, enter the Primary APC IP address. When prompted, enter the user ID and password.
ii. If running the APC using HTTPS - run the network scan by selecting Scan Device, click the Import button, and navigate to the YYYYMMDD-HHMMSS folder that contains the configuration files (in binary format).

6. (Optional) After the scan completes, you can enable HTTPS support to use HTTPS to communicate with the APC (this requires a browser user ID and password).

7. If you use HTTP to communicate with the APC, you can configure the web browser user ID and password.

Note The APC name that is scanned into the PIC iX configuration depends on the PIC iX revision and if the APC is using HTTP or HTTPS. The APC web browser interface view displays APC names, along with the current role of the device and its priority setting. This impacts what you see on the PIC iX server after the network scan completes. You can edit the names for consistency. See Table 3-4 for more information on the imported APC names.

Web browser	PIC iX B.xx, C.01, or C.02 network scan	PIC iX C.03.01 network scan	PIC iX C.03.01 network scan using export file	In PIC iX, edit name for consistency (optional)
	HTTP	HTTP	HTTPS	
B-0-APC2	B-0-APC2	B-0-APC2	APC2	APC2
P-0-APC1	P-0-APC1	APC1	APC1	APC1
S-2-APC3	S-2-APC3	S-2-APC3	APC3	APC3
S-2-APC4	S-2-APC4	S-2-APC4	APC4	APC4

Table 52: APC names on PIC iX after network scan

Note When adding Smart-hopping telemetry devices (such as Access Points or Access Point Controllers), the list of APCs and APs imports when you run a network scan on a PIC iX server. Manually entering Smart-hopping APC and AP information may cause duplicate or non-existent devices to appear in the Focal Point inventory. This may cause duplicate or erroneous statistical and alert data to appear in Focal Point.

4.17 Install patient monitors

Once you have completed all of the steps to install the Smart-hopping infrastructure, you can add wireless clients into the Information Center configuration. You can then configure the wireless clients for use by using the Label Assignment function from the Philips Information Center server.

Turn on Patient Monitors that have been configured for use (i.e. equipment labels have been assigned in the Philips Information Centers, and equipment labels and RF Access Code have been set in the IPMs). The IPMs should associate with APs in the system and begin to pass data to the central station displays.

5 Expanding or modifying an installed Smart-hopping infrastructure

This chapter provides procedures to expand or modify an existing, installed Smart-hopping infrastructure, and includes:

- Upgrading the APC and AP Software
- Expanding an Installed Smart-hopping Infrastructure
- Smart-hopping infrastructure Expansion Prerequisites
- Archiving the Configuration Files
- Upgrading Smart-hopping APCs and APs Using the Philips Upgrade Tool
- Adding APCs to an Existing Smart-hopping infrastructure
- Adding APs to an Installed Smart-hopping infrastructure
- Adding Patient Monitors
- Replacing an AP, Remote Antenna, or APC in an Existing System

5.1 Upgrading the APC and AP software

For detailed instructions on upgrading APC and AP software, see the Upgrading Smart-hopping Access Point Controllers and Access Points, available on the Philips InCenter web site.

5.2 Expanding an installed Smart-hopping infrastructure

This section describes the Smart-hopping Infrastructure expansion scenarios and procedures. We assume that you will execute these procedures only on an installed and fully functional Smart-hopping infrastructure.

Expanding an installed Smart-hopping infrastructure has three facets:

- Adding APs to the Smart-hopping infrastructure
- Adding APCs to the Smart-hopping infrastructure
- Adding AP Groups to an Smart-hopping infrastructure Configuration - While this is not a hardware expansion, adding additional AP Groups to the system configuration might be common in a system where APs were being added. AP Group additions to the configuration without the addition of APs is considered a re-configuration exercise and is not covered in this document.

The scope of the system expansion needs to be analyzed to determine the proper sequence of events. The flow chart below identifies and facilitates the approach to system expansion and the order of the tasks that must be completed.

Prior to expanding an installed Smart-hopping infrastructure, be sure you have properly documented the expansion by modifying the Smart-hopping infrastructure Installation Worksheets for the site.

The general flow of tasks associated with an Smart-hopping infrastructure expansion is shown in Figure 51.

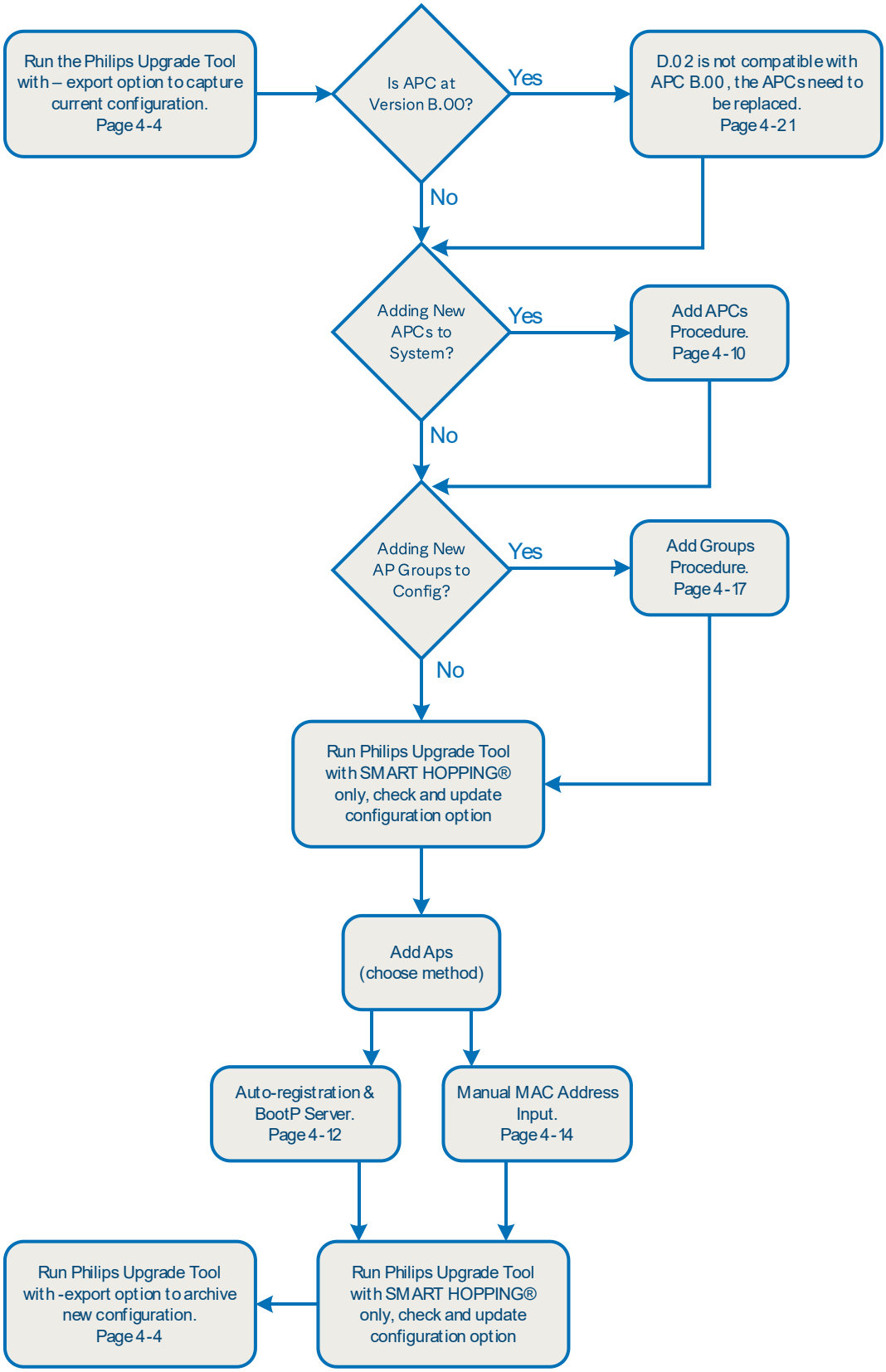


Figure 50: Smart-hopping infrastructure Expansion Tasks

5.3 Smart-hopping infrastructure expansion prerequisites

Note Implementing and executing any of the expansion procedures listed in this Chapter will cause interruptions to monitoring if the system is "live"—i.e., if the Smart-hopping infrastructure is up and running and monitoring patients. Changing APC mastership relationships or AP/APC partnering will cause monitoring interruptions. You must notify the hospital staff of all planned service events to the Smart-hopping Infrastructure prior to implementing these service events.

Note the following requirements you must complete prior to expanding or modifying a Smart-hopping infrastructure:

1. Define the expanded RF coverage area. You may need to conduct an additional RF survey to ensure proper coverage for the additional area. See Chapter 2 for details.

2. Install additional network switching infrastructure as required for new coverage area. See Chapter 2 for details.

3. Expand the Sync network as required to support additional APs. See Chapter 2 for details.

4. APCs in the system running A.00 or B.00 code indicate they are 862147 APCs (serial console and LAN connections on rear of device). These are not compatible with D.02. Before upgrading to D.02 software, you must replace all 862147 APCs with the 865346 APC (serial console and LAN connections on front). For more information on replacing APCs, see "Replacing an AP, Remote Antenna, or APC in an Existing System" on page 122.

5. Export the current configuration to a service PC before expanding the Smart-hopping infrastructure. See the next section for details.

5.4 Archiving the configuration files

Prior to expanding or modifying a Smart-hopping infrastructure, upgrading Smart-hopping APC or AP software, and upon completion of the Smart-hopping infrastructure expansion, you must save the following files to disk on your service PC:

- Smart-hopping infrastructure configuration file
- Upgrade Tool report
- logfile.txt file automatically generated by the Upgrade Tool

Note Do not run the Philips Upgrade Tool on a computer with a browser open.

Export a Configuration File

1. Run the Upgrade Tool on your Service PC by double-clicking the Upgrader.exe file located in the folder you copied the Upgrade Tool.
   The Upgrade Tool splash screen appears.
2. Click Next> to continue.

The APC/AP firmware selection screen (Figure 52) appears.

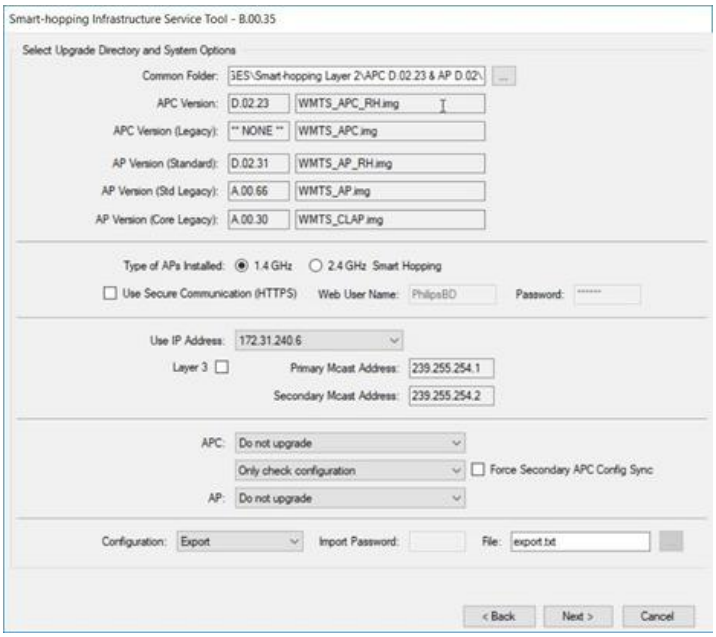


Figure 51: Exporting an Smart-hopping Configuration

a. Specify what type of APs you have installed by marking the appropriate radio button - 1.4 GHz Smart Hopping or 2.4 GHz Smart Hopping.
b. Deselect the Layer 3 check box for Layer 2 operation. If operating in Layer 3 mode, select the Layer 3 check box, and enter the Primary and Secondary Multicast Addresses.
c. Check the configuration for errors. For the upgrade options in the firmware selection dialog box, choose these specific options for each respective selection – see table 53 below.

Label	Option	Information
APC	Do Not Upgrade	Do not allow each APC to be upgraded
	Only Check Configuration	Verify the APC configuration
AP	Do Not Upgrade	Do not allow each AP to be upgraded

Table 53: Upgrade options

If you encounter errors, make sure you correct the errors and run the Upgrade Tool again, to verify there are no errors.

d. Export the configuration file. For the upgrade options in the firmware selection dialog box, choose these specific options for each respective selection – see table 54 below.

Label	Option	Information
APC	Do Not Upgrade	Do not allow each APC to be upgraded
	Only Check Configuration	Verify the APC configuration
AP	Do Not Upgrade	Do not allow each AP to be upgraded

Table 54: Upgrade options

e. In the Configuration drop-down box, select Export.
f. The file name is export.txt. Do not change the file name.
g. Click Next to create the specified Smart-hopping configuration file.

The exported file containing the configuration archive is stored on the service PC (in the logs folder on the directory from which you run the Upgrade Tool). All configuration items on the APC are archived to the specified file.

A sample exported APC configuration file is shown in Figure 52.

```
########################################
#    SMART HOPPING SYSTEM EXPORT FILE     #
########################################
System {  APC MAC 00:09:FB:97:00:DA {    File String  "BOOTROM.NVP" {      MAC 00:09:FB:97:00:
    File String  "PASSWORD.TLV" {      Tag Word 1700      {        Bytes { 00 00 00 00 }
    File String  "PARAM/SYSTEM.TLV" {      Tag Word 1310      #Possible tag names:
      #SYS_WEB_USERNAME_TAG
      {        String  "PhilipsBD"        Bytes { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      #SYS_WEB_PASSWORD_TAG
      {        Bytes { 2C 38 2C E2 A2 9A A4 9A F0 5A 84 DF A6 07 44 E3 }        Bytes { F6 C2
      #SYS_WEB_PORT_TAG
      {        Bytes { 00 00 00 50 }      }      Tag Word 1320      #Possible tag names:
      #SYS_WEB_ENABLED_TAG
      {        Byte 01      }      Tag Word 1322      #Possible tag names:
      #SYS_MCAST_ENABLED_TAG
      {        Bytes { 00 00 00 00 }      }      Tag Word 1324      #Possible tag names:
      #SYS_TRAP_CFG_MASTER_RESOLUTION_ENABLE_TAG
      {        Byte 01      }      Tag Word 1325      #Possible tag names:
      #SYS_TRAP_CFG_TUNNELED_STATION_THRESHOLD_TAG
      {        Bytes { 00 00 00 32 }      }      Tag Word 1326      #Possible tag names:
      #SYS_TRAP_CFG_TUNNELED_AP_THRESHOLD_TAG
      {        Bytes { 00 00 00 1E }      }      Tag Word 1327      #Possible tag names:
      #SYS_TRAP_CFG_MANAGED_AP_THRESHOLD_TAG
      {        Bytes { 00 00 00 32 }      }      Tag Word 1328      #Possible tag names:
      #SYS_TRAP_CFG_SYSTEM_UTILIZATION_THRESHOLD_TAG
      {        Bytes { 00 00 00 50 }      }      Tag Word 1303      #Possible tag names:
      #PROXIM_TAG_APC_NAME2
      {        String  "APC-CL115"      }      Tag Word 1304      #Possible tag names:
      #SYS_SYSTEM_NAME_TAG
      #PROXIM_TAG_AP_SYSTEM_NAME
      {        String  "Philips"      }      Tag Word 1305      #Possible tag names:
      #SYS_AP_ADD_ENABLED_TAG
      {        Byte 01      }      Tag Word 1311      #Possible tag names:
      #SYS_WCS_REPEATING_ENABLED_TAG
      {        Byte 00      }      Tag Word 1307      #Possible tag names:
      #SYS_CONFIGURATION_KEY_TAG
      {        Bytes { 00 00 B7 68 }      }      Tag Word 1308      #Possible tag names:
```

Figure 52: Sample Exported APC Configuration File.

3. Click Finish to close the Upgrade Tool.

   Note the Upgrade Tool automatically creates a log file, logfile.txt, in the directory from which it was run.

4. Locate the Smart-hopping configuration file (<filename.txt>), the Upgrade Tool report, and the Upgrade Tool log file (logfile.txt) in the directory from which the Upgrade Tool was run and move these files to an archive folder on your service PC for safekeeping.

5.5 Upgrading Smart-hopping APCs and APs using the Philips Upgrade Tool

This section describes use of the Philips Upgrade Tool tool to upgrade devices on an installed Smart-hopping infrastructure and includes:

- An Overview of the Upgrade Tool
- Access Point Controller Upgrade Process Summary
- Access Point Upgrade Process Summary
- Upgrade Prerequisites
- Upgrade Procedure

5.5.1 An overview of the Upgrade Tool

The Philips Upgrade Tool is a PC-based utility that:

- Upgrades the firmware on Smart-hopping Access Point Controllers (APCs) and 1.4 GHz. and 2.4 GHz Smart-hopping Access Points (APs).
- Verifies that APCs on your network are configured correctly.
- Displays warning and error messages that you may use to troubleshoot any configuration errors that may exist on your network.

The Philips Upgrade Tool runs on a Windows 10 (or higher) PC connected to your network. The Upgrade Tool scans the network for APCs, and connected APs, and Patient Monitors. It then guides you through the upgrade process, one APC and two APs at a time. Before upgrading an AP, the Philips Upgrade Tool roams any active IPMs connected to the AP to alternate APs so that minimal patient data is lost.

The Upgrade Tool exports the APC system configuration and check that it conforms to the system requirements and installation rules, and verifies that the Secondary APC configuration matches the Primary APC configuration.

The Philips Upgrade Tool updates the APC configuration using normal APC update processing, so the APC does not need to be rebooted and data flow is not interrupted during the configuration update process.

If the Philips Upgrade Tool detects that an APC installation or configuration rule is broken, it generates a warning message after the upgrade process is complete. If the Philips Upgrade Tool detects that a system requirement is broken, it generates an error and stops the upgrade process. If the APC Primary and Secondary configurations are mismatched, then the Upgrade Tool attempts to force the secondary to upload a copy of the primary configuration.

5.5.2 Access Point Controller upgrade process summary

Upgrading Smart-hopping Access Point Controllers using the Philips Upgrade Tool proceeds as follows:

1. The Upgrade Tool will automatically retrieve the Primary Configuration file from the primary APC to allow the process to maintain system configuration and return the system to original configuration.
2. Select the AP group to be upgraded. If the primary APC manages this AP group, then the Upgrade Tool will act as the primary to allow upgrade of the primary APC.
3. Before an APC can be upgraded, any attached APs are dispersed to other APCs in the system. During the dispersion of APs there ought to be minimal loss of monitoring (in some cases, monitoring loss from the affected APs may last 10 to 20 seconds).
4. The Upgrade Tool will verify configuration of APC against the Primary Configuration file, and notify the service user if differences exist and assist in corrective action if necessary.
5. At this point the Upgrade Tool notifies the APC being serviced to start the upgrade, a new software image is downloaded to the APC via TFTP and then verified. The service user will be prompted for input and notified of upgrade progress and status. The download of APC image takes approximately 3 minutes, and at the end of the process the APC will reboot.
6. On completion of the APC upgrade, the APs from that AP group are re-partnered with the upgraded APC. There will be loss of monitoring while APs are re-partnered.
7. After you have upgraded all the APCs on a Smart-hopping infrastructure, the current primary APC may function as a secondary APC to a new primary APC (depending on network status [for example, there is a network disruption between the upgraded and rebooted APC and existing APCs]).

8. If you are upgrading the software on Smart-hopping APs, then proceed to the next section “Access Point Upgrade Process Summary” below. Otherwise, run the Philips Upgrade Tool again to verify the APC and AP configurations system wide, and archive the configuration files as described on page 108.

5.5.3 Access Point upgrade process summary

Upgrading Smart-hopping Access Points using the Philips Upgrade Tool proceeds as follows:

1. If both APs and APCs need to be upgraded, then the APCs will be upgraded first.

2. Attach the service PC/laptop to the Smart-hopping infrastructure subnet.
The PC must be connected to the subnet that the wireless infrastructure equipment is connected. The Philips Upgrade Tool will passively discover all active network components and display the active equipment labels for Patient Monitors, APs, and APCs to allow for easy identification.
3. You are provided with equipment label information to provide adequate notification to clinical staff of any affected equipment.

4. For the AP group, perform AP upgrade on all APs with no mobile clients currently connected to them. You are prompted for input and notified of the upgrade progress, status, and outcome.

5. For each AP in an AP group with active IPMs, forced roaming will be attempted. You are prompted to move active IPMs if the roam fails. Once the active IPMs are off the AP, the AP upgrade is user-initiated, and you are prompted for input and notified of progress, status, and outcome.

6. Repeat for each AP group.

7. APs will reboot when their partnered APC is power cycled.

8. Run the Philips Upgrade Tool again to verify the APC and AP configurations system wide, and archive the configuration files as described on page 108.

Note The Philips Upgrade Tool requires supported, and compatible AP and APC firmware.

5.5.4 Upgrade prerequisites

Note the following requirements you must complete prior to upgrading a Smart-hopping infrastructure using the Philips Upgrade Tool:

1. Install the Upgrade Tool on your service PC as described on page 82.

2. Connect your service PC to the Smart-hopping infrastructure wireless subnet as described on page 77.

3. Export the current configuration to a service PC before upgrading the Smart-hopping infrastructure. See details on page 103.

4. Run only Version A.00.19 (or greater) of the Philips Upgrade Tool when expanding or upgrading an Smart-hopping infrastructure.

5. Upgrade the existing system APC software to B.00.19 or greater prior to expanding an Smart- hopping infrastructure.

6. APCs in the system running A.00 or B.00 code indicated they are 862147 APCs (serial console and LAN connections on rear of device). These are not compatible with D.02. Before upgrading to D.02 software, you must replace all 862147 APCs with the 865346 APC (serial console and LAN connections on front). For more information on replacing APCs, see “Replacing an AP, Remote Antenna, or APC in an Existing System” on page 122.

7. Close all browser windows on the Service PC prior to running the Upgrade Tool.

5.5.5 Upgrade procedure

Refer to “Run the Philips Upgrade Tool” on page 103or the document Upgrading Smart-hopping Access Point Controllers and Access Points for information on the upgrade procedure.

5.6 Adding APCs to an existing Smart-hopping infrastructure

Adding an APC to an existing Smart-hopping Infrastructure may be required as a preliminary step to adding APs. Before adding an APC to a Smart-hopping infrastructure, ensure that you have verified the following:

- Before a new APC is added to an Smart-hopping infrastructure, it must be in its factory default state. If the APC has not been received directly from the factory, then connect the service PC to the APC serial port and reset the APC to its factory default settings.

  If you properly reset an APC to its factory defaults before adding it to an existing Smart-hopping infrastructure, the new APC becomes a Secondary, and it will determine that the Primary configuration key is larger than its own, and properly request an update from the Primary.

Caution Ensure that the subnet mask of the APC to be added is configured to match the network type. If the subnet mask is set incorrectly, it can cause system-wide failure on the Smart-hopping infrastructure, as this APC will not be able to communicate effectively with other APCs on the Smart- hopping infrastructure.

- Before you begin this procedure, ensure that the APC is not connected to the Smart-hopping network.

To add an APC to an installed Smart-hopping infrastructure, complete the following steps:

1. Perform the APC initial configuration procedure described on page 83.
   This APC initial configuration procedure configures the following:
   a. Verify the firmware revision of the replacement APC matches that of the APCs already on the Smart-hopping infrastructure.
   b. Reset the APC to its factory default settings. This will zero the APC configuration key and ensure that no configuration can be copied from the APC (since the original configuration is removed).
   c. When you reset an APC to factory defaults, wait two minutes until attempting to access the APC. The two minutes allows the configuration to save properly.
   d. Set the APC IP address.
   e. Configure the APC for the desired system type (1.4 GHz Smart Hopping or 2.4 GHz Smart Hopping).
   f. If applicable, set the Primary and Secondary APC Multicast Address for Layer 3 operation.
   g. Enable APC Multicast Layer 3 operation (if applicable).
   h. Enable the Client CI Multicast Spoof feature (if applicable).
   i. APC backup priority level
   j. Serial port console password
   k. Web interface user ID and password
   l. Web communications mode - HTTP or HTTPS

2. Disconnect then exit the terminal emulation session and disconnect the serial cable from the PC and APC.

3. Disconnect the power cable from the APC to power off the APC.

   Caution Connect the APC network cable first, then connect the power cable. Otherwise, the result could be a loss of monitoring and a loss of system configuration.

   Warning Implementing and executing any of the expansion procedures listed below will cause interruptions to monitoring if the system is “live” - i.e., system is up and running and monitoring

patients. You must notify the hospital staff of all service events to the Philips IntelliVue Wireless Network prior to performing or implementing the service events.

4. Connect the new APC to the network, ensuring it is on the same subnet as the other APCs on the system:
    a. Connect a Category 5 (or higher) Shielded Twisted pair network cable between the switch port and the APC.
    b. Connect a power cable to the APC to power up the APC.
    Since this APC is being added to an existing system, verify that the APC LED turns flashing orange indicating it is operating as a Secondary APC after its self-test.

5. Connect to the APC web-based management interface by opening a browser on the service PC on the Smart-hopping infrastructure subnet. Refer to page 77 if you need to configure your service PC to connect to the Smart-hopping infrastructure wireless subnet.

6. Select the APC in the View Device tree (selected device is displayed green) and then select the Configure tab.
    In the AP Controller Network Configuration screen, configure the following parameters as necessary:
    a. System ID - Verify the setting is Philips. If not, change it to Philips.
    b. AP Controller Name - Enter the APC Name from the APC worksheet (page 59).
    c. IP Addressing - Verify that the Specify IP radio button is marked and that the IP Address, Subnet Mask and Default Gateway settings are as expected per the APC worksheet (page 59). If not, change the settings to match the worksheet.

7. Click SAVE, and then verify the settings by selecting the Status tab.

8. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool to verify the APC and AP configurations system wide, and save the configuration files as described on page 103.

9. At this time, add all other APCs to the network by repeating Steps 1 to 8 for each APC to be added.

5.7 Adding APs to an installed Smart-hopping infrastructure

There are two procedures that you can use to add APs to an existing Smart-hopping Infrastructure:

- The first procedure involves allowing the AP to automatically register on the system via the APC BootP server.
- The second procedure allows pre-configuration of the AP in the system so that when you do connect it to the Smart-hopping infrastructure, the AP will come up with the correct settings.

After you have added the APs and Remote Antennas to your Smart-hopping infrastructure, be sure to rename the newly added APs and Remote Antennas from their default values to more meaningful, user-friendly names as described on page 118.

Before beginning the procedures given in this section, ensure that the Smart-hopping infrastructure (Switches, PoE switches, Sync Units) has sufficient capacity to connect the additional APs.

When adding new APs to an Smart-hopping infrastructure, be sure to:

- Add only one AP at a time, wait for it to boot up, and then install the next AP only after waiting for a period of 60 seconds.

- Do not add multiple APs simultaneously on a Smart-hopping infrastructure to prevent excess system stress due to high data traffic.

- Refrain from accessing the APC web interface during the 60 second waiting period after you have added an AP to the system.

- Always allow two to three minutes after making changes or additions to the Smart-hopping infrastructure before accessing the web interface to check the status of the changes or additions.
- Run the Upgrade Tool periodically as APs are added to the system (e.g., every 5 - 10 newly added APs). Running the Upgrade Tool periodically during the system expansion provides these benefits:
    - Provides error checking/warning for newly added APs; This ensures that any errors or warnings are detected early.
    - Using the Upgrade Tool will phase in the system changes and slow down the system expansion to a pace manageable by the active APCs.

- To minimize the impact on APC performance, restrict the number of open web servers during direct access, network scan, or when adding APs.

- Run the Upgrade Tool at the end of the expansion process with the Export option enabled in Check and Update Configuration mode.

When replacing an AP (see page 122) on an installed Smart-hopping infrastructure, be sure to assign the new replacement AP IP address as a static address. Assign the replacement AP the same IP address that was previously assigned to the old defective AP.

5.7.1 Adding an AP via auto-registration

To add an Access Point to an already up and running Smart-hopping infrastructure using the auto-registration method:

1. Prior to adding the AP to the Smart-hopping infrastructure, complete the 1.4 GHz Default AP Configuration Worksheet (page 66) or the 2.4 GHz Default AP Configuration Worksheet (page 67). **Note** Record the MAC address of the new AP prior to installing it. The MAC address is printed on the label found on the bottom of the AP. Also, to simplify the AP addition and configuration procedure, you may find it helpful to connect the AP directly to a Sync Unit in an equipment closet using a patch cable until the AP configuration is complete, and then disconnect and move the AP to its permanent mounting location. This may be desirable if you are connecting your service PC to a network switch to manage an AP in the same equipment closet.

2. If you have installed an Access Point with Remote Antennas, connect the Access Point to its RAs now using the provided 74-ft. UTP-and-Coaxial cable bundles.

    1.4 GHz Smart-hopping AP Configuration Screen:

    a. Set the AP Name as appropriate for this AP.
    b. The Enable AP checkbox should be CHECKED.
    c. Leave the Partnered AP Controller drop-down list set to “ANY.” In this screen, the Partnered APC will get set correctly based upon the AP Group membership setting specified below.
    d. Set the Group Membership as appropriate for this AP.
    e. The WMTS Channels matches the existing Smart-hopping configuration.
    f. The RF Access Code matches the existing Smart-hopping configuration. Set the Enable Box to CHECKED.
    If you need to modify the WMTS or RF Access Code settings, then the 1.4 GHz. AP defaults may not be set correctly. See page 92 for details.
    g. Mark the Use DHCP or Specify IP radio button as appropriate for your network. When specifying the IP address, you must set the Subnet Mask and Default Gateway fields to match the existing Smart-hopping configuration. When replacing an AP, be sure to assign the replacement AP IP address as a static address.

    2.4 GHz Smart-hopping AP Configuration Screen:

    a. Set the AP Name as appropriate for this AP.
    b. The Enable AP checkbox should be CHECKED.
    c. Leave the Partnered AP Controller drop-down list set to “ANY.” In this screen, the Partnered APC will get set correctly based upon the AP Group membership setting specified below.
    d. Set the Group Membership as appropriate for this AP.
    e. The Radio Regulations matches the existing Smart-hopping configuration.

f. The Frequency Plan matches the existing Smart-hopping configuration.
g. The ZigBee channel used for medical purposes option is no longer used. The selection should be left to the default of None.
h. The RF Access Code matches the existing Smart-hopping configuration. Set the Enable Box to CHECKED.
If you need to modify the Radio Regulations, Frequency Plan, Zigbee channel, or RF Access Code settings, then the 2.4 GHz. AP defaults may not be set correctly. See page 92for details.
i. Mark the Use DHCP or Specify IP radio button as appropriate for your network. When specifying the IP address, you must set the Subnet Mask and Default Gateway fields to match the existing Smart-hopping configuration. When replacing an AP, be sure to assign the replacement AP IP address as a static address.
j. Click SAVE and then verify the AP Configuration settings.
The Partnered APC value will change to match the AP group to which you assigned the AP.
k. Refresh Internet Explorer (by pressing F5), and in the View Devices tree, verify that the AP appears under the correct Access Point Controller.
This may take several minutes and in the process; the Access Point may appear (for a moment) in the Unregistered List of the View Devices tree. If after five minutes the Access Point remains in the Unregistered List of View Devices tree, select the Access Point in the Unregistered List and click the Delete AP button at the bottom of the page. Remove power to the Access Point and repeat this procedure beginning from Step 1.
l. Disconnect the AP from the Sync Unit, and then reconnect it.
This will recycle power to the AP and force the AP to apply the configuration changes.
m. Click on the STATUS tab for the newly added AP and verify that the IP shown for that AP is correct. If not, recycle power to the AP and then check and verify the status again.
Note If you encounter a Duplicate IP address system-level alert after adding an Access Point to a Smart- hopping infrastructure, then reconfigure the AP with a unique IP address, and then reset the AP.
n. Repeat Steps 1 to 10 for each AP to be added to the installed Smart-hopping infrastructure. Run the Upgrade Tool periodically as APs are added to the system (e.g., every 12 newly added APs).
o. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool to verify the APC and AP configurations system wide, and save the configuration files as described on page 103.
p. Add the new Smart-hopping infrastructure devices to the Information Center configuration.

5.7.2 Adding an AP via manual MAC address input

By using an AP MAC address, you can fully pre-configure the AP before connecting it to the Smart-hopping infrastructure.

Complete the following steps to manually add an Access Point to the system. This method allows you to pre-configure the AP off-line so that when you do connect it to the Smart-hopping infrastructure, it will come up with the correct settings.

1. Before beginning this procedure, record the AP MAC address (found on the label on bottom of the AP), and complete the 1.4 GHz Default AP Configuration Worksheet (page 66) or the 2.4 GHz Default AP Configuration Worksheet (page 67).

2. Ensure the AP you want to add is disconnected from the network. In the APC management interface Device view, click the Add AP button.
The Add New Access Point (Figure 54) screen appears.

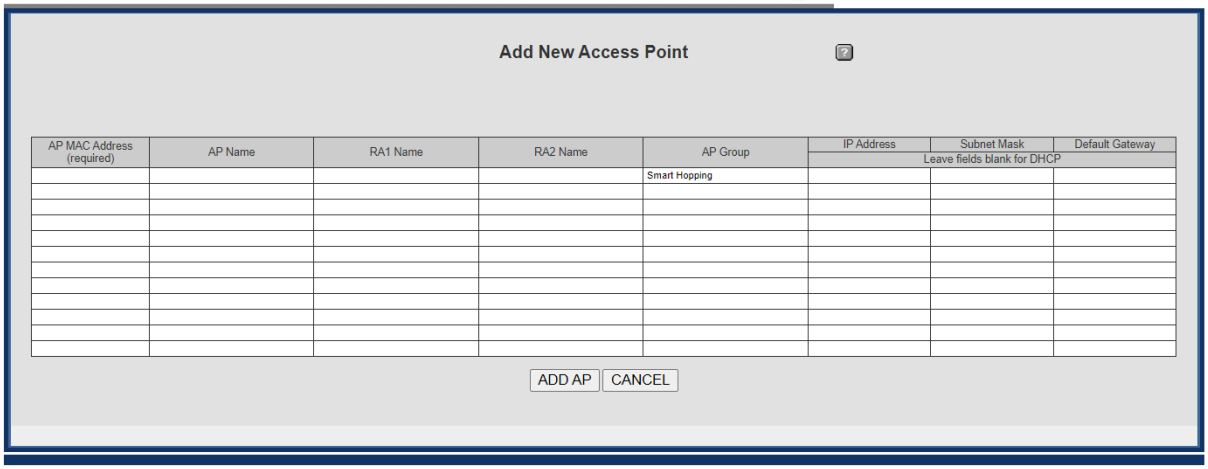


Figure 53: Add New Access Point Screen.

3. Configure the following settings:
    a. AP Name - Enter the AP Name
    b. Physical Address - Enter the AP MAC Address
    c. AP Type - Select Smart-hopping from the drop-down menu.

4. Click the Add AP button, and then click the Network button to return to the Device view. The newly added AP should appear in the unregistered APs list.

5. In the Unregistered List, select the AP just added and press the Basic Settings tab. Set the following AP-specific configuration parameters:
    a. Group Membership - Set as documented on the AP Configuration Worksheet.
    b. IP Address - Set the IP address, Subnet Mask, and Default Gateway as documented on the AP Configuration Worksheet.

6. Click the SAVE button and verify the results. If the AP configurations settings are incorrect, repeat Step 5.

7. Add all other APs to the system configuration by completing Steps 1 to 6 for each AP.

8. Power on the AP. Each AP will take approximately one minute to become operational.
For Access Points, complete the following additional steps:
    a. Connect the first Remote Antenna to the Access Point using the UTP and Coaxial cable connectors.
    b. Connect the second Remote Antenna to the Access Point using the UTP and Coaxial cable connectors.
    c. Be sure to label the UTP cable bundles and the Remote Antennas themselves as RA 1 and RA 2 corresponding to the cable connections you made in steps a and b
    d. Reboot the Access Point by disconnecting its cable.
    e. Observe the Remote Antenna status LEDs to verify that the Remote Antenna is powered and operational.

9. In the Device view, verify that the AP appears associated under the appropriate APC and in the appropriate AP group.

10. Select each newly added AP, and then click on the Status tab for that AP and verify that the IP address shown for the AP is correct.

    Note If you encounter a Duplicate IP address system-level alert after adding an Access Point to a

Smart- hopping infrastructure, then reconfigure the AP with a unique IP address, and then reset the AP.

11. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool to verify the APC and AP configurations system wide, and save the configuration files as described on page 103. Run the Upgrade Tool periodically as APs are added to the system (e.g., every 12 newly added APs).

12. Add new Smart-hopping devices to the Configuration Wizard.

5.7.3 Renaming newly installed APs and Remote Antennas

You can change the names of installed Access Points from their default values to more user-friendly names by following these steps:

1. Click on the APC in the APC web interface that is associated with the newly added APs and Remote Antennas you wish to rename.

2. Click the NAMES tab.
   The AP and Remote Antenna Friendly Name Management screen appears as shown in Figure 55.

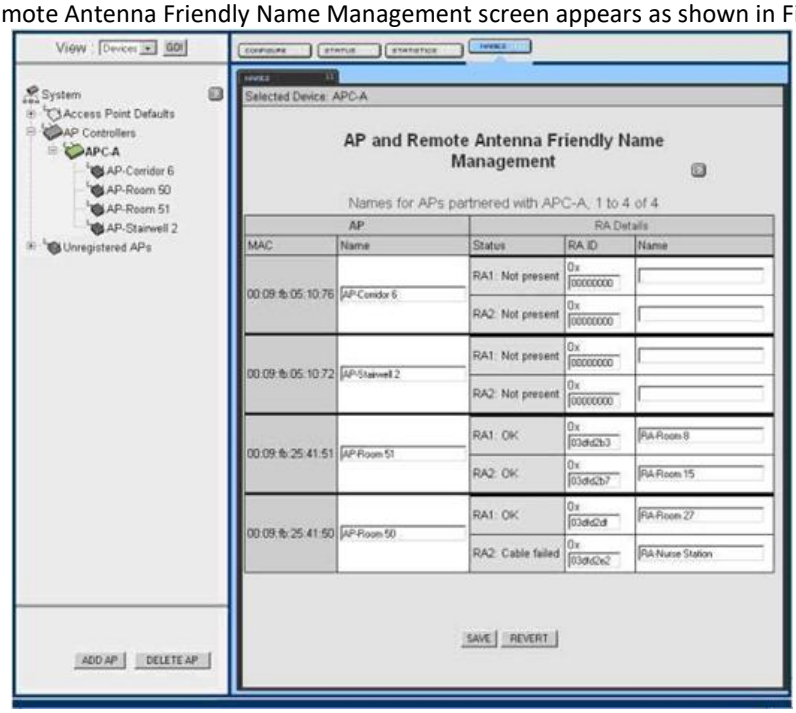


Figure 54: Renaming APs and RAs.

3. Enter meaningful, user-friendly names for the installed Standard APs, Access Points, and Remote Antennas in the AP Name and RA Name fields.
   a. You may enter a string of up to 32 characters for the name values.
   b. First-generation Access Points display Remote Antennas as Not Present.
   c. Second-generation (and later) Access Points list Remote Antennas and provide the general status of connected Remote Antennas.

4. Click SAVE and then verify the AP Configuration settings.

5. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool to verify the APC and AP configurations system wide, and save the configuration files as described on page 103.

Warning Wait two to three minutes after closing the APC web browser interface prior to running the Philips Upgrade Tool or system disruption can occur.

5.8 Adding new AP groups to an existing configuration

As described in “Planning Your AP Groupings” on page 50, an AP Group allows for logically associated Access Points within a clinical unit to be given a common set of configurations. These configurations govern everything from AP to APC partnership rules, RF Channel and Access Code usage and Alert Settings.

The AP Groups within the system should logically map to the Clinical Units that have been established for the monitoring network and databases.

If additional APCs are being added to the Smart-hopping infrastructure, then make sure that they have already been added to the system prior to adding the new AP groups.

Prior to beginning this procedure, ensure that you have the following information for each new AP group to be added:

- AP Group Name
- AP Group type (Smart-hopping)
- Partnered APC
- Alert Destination

5.8.1 Add new AP groups

To add a new AP group to an existing configuration:

1. Connect to the APC web-based management interface.

2. Select the Groups View in the APC web interface drop-down menu and then click the GO! button.

3. Click ADD GROUP at the bottom left of the screen.

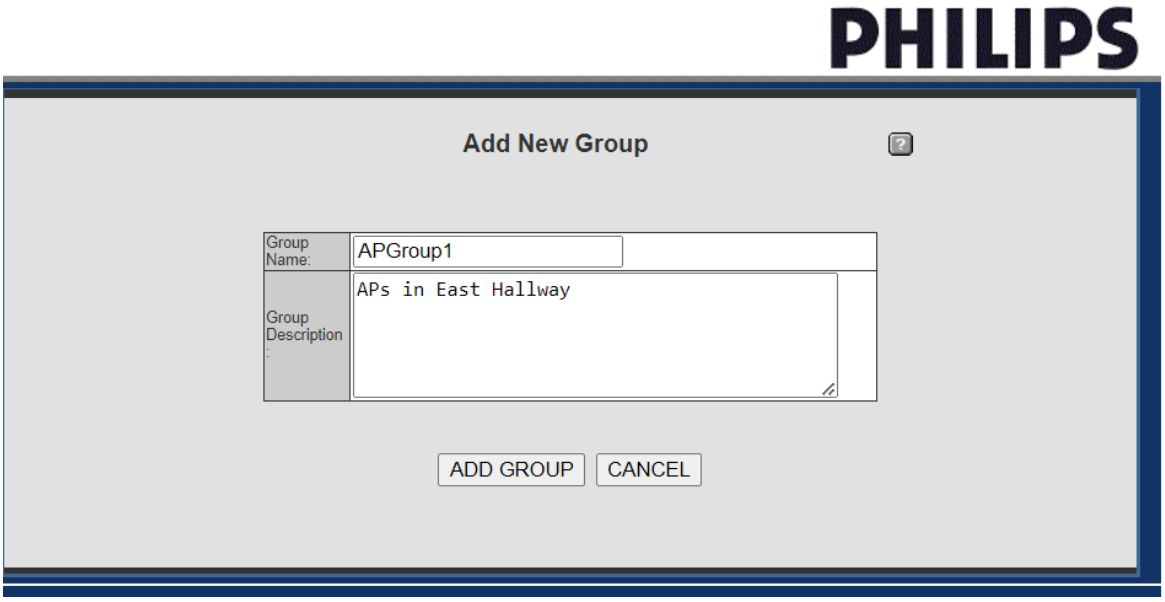


Figure 55: Adding New AP Group.

4. In the Add New Group screen (Figure 4-6), configure the following settings:
    a. Group Name - Set as documented in AP Group Configurations Worksheet (do not include spaces in the group name).
    b. Group Type - Set to Smart-hopping.
    c. Group Description - Optional. Enter a description for this AP Group. Typically, you may want tenter the name of the clinic, unit, or department in which the APs are installed.

5. Click the ADD GROUP button. Repeat Steps 3 to 5 for each AP Group being added on this system. When all AP Groups have been added, click the NETWORK button to return to the View Groups tree screen.

5.8.2 Configure the new AP groups

For each AP Group that has been added, complete the following steps:

1. In the View Groups tree, select an AP Group that was created and select the BASIC SETTINGS tab.

   In the 1.4 GHz AP Group Configuration Basic Settings screen, set the following configuration for this AP Group:

   a. Select the appropriate APC for this AP group from the Partnered AP Controller drop-down list. Refer to your completed AP Group Configuration Worksheet.

   In the 1.4 GHz AP Group Configuration Basic Settings screen, verify the following configurations for this AP Group. If they are not correct, delete the AP group and then edit the AP default settings (see page 92):

   b. Set the WMTS Channels as appropriate for your geography and as documented in the 1.4 GHz Access Point Default Configuration Worksheet.
   c. Set the RF Access Code field as documented in the 1.4 GHz Access Point Default Configuration Worksheet, and set the Enable Box to CHECKED.
   d. Set the Subnet Mask and Default Gateway fields as documented in the 1.4 GHz Access Point Default Configuration Worksheet.

   In the 2.4 GHz AP Group Configuration Basic Settings screen, set the following configurations for this AP Group:

   e. Select the appropriate APC for this AP group from the Partnered AP Controller drop-down list. Refer to your completed AP Group Configuration Worksheet.

      In the 2.4 GHz AP Group Configuration Basic Settings screen, verify the following configurations for this AP Group. If they are not correct, delete the AP group and then edit the AP default settings (see page 93):

   f. Select the Radio Regulations from the drop-down list that apply to the country in which you are installing the 2.4 GHz Smart-hopping infrastructure as documented in the 2.4 GHz AP Default Configuration Worksheet.
   g. Select the Frequency Plan from the drop-down list to specify the 802.11 channel configuration with which the 2.4 GHz Smart-hopping infrastructure will co-exist.
   h. The ZigBee channel used for medical purposes option is no longer used. The selection should be left to the default of None.
   i. Set the RF Access Code field as documented in the 2.4 GHz Access Point Default Configuration Worksheet, and set the Enable Box to CHECKED.
   j. Set the Subnet Mask and Default Gateway fields as documented in the 2.4 GHz Access Point Default Configuration Worksheet.

2. Click SAVE and then verify that the AP Group Basic Configuration settings are correct.

3. Select the ALERTS SETTINGS tab. See Figure 57: *AP Group Configuration Alert Settings*
   In the AP Group Configuration Alerts Settings screen, set the following configurations for this AP Group:

   a. Alert Destination - Set as documented in the AP Group Configuration Worksheet.
   b. Sync Loss Alert - Verify all boxes are CHECKED.

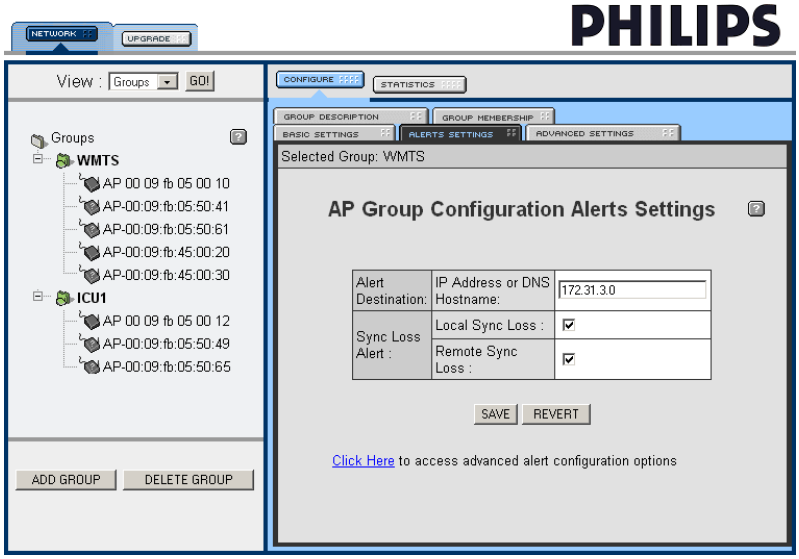


Figure 56: AP Group Configuration Alert Settings

4. Click SAVE and then verify the AP Group Alerts Configuration settings are correct.

5. Select the ALERTS SETTINGS tab again. In the AP Group Configuration Alerts Settings screen, click on the Click Here link at the bottom of the screen to display the AP Group Configuration Advanced Alerts Settings screen (See Figure 3-17 and Figure 3-18.)
   The settings in the Advanced Alerts Settings screen will be populated as part of the factory defaults. Verify the correct settings against Figure 3-17 and Figure 3-18.

6. Click SAVE and then verify the AP Group Configuration Advanced Alerts Results page.
7. Repeat Steps 1 to 6 until you have configured every AP group that you have added to the system.

8. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool to verify the APC and AP configurations.

Warning Wait two to three minutes after closing the APC web browser interface prior to running the Philips Upgrade Tool or system disruption can occur.

5.9 Adding patient monitors

Before adding Patient Monitors, you must configure new equipment labels into the Information Center. This may need to be done manually for live, active systems.

Adding new Patient Monitors to the system generates new DHCP entries that forces automatic system replication of the configuration file from the Primary APC to all Secondary APCs. For this reason, we recommend that you run the Philips Upgrade Tool to verify the APC and AP configurations system wide, and save the configuration files as described on page 103 after adding any monitoring devices to the Smart-hopping infrastructure.

5.10 Replacing an AP, Remote Antenna, or APC in an existing system

At some point during the life of the Smart-hopping network, it may be necessary to replace an Access Point, Remote Antenna, or Access Point Controller due to service, repair, or upgrade. Follow the replacement procedures listed below.

Note The Test and Inspection procedures provided in Chapter 4 must be followed by Philips Service Providers when the Philips Smart-hopping Infrastructure is installed, and after any service event, upgrade, or repair.

5.10.1 Replacing a Smart-hopping Access Point

In the event of a failed AP, the following steps should be taken to replace it with a new one. Make note of the following settings for the AP that is to be replaced (write this information down and have it readily available):

- AP Name
- IP Address
- Subnet Mask
- Default Gateway
- Group Membership

Note You must assign the new replacement AP IP address as a static address. Assign the replacement AP the same IP address that was previously assigned to the old defective AP.

To replace an Access Point within an installed Smart-hopping infrastructure:

1. Physically disconnect the AP requiring replacement from the system and remove it from its installation location.

2. Access the APC management interface and verify that the AP was removed and has moved to the Unregistered list. This may take several minutes to occur.

   If the AP continues to stay in the registered list, uncheck the Enable AP button in its Configuration screen and then click the SAVE button at the bottom of the screen. This will force the AP to move to the Unregistered list. Before disabling the AP, ensure that you have selected the correct AP, especially on a “live” system that is monitoring patients.

   Note One way to verify that an AP that has been disconnected but has not yet fallen to the Unregistered list, is to click on the Status tab for that AP after it has been disconnected but still remains in the registered list. Such an AP will report an error message if its status is requested.

3. Once the AP is in the Unregistered list, select it (so that it highlights), and then click on the Delete AP button at the bottom of the screen (on the left side).

4. After the above steps have been completed, continue with the procedure, “Adding APs to an Installed Smart-hopping infrastructure” on page 114.

5. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool to verify the APC and AP configurations.

Warning Wait two to three minutes after closing the APC web browser interface prior to running the Philips Upgrade Tool or system disruption can occur.

5.10.2 Replacing a Remote Antenna

To replace a Remote Antenna (RA) connected to an Access Point:

1. Disconnect the UTP and Coax cables from the failed Remote Antenna and physically remove the RA from its mounting location.

2. Mount the replacement RA and note its ID number.

3. Reconnect the UTP and Coax cables from the Access Point.

4. Reboot the Access Point to detect the presence of the new RA. You can reset the Access Point from the APC web interface.

5. Verify that the RA is powered and connected properly by observing the RA two status LEDs.
   The Access Point and its connected Remote Antenna(s) will be auto-detected by the APC after the Access Point has been rebooted or reset.

6. Change the name of the RA from the default value to a more user-friendly name using the procedure, “Renaming Newly Installed APs and Remote Antennas” on page 118.

5.10.3 Replacing a Smart-hopping APC

Prior to removing an APC from the system, note the following information:

- APC IP Address
- APC Name
- APC Firmware Revision
- AP Groups and APs that are or were partnered with the APC

To replace a Secondary APC on an existing system, perform the following steps:

1. Disconnect the Secondary APC from the system.
   Note Step 1 may cause some system dropouts as “orphaned” APs are picked up by the existing APCs. If this is being done on a “live” system, ensure that all appropriate clinical personnel have been notified of the potential impact.

2. Access the APC management interface and verify that all of the orphaned APs have been picked up by other APCs using the APC management screens.
   Ensure that the system is stable and that all configuration parameters are correct. It will be “normal” for APs “orphaned” by the missing APC to have been picked up by the remaining APC(s).

3. Power up the replacement APC but do not connect it to the network.

4. Perform the procedure “Perform Initial Configuration of the APCs to be Installed” on page 82.
   Warning Wait two to three minutes after closing the APC web browser interface prior to running the Philips Upgrade Tool or system disruption can occur.
5. With the replacement APC power cord disconnected, connect the replacement APC to the network where the old APC was connected ensuring it is on the same subnet as the other APCs on the system.

6. Power up the replacement APC.

7. Access the APC management interface and verify that the replacement APC shows up on the device list. It will show up with its MAC address as its name. Set the APC name to the value of the APC it replaced and click the SAVE button.

8. Reconfigure the AP Groups that were partnered with the replaced “bad” APC. Point the Groups to the new APC (Partnered APC). If configuration was done properly all APs associated with the group should now be partnered with the replacement APC.

   Reconfigure each AP group from the ‘old’ APC to the new ‘APC’ as follows:
   a. Select the existing AP Group that was assigned to the old, failed APC, and then click on the Group Membership tab.
   b. Select all APs that were assigned to the existing AP Group, and then click the right arrow button to un-assign all APs from the group.
      The APs are assigned to the default group Smart-hopping.
   c. Create a new AP Group for the new, replacement APC.
   d. Select the new AP Group, and then click on the Group Membership tab.
      Selecting a maximum of five APs at a time that were unassigned from the old AP Group, click the left arrow button to assign the APs to the new AP Group associated with the new, replacement APC.
      Repeat Step d until you have moved all APs that were unassigned from the old AP Group to the new AP Group.
      Note Reassign no more than five APs at a time to reduce the configuration load on the APC.

9. Shutdown the APC web interface browser session, and then run the Philips Upgrade Tool (see page 99) to verify the APC and AP configurations.

Warning Wait two to three minutes after closing the APC web browser interface prior to running the Philips Upgrade Tool or system disruption can occur.

5.11 Perform network scan on an expanded system

The Network Scan tool in the PIC or PIC iX DBS discovers all of the APCs and APs on the system and creates the DBS entries for them. Please see “Perform Network Scan” on page 103 for detailed instructions on running the network scan.

Warning Using the Network Scan tool on a live system is not recommended as it will force reboot all Philips Information Center servers on the system.

If your APC is operating using the HTTPS protocol, network scans from the Philips Patient Information Center server fail. To resolve this, manually enter the APC information on the Information Center.

Do not run the Upgrade Tool during a Network Scan or system disruption can occur.

If a Secondary APC is the first in the Network Scan, the Primary APC may experience undesired web page loops.

6 Smart-hopping system testing

This chapter provides procedures you should follow to inspect and verify your Smart-hopping Infrastructure, and includes:

- Smart-hopping Access Point Test and Inspection Procedures
- Smart-hopping Access Point Controller Test and Inspection Procedures
- Sync Unit Test and Inspection Procedures
- Power over Ethernet Unit Test and Inspection Procedures

Note You must follow the tests and inspections provided in this chapter after you initially install the Smart-hopping Infrastructure and also after you perform any service event on the Smart-hopping infrastructure.

6.1 Smart-hopping Access Point test and inspection procedures

This section documents RSSI (Received Signal Strength Indication) thresholds to use when performing the Coverage Area Verification (CAV) in a Smart-hopping network deployment.

Table 54 lists which tests you must perform when performing service events on Smart-hopping Access Points.

When performing this service event	Complete these required test(s)
Installation	Visual, Power On, Performance, Coverage Area Verification
Preventive Maintenance	N/A
Any component repair or replacement	Power On, Performance, Coverage Area Verification
Hardware Upgrade	N/A
Software Upgrade	Power On, Performance, Revision Check
All other Service Events	Visual, Power On, Performance

Table 53: Smart-hopping Access Point test and inspection requirements

Test block name	Test or inspection to perform	Expected results	Information to record on service record
AP **V**isual	Inspect all system components for obvious damage. Visually inspect all system components, Remote Antennas, cables, and connectors. Check for signs of abrasion, wear, or other damage. Check the fixed antennas for secure connection, proper orientation and direction.	No visible damage	**V:P** or **V:F** where: **P** = Pass **F** = Fail
AP **P**ower **O**n	With power connected to each active Network device, observe that all lights visible on the front panel are in proper status and that no error conditions are shown. Note that for 1.4 GHz Access Points and 2.4 GHz APs, you can view the Power, Network and Radio LEDs from the AP Status page in the APC web interface. Remote Antenna status can be checked from the Names tab in the APC web interface. **867216**	Devices power up into expected status; no error indications are shown.	**PO:P** or **PO:F** where: **P** = Pass **F** = Fail

	Verify that the Power/Sync LED on the AP is Solid GREEN. Verify that the Network LED on the AP is Blinking GREEN. If the AP has no Remote Antenna, verify that the Radio LED on the AP is Blinking GREEN. If the AP has Remote Antennas attached, verify that the Radio LED on the AP is Blinking AMBER. **989803171211, 989803171221 and 862228** Verify that Link and Power/Sync LEDs on Access Point are lit Solid GREEN. Verify that Activity LED is Blinking YELLOW. Verify that Radio and Network LEDs on Access Point are lit Blinking GREEN. **989803171211, 862228, 865052, and 867151** Verify that GREEN and YELLOW status LEDs on Remote Antennas are lit solid. **862113 and 862232** Verify that FDX, 100M, Link and Power/Sync LEDs are lit Solid GREEN. Verify that Activity, Radio and Network LEDs are lit Blinking GREEN.		
AP **P**erformance	Does the AP appear in the AP web browser management screens? Does data from a wireless device appear at the Information Center?	Expected answers are “Yes”. If so, Performance test passed.	**P:P** or **P:F** where: **P** = Pass **F** = Fail
AP **R**evision **C**heck	Does the revision reported in the APC web browser screen match the revision loaded? Run the Philips Upgrade Tool to check and verify final configurations.	Expected answer is “Yes”. If so, Revision Check test passed.	**RC:P** or **RC:F** where: **P** = Pass **F** = Fail
AP **S**afety	No safety test is required		**S:NA** where: **NA** = Not Applicable
Coverage **A**rea **V**erification — MX40	**Note** You can perform the CAV without connecting to central station sector; Average RSSI, Retries, LQI, and Connection status is available from the MX40. RF signal inops are not available. 1. Attach the lead set to the MX40. 2. Hold the MX40 by the lower half of the device to avoid contact with the antenna. The antennas are located on the sides near the top of the MX40. Keep the MX40 close to your body, near your stomach, with your back to the closest access point (AP) to perform the coverage assessment. These two placements mimic body blocking that is crucial for accurate CAV. 3. Measure the RSSI at all key locations; patient bed, bathrooms, and windows (if the window is more than 6ft. (2m) from the bed); reduce any variations by limiting movement while taking the measurements.	For 1.4 GHz installations - If there is ONLY Rev. B.X MX40 hardware, the expected RSSI must be greater than or equal to -67dBm. For 2.4 GHz installations - If there is ONLY Rev. B.X MX40 hardware, the expected RSSI must be greater than or equal to -68dBm. For 1.4GHz or	**CAV:P** or **CAV:F** where: **P** = Pass **F** = Fail

	You can perform these measurements in any of the following ways: • Using the automated coverage assessment feature (Assessment Mode/Assess Coverage) available in Service Mode on the MX40. For more details on the MX40 coverage assessment feature, refer to the IntelliVue MX40 Installation and Service, Release B.06.5x (part number 453564742251). • Using the AirSpy mapping software and the MX40. For more details on using AirSpy for the MX40 coverage assessment, refer to the AirSpy Instructions for Use (part number 453564923631) • Manually use the procedure that follows (Steps 4-9). 4. Set the screen time to always on. (SmartKeys-> Screen Setup-> Always On). 5. Navigate to the Link Info screen by touching the Device Status area and the Link Quality Indicator. **Note** The device screen locks after the configured period of time unless there is some interaction with the touch screen. This closes the Link Info window. If the device locks, touch the SmartKeys button, navigate to the second screen, and touch the Lock icon to unlock. 6. Use the Link Quality Indicator (LQI) to view the Received Signal Strength Indication (RSSI). 7. If you do not use the automated MX40 Assessment Mode, record the measurements for each location for 25 seconds, taking one reading every five seconds. 8. Average the results for each location. 9. Verify that at the edge of the coverage area, no Weak Signal or No Central Monit messages are reported and that the link quality is not in the red level. The Connection Status must remain Active on the MX40. The edge of the coverage area for hardware revision B.X is defined as an average RSSI -67 dBm (LQI > 3 bars) with body blocking to the Access Point for 1.4GHz installations and an average RSSI of -68dBm for 2.4 GHz installations. For hardware revision A.X, the edge of the coverage area is defined as an average RSSI -63 dBm (LQI > 3 bars) with body blocking to the Access Point for both 1.4GHz and 2.4GHz installations.	2.4GHz installations - If there is ANY Rev. A.x MX40 hardware, the expected RSSI must be greater than or equal to -63dBm.	

Coverage Area Verification — Mixed Deployments	CAV for mixed deployments Deploying both MX40 & IIT bedsides in the same area, the MX40 defines coverage. When the MX40 defines coverage, it also ensures that IIT bedsides perform acceptably in the coverage area.	For 1.4 GHz installations - If there is ONLY Rev. B.X MX40 hardware, the expected RSSI must be greater than or equal to -67dBm. For 2.4 GHz installations - If there is ONLY Rev. B.X MX40 hardware, the expected RSSI must be greater than or equal to -68dBm. For 1.4GHz or 2.4GHz installations - If there is ANY Rev. A.x MX40 hardware, the expected RSSI must be greater than or equal to -63dBm.	**CAV:P** or **CAV:F** where: **P** = Pass **F** = Fail

Table 54: Smart-hopping Access Point test and inspection matrix

6.2 Smart-hopping Access Point Controller test and inspection procedures

Table 56 lists which tests you must perform when performing service events on Access Point Controllers.

When performing this service event	Complete these required test(s)
Installation	Visual, Power On, Performance
Preventive Maintenance	N/A
Any component repair or replacement	Power On, Performance
Hardware Upgrade	N/A
Software Upgrade	Power On, Performance, Revision Check
All other Service Events	Visual, Power On, Performance

Table 55: Smart-hopping Access Point Controller test and inspection requirements

Test block name	Test or inspection to perform	Expected results	Information to record on service record
APC **V**isual	Inspect all system components for obvious damage. Visually inspect all system components, cables, and connectors. Check for signs of abrasion, wear, or other damage.	No visible damage	**V:P** or **V:F** where: **P** = Pass **F** = Fail

APC **P**ower **O**n	With power connected to each active Network device, observe that all lights visible on the front panel are in proper status and that no error conditions are shown. The following are normal conditions: **865346** • LAN Port Link Status LEDs - On blinking Green, and solid Yellow • Primary/Secondary LED: ○ C.00.xx firmware - Solid Green: Primary, Solid Orange: Secondary ○ D.00.xx firmware (Layer 2) - Blink rate is on for one second and off for one second. On flashing Green: Primary, On flashing orange: Secondary ○ D.00.xx firmware (Layer 3) - Blink rate is on for two seconds and off for one second. On flashing Green: Primary, On flashing orange: Secondary **862147** • Power LED - On Green • 100 BaseT LED - On solid Green • Link/Act - On primarily orange, flashes when network activity is present	Devices power up into expected status; no error indications are shown.	**PO:P** or **PO:F** where: **P** = Pass **F** = Fail
APC **P**erformance	Does the APC appear in the APC web browser management screens? Does data from a wireless device associated with this APC appear at the Information Center? Run the Philips Upgrade Tool to check and verify final configurations.	Expected answers are "Yes". If so, Performance test passed.	**P:P** or **P:F** where: **P** = Pass **F** = Fail
APC **R**evision **C**heck	Does the revision reported in the APC web browser screen match the revision loaded? Run the Philips Upgrade Tool to check and verify final configurations.	Expected answer is "Yes". If so, Revision Check test passed.	**RC:P** or **RC:F** where: **P** = Pass **F** = Fail
APC **S**afety	No safety test is required		**S:NA** where: **NA** = Not Applicable

Table 56: Smart-hopping Access Point Controller test and inspection matrix

6.3 Sync unit test and inspection procedures

Table 58 lists which tests you must perform when performing service events on Sync Unit.

When performing this service event	Complete these required test(s)
Installation	Visual, Power On, Performance
Preventive Maintenance	N/A
Any component repair or replacement	Power On, Performance
Hardware Upgrade	N/A
Software Upgrade	N/A
All other Service Events	Visual, Power On, Performance

Table 57: Sync unit test and inspection requirements

Test block name	Test or inspection to perform	Expected results	Information to record on service record
Sync Unit **V**isual	Inspect all system components for obvious damage. Visually inspect all system components, cables, and connectors. Check for signs of abrasion, wear, or other damage.	No visible damage	**V:P** or **V:F** where: **P** = Pass **F** = Fail

Sync Unit **P**ower **O**n	With power connected to each active Network device, observe that all lights visible on the front panel are in proper status and that no error conditions are shown.
	The following are normal conditions for each LED:
	• Power LED - On GREEN
	• Ext Ref LED - Off
	• Sync In LED
	  ○ if Sync is Primary – Off
	  ○ if Sync is Secondary - On
		Devices power up into expected status; no error indications are shown.	**PO:P** or **PO:F**
			where:
			P = Pass
			F = Fail

Sync Unit **P**erformance	Are there active Sync Unit alerts in Wireless Status Log? Do all associated APs appear as registered in the APC web browser management screens?	Expected answer is “No.” Expected answer is “Yes”. If so, Performance test passed.	**P:P** or **P:F** where: **P** = Pass **F** = Fail
Sync Unit **R**evision **C**heck	No Revision Check is required.		**RC:NA** where: **NA** = Not Applicable
Sync Unit **S**afety	No safety test is required		**S:NA** where: **NA** = Not Applicable

Table 58: Sync unit test and inspection matrix

6.4 Power over ethernet unit test and inspection procedures

Table 60 lists which tests you must perform when performing service events on the PoE Unit.

When performing this service event	Complete these required test(s)
Installation	Visual, Power On
Preventive Maintenance	N/A
Any component repair or replacement	Power On
Hardware Upgrade	N/A
Software Upgrade	N/A
All other Service Events	Visual, Power On

Table 59: PoE unit test and inspection requirements

Test block name	Test or inspection to perform	Expected results	Information to record on service record
PoE **U**nit **V**isual	Inspect all system components for obvious damage. Visually inspect all system components, cables, and connectors. Check for signs of abrasion, wear, or other damage.	No visible damage	**V:P** or **V:F** where: **P** = Pass **F** = Fail
PoE **U**nit **P**ower **O**n	With power connected to each active Network device, observe that all lights visible on the front panel are in proper status and that no error conditions are shown. Verify that the AC LED on front panel is solid GREEN. Verify that the Link LED is lit GREEN for each connected cable.	Devices power up into expected status; no error indications are shown.	**PO:P** or **PO:F** where: **P** = Pass **F** = Fail
PoE **U**nit **P**erformance	No performance check is required.		**P:NA** where: **NA** = Not Applicable
PoE **U**nit **R**evision **C**heck	No revision check is required.		**RC:NA** where: **NA** = Not Applicable
PoE Unit **S**afety	No safety test is required.		**S:NA** where: **NA** = Not Applicable

Table 60: PoE unit test and inspection matrix

7 Troubleshooting system issues

This chapter provides procedures you should follow to troubleshoot issues on your Smart-hopping Infrastructure, and includes:

- Troubleshooting Known Issues
- Configuration Synchronization
- Using the Serial Port Menu to Resolve Issues
- Common solutions to problems with poor RSSI and LQI
- Wireless Alerts Explanations
- Upgrade Tool Warning and Error Messages
- Restore the APC Configuration Files
- Tools for Troubleshooting
- Configuration Errors After Synchronization
- Downgrade D.02 Software to Version D.01
- Verify the Configuration of APCs and APs Using the Smart-hopping 1.0 Upgrade Tool
- Exporting and Importing APC Configuration Files

7.1 Troubleshooting known issues

Note Always use the latest version of the Upgrade Tool.

7.1.1 Upgrade Tool issues

Please note the following known issues associated with the Upgrade Tool.

- Issue: On a Philips-supplied network with redundant Core routers and Distribution Layer switches, and primary APC is connected to the Philips Supplied Network Distribution A switch, a flooding situation can occur on the network, causing an increase in broadcast network traffic. In this network state, when Upgrader.exe is run the APs may become unresponsive to the upgrade command and will either not upgrade or will take many retries to complete.

  Solution #1: Install all APCs on the Distribution Layer switch B or on any Access Layer switch.
  Solution #2: Make sure all APs are assigned to AP groups and that AP groups are associated with a specific APC. Make sure no APs are part of the Smart-hopping AP group.

- Issue: The Upgrade Tool may generate errors when roaming back from APs to an APC; especially when that APC failed to be upgraded (e.g., due to an MAPC response timeout).
  When first started, the Upgrade Tool will scan the overall Smart-hopping infrastructure and build its system configuration. From that point on, the Upgrade Tool does not scan the Smart- hopping infrastructure again. It is possible that the actual configuration may change (e.g., APC- AP-IPM partnerships may change) in the interim. Such a change would make the Upgrade Tool configuration different from that of the actual Smart-hopping infrastructure.

  Solution: The Upgrade Tool can be terminated safely at any time. We recommend that you do not run the Upgrade Tool for a very long time (in a single activation). It is best to run the Upgrade Tool to complete a specific set of tasks and then re-run it again to complete the next set of tasks. Periodically, restarting the Upgrade Tool allows it to re-scan and update its overall configuration and allow its configuration to remain in sync with that of the actual Smart-hopping infrastructure.

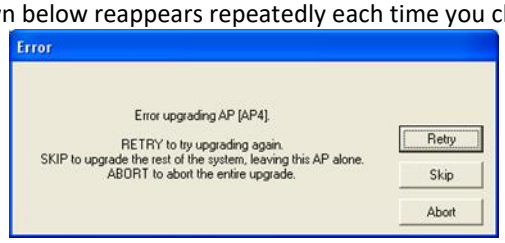
- Issue: After an APC has been upgraded, any roamed APs need to be roamed back to the upgraded APC. Although it seems that the roamed APs have been roamed back successfully, the Upgrade Tool may show the screen to roam back from APs and not let a user advance to the next screen to upgrade other APCs.

  Workaround: If you encounter this situation where you cannot advance beyond the “AP Roam Back” screen, click Cancel to exit the Upgrade Tool, and then re-run the Upgrade Tool with the Only Check Configuration option selected to confirm that the Patient Monitors have been roamed back correctly.

- Issue: Running the Philips Upgrade Tool fails to upgrade an APC on the Smart-hopping infrastructure.

  Solution: You must disconnect the APC from the Smart-hopping infrastructure, recycle power to the APC, reconnect the APC to the Smart-hopping infrastructure, and then run the Philips Upgrade Tool again.

- Issue: The error dialog shown below reappears repeatedly each time you click Retry.



  Solution: Click Skip to bypass this AP in the upgrade process. After the upgrade process completes, you must then run the Upgrade Tool again to upgrade the AP that was bypassed.

- Issue: An APC disappears from the APC web interface after being upgraded.

  Solution: Recycle power to the APC. Note, do not disconnect the APC from the Smart-hopping infrastructure before cycling its power.

- Issue: The Upgrade Tool displays a Tag 0x1103 error message.

  Cause: During an upgrade or the APC configuration synchronization process, the APs are temporarily roamed away from their preferred APC partner, and then are roamed back. This activity results in configuration changes to Tag 0x1103. After 3 minutes, the APs renew their registration which ought to eliminate any mismatches associated with this tag.

  Solution: After the Upgrade Tool completes an upgrade or synchronization process, you must wait for at least three minutes for the APs to renew their registration. After waiting three minutes, run the Upgrade Tool with the following settings to confirm that all of the errors have been corrected:
  - APC – Do not upgrade
  - Only check configuration
  - AP – Do not upgrade

7.1.2 Troubleshooting installation issues

Be sure to refer to the following list of known issues when troubleshooting operation of an installed Smart-hopping infrastructure:

- Issue: You experience poor system performance, signal dropout, and “Weak Signal” messages. Patient Monitors have difficulty roaming from one access point to another. The Power/Sync LED on the Access Points is flashing red. You receive Local Sync Loss alerts.

  Cause: Access Points are not connected to the network properly. Access Points are not synchronized to each other making roaming difficult because the Patient Monitors cannot hear the beacon from the other APs.

  Solution: Connect the APs to the Sync Unit.

- Issue: At the Philips Information Center server in the device location field, nothing is displayed; no location icon and no text.

  Cause #1: The Philips Information Center server does not have the Device Location option enabled.
  Solution #1: Device Location is an option on the Philips Information Center server, not on the DBS. It must be ordered and enabled on each Philips Information Center server.

Cause #2: The wireless client is not reporting an FMID to the Philips Information Center server.
Solution #2: The wireless client is not running a Device Location compatible revision of code.

Patient Monitors require Device FW A.00.54 and Radio FW A.00.49 or higher to support Device Location.
IntelliVue Instrument Telemetry monitors must have Revision E.00 or greater product software and Instrument Telemetry Radio Module Device FW A.00.17 plus Radio FW A.00.52 or greater.
The MRx needs Revision 9.00.00 or greater product software and Instrument Telemetry Radio Module Device FW A.00.17 plus Radio FW A.00.52 or greater.

- Issue: Layer 3 Smart-hopping on Customer Supplied Network, APC VLAN: When an APC is added to the network, or if the APC is rebooted, there may be a change in which APC is operating as the Primary APC.

  Cause: The APC VLAN is configured for IGMP v1 or v2. The APCs are using IGMP v3. When booting an APC in an existing Layer 3 Smart-hopping environment, the new APC sends out IGMP version 3 join messages. In an environment using IGMP version 2, the APC falls back to IGMP version 2 join requests (per the IGMP version 3 fall-back mechanism defined in the IGMP standard). However, by the time this fall-back to IGMP version 2 happens, the APC concludes there is no Primary present and assumes the role of a Primary APC.

  Solution: Configure the VLAN on which the APCs reside to use IGMP v3.

- Issue: Layer 3 Smart-hopping on Customer Supplied Network, AP VLANs: APs power on and operate for 1-2 minutes and then reboot.

  Cause: The AP VLAN is configured for IGMP v2 or v3. The APs uses IGMP v1.

  Solution: Configure the AP VLAN to use IGMP v1.

- Issue: After making configuration changes to the APC the changes are not applied.

  Solution: Run the AP/APC Upgrade Tool to check and update the configuration.

- Issue: If your APC uses HTTPS to communicate with the web browser and you make configuration changes to the APC, the changes are not applied.

  Solution: Before accessing the APC with a web browser and if you configured SSL encryption, make sure you installed the proper SSL certificate on the system you use to access the APC using a web browser. The certificate is available in the SSL Certificates folder in the same directory as the Upgrade Tool.

- Symptom: After new devices are added to the network, the APC configuration does not display them. Refer to FCO86200857 for complete description.

  Solution: Upgrade AP & APC software to latest version.

- Issue: After an install, a powered Remote Antenna was disconnected from and then reconnected to its Access Point via its Coax/UTP cable bundle, the Remote Antenna failed to start communicating with the Access Point.

  Solution: You must power cycle the Access Point to re-establish communications with its connected Remote Antenna.

- Issue: An Smart-hopping Access Point fails “System Validation.” The IP address in the APC AP configuration screen does not match the IP address in the AP status screen. The Bootp address is displayed in the AP status screen.

Solution: The AP never received the configured IP address change. Simply power cycle the AP so that it loads its configuration properly.

- Issue: On a routed topology, the first message to the Patient Monitor doesn't make it all the way through the network and the label assignment for each IPM must be done twice.

  Solution: Perform the label assignment twice, or upgrade the PIC to Release G or F.00.43 (FCO86200523). In these PIC releases, the message is sent twice automatically.

- Issue: The UPS connected to the Smart-hopping infrastructure devices overloads.

  Solution: During the Smart-hopping infrastructure design process, ensure that the power rating of the UPS is not exceeded by the connected devices. Refer to Table Table 1: Standard WMTS frequencieson page 32 for a list of Smart-hopping infrastructure device power draws.

- Issue: Some Smart-hopping Access Points were shipped with an incorrect MAC address range. Such APs will not appear automatically in the APC web-based management interface.

  Solution: Refer to Service Bulletin SB86200390 – 862113 for details. Manually add the AP to the Smart-hopping infrastructure by following the procedure "Adding an AP via Manual MAC Address Input" on page 116.

- Issue: On a Philips Information Center server with the Device Location application installed, "No Location" is displayed.

  Cause #1: The Device Location option is enabled on the Philips Information Center server, but the Access Point or Remote Antenna being reported by the Patient Monitor is not known to the Philips Information Center server – i.e. the AP or Remote Antenna has not been entered into the Information Center configuration.
  Solution #1: All Access Points and Remote Antennas must be entered into Information Center configuration in the DBS or standalone Philips Information Center server.

  Cause #2: During a repair, a Remote Antenna is connected to the "wrong" RA port – i.e. at the original installation, the RA was connected to the RA1 port, but after the repair it was connected to the RA2 port. The Philips Information Center server does not know RA2.
  Solution #2: When doing a repair, the Remote Antenna needs to be connected to the same RA port to which the failed device was connected.

- Issue: The clinical user is unable to take a patient out of Standby from the Information Center server. The Information Center server must be able to send a message to an APC for a clinician to be able to take a patient out of Standby from the Philips Information Center server. If the Information Center server cannot contact an APC, then the clinician cannot take a patient out of Standby from the Information Center server. Note; however, the clinician could alternately take the patient out of Standby at the Patient Monitor.

  Solution: Enter all APCs into the Information Center configuration to correct this problem.

- Issue: You encounter a Duplicate IP address system-level alert after adding an Access Point to a Smart-hopping infrastructure.

  Solution: Reconfigure the AP with a unique IP address, and then reset the AP.

- Issue: A newly added AP is not listed in the APC web interface.

  Solution: In the APC web interface, click System in the View Device tree, click Configure and then select the Advanced tab. Verify that the Allow new APs to be added automatically option is set to True.

7.2 Configuration synchronization

If the Upgrade Tool displays error messages related to the configuration between the primary and secondary APC configuration files, do the following:

1. Run the Upgrade Tool with the following settings to correct the synchronization errors:
    a. APC – Do not upgrade
    b. Smart-hopping only, check and update configuration
    c. AP – Do not upgrade

2. After the Upgrade Tool completes the synchronization process, you must wait for at least three minutes for the APs and APCs to complete synchronizing. If you do not wait three minutes, the Upgrade Tool displays new Tag 0x1103 error messages. After waiting 3 minutes, run the Upgrade Tool with the following settings to confirm that all of the errors have been corrected:
    a. APC – Do not upgrade
    b. Only check configuration
    c. AP – Do not upgrade

7.3 Using the serial port menu to resolve issues

Note The following solutions using the serial port menu apply to Revision D.02 only.

- Issue: The Primary APC stops responding.
  Solution: Connect to the serial interface menu and enter **16** at the main menu to perform a Safe Reset.

```
Please confirm: SAFE Reset MASTER Access Point Controller
        1. yes
        2. no
Enter a selection number or <ESC> -> 
```

Figure 57: Safe Reset Primary APC

Enter 1 to confirm you want to perform a safe reset of the Primary APC.

This feature saves a snapshot of the configuration currently running on the Primary APC and then reboots the Primary APC. Rebooting this Primary APC will not disrupt the rest of the system. The snapshot is only saved until the Primary APC reboots.

- Issue: The Primary APC has not acquired a physical gateway (MAC) address.
  Solution: APCs running version D.02 automatically acquire the gateway MAC address. This issue only occurred with software versions prior to D.02.

7.4 Common solutions to problems with poor RSSI and LQI

- Adjust the Access Point installation.
- The Access Point positions may need to be adjusted to avoid interference from large metal objects that can block the Access Point antennas.
- Add more Access Points.
- Add Remote Antennas if applicable.
- Place APs in the hallway.
- In some building constructions there may be significant RF loss between patient beds and the hallways where Access Points are located. In this situation the APs or Remote Antennas may need to be located

inside selected patient rooms in addition to APs in the hallway.

- A rapid change in the MX40 IPM readout indicates that some infrastructure components have not been installed correctly. Verify that all components have been correctly installed.

- Eliminate persistent noise sources.

7.5 Wireless alerts explanations

Alerts are generated by the Information Center and transmitted to Focal Point.

- Duplicate IP Address: This alert is called by an APC if it detects a duplicate IP address with any of the wireless devices.

- Duplicate FMID: This alert is called by two (or more) APs if they discovered that the last 10 bits of their IP addresses (the FMID) are the same.

- Loss of APC: This alert is called by an AP when it loses communication with the APC that is currently managing it.

- Loss of AP: This alert is called by an APC when it determines that it has lost communication with an AP (when the AP falls into the Unregistered list in the APC web browser).

- No Primary APC: This alert is called by an AP when it determines that the Primary APC has been lost. The alert will be cleared when a new APC is elected Primary.

- No Backup APC: This alert is called when the system does not meet the following criteria:
    - All APCs in the system have a priority of 0
    - Two APCs in the system have a priority of 0 and the rest have a priority of 2
      The alert is cleared when the system meets the criteria listed above.

- Loss of Remote Antenna: 1.4GHz Only - This alert is called by an AP when it determines an attached Remote Antenna is no longer responding.

- Local Sync Loss: This alert is called by an AP when it has no sync pulse.

- Remote Sync Loss: This alert is called by an AP when it determines from the sync pulse width that the sync signal from a Sync Unit upstream from its Sync Unit is not present.

- Insufficient Spectrum: This alert is called by access points. It is an indication of whether interference is impacting performance of the system. This alert only applies to the 2.4 GHz product.
  Two levels of alerts:
  Action level: Generates a “Wireless Monitoring Loss – Contact Service” system message.
  Warning level: Logged but only reported in APC Web Browser.

7.6 APC roles

APCs are assigned priorities (roles) based on the Priority Level configured using the APC serial port configuration menu:

- P: Primary – Current Primary APC
- B: Backup – Priority set to 0, and is not the current Primary APC
- S: Secondary – Priority set to 2, and is not the current Primary APC

They are displayed on the APC web view, as shown in Figure 59.

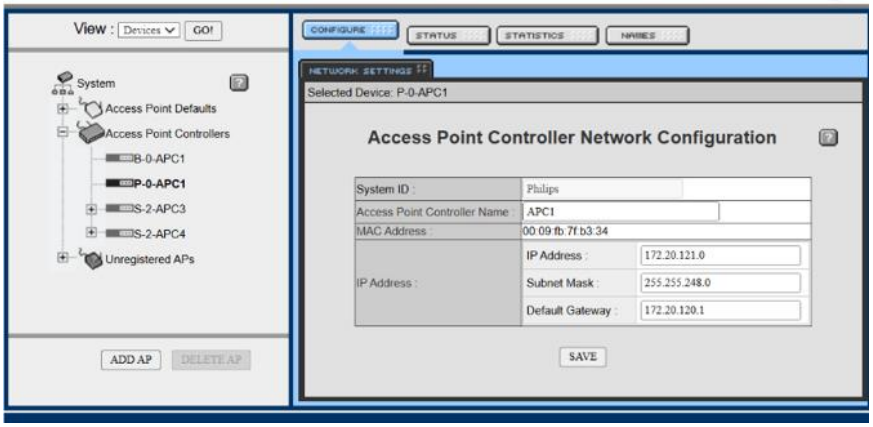


Figure 58: APC Role and Priority Displayed in Web Interface View

The backup primary APC feature requires three or more APCs - one primary APC (shown with a P in the web view), one backup primary APC (shown with a B in the web view), and at least one secondary APC (shown with an S in the web view).

7.7 Upgrade Tool warning and error messages

The Upgrade Tool will upload the APC system configuration and check that it conforms to the system requirements and installation rules, and verify that the Secondary APC configuration matches the Primary APC configuration.

Configuration update is done by normal APC update processing, so the APC does not need to be rebooted, and data flow is not interrupted, while configuration update is performed.

If an installation rule is broken, a Warning Message is generated and written to the summary report. If a system requirement is broken, an Error Message is generated and written to the summary report, and the upgrade is aborted. If the Primary and Secondary configuration are mismatched, the Upgrade Tool attempts to force the Secondary APC to upload a copy of the Primary APC configuration.

You should take the appropriate response to a warning or error message as follows:

- Warning Message - A warning allows you to continue with the APC upgrade.
    - Issue: If the system is not configured properly, or if a Primary or Backup Primary APC has failed, service personnel are notified with this warning:

      ```
      WARNING: System installation requires APC Priority setting to be 0 for
      either all APCs or exactly 2x APC (Primary and 1x Backup APC)
      ```

      Solution: To properly use the backup primary feature, see “APC Roles” on page 137 for more information.

- Error Message - An error must be corrected before the upgrade can be completed. To correct an error, it may be necessary to take the APC down. Appropriate notification will be given under these circumstances.

    - You can fix errors on the primary APC through the web interface or the APC serial console menu. Examples:

      ```
      *** ERROR: All APs do not have same WMTS channel configuration,
      00:09:FB:15:D7:67 has [1 2 3 4 ] enabled, 00:09:FB:25:40:81 has [1 2 3
      4 5 6]enabled

      *** ERROR: RF Access Code: AP is 1, AP's Group is 92
      ```

- Errors on the secondary APC file can be corrected by running the Upgrade Tool using the Smart-hopping Only, Check and Update Configuration option. Errors in the Secondary APC configuration are corrected automatically when possible by forcing the Secondary APC to synchronize with the Primary APC. For example:

```
*** ERROR: Tag in Secondary, not present in Primary: 0x1102 (Possible tag names:
PROXIM_TAG_WCS_MANUAL_PART, PROXIM_TAG_FILTER_NETBEUI_ENABLE_TAG)length 1, value 1
(0x1)
```

The Upgrade Tool generates warning and error messages based on the presence of and content of a number of configuration files resident on the APC.

This section lists and describes the possible warning and error messages generated by the Upgrade Tool in the context of their associated configuration file.

The following tables document APC configuration files and their associated warning and error messages.

Item/Rule	Description
Comments	• APC specific information such as MAC address and IP address settings. • This file must be present. • This file will be checked if the Smart-hopping only option is selected. • To fix errors or warnings in this file, use the APC serial menu to correct the settings.
General Rules	• Check that the file itself is not corrupt (correct length, all fields given below are present). Error: APC boot file length is incorrect Error: [Data item] not found in boot file • Check that last 3 bytes of MAC address are non-zero. Warning: APC MAC address is default • Check that the MAC address is either Philips (00:09:FB:xx:xx:xx) Error: MAC address is corrupt • Check that the APC has a static IP address. Warning: DHCP flag set • Check that the static IP address is not class D or E. Error: Class D/E IP addresses are illegal • Check that the subnet mask is non-zero. Error: Subnet mask must not be zero • Check that the default gateway is either zero or on the same subnet as the APC. Error: Gateway and IP address are on different subnets
Primary APC	No checks
Secondary APC	Check that the secondary APC is on the same subnet as the primary APC. Error: Secondary and primary are not on same subnet

Table 61: BOOTROM.NVP warnings and erros

Item/Rule	Description
Comments	• This file must be present. • This file is checked if the Smart Hopping only option is selected.
General Rules	No checks.
Primary APC	No checks.
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…]

Table 62: PASSWORD.TLV warnings and errors

Item/Rule	Description
Comments	• System specific information. • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • Errors on the secondary file can be corrected by running the Upgrade Tool (using the Smart-hopping Only, Check and Update Configuration option). • Errors on the primary can be fixed through the web interface, on the System config screens (“BOOTP/DHCP” and “SUBNET TABLE” tabs). System type on the APC can be configured through the APC serial menu. • The Upgrade Tool allows you to initiate the scan with the Use Secure communication option when HTTPS is enabled all APCs • User and password info for logging in to the APC web interface.
General Rules	No checks.
Primary APC	• Check that the System Type (1.4 GHz or 2.4 GHz) stored in the APC matches the selection made on the Upgrade Tool UI. Error: System type on APC is [type], tool has been configured to verify a [type] system • Check that the DHCP configuration matches the default. Warning: Non-default System DHCP Table configuration • Check that the subnet table configuration matches the default. Warning: Non-default subnet table configuration • Check that any ranges in the DHCP configuration that would match AP MAC addresses would not allow two APs to have duplicate ten low bits of IP address. • Error: Range n in DHCP table is invalid: duplicate FMIDs could result. Low ten bits of AP IP addresses must be guaranteed unique
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though); except the APC name TLV. Error: Secondary and primary files have differing contents [details…]

Table 63: PARAM/SYSTEM.TLV warnings and errors

Item/Rule	Description
Comments	• Filter configuration information. • This file must be present. • This file will be checked if the Smart Hopping only option is selected. Errors on the secondary file can be corrected automatically; errors on the primary can be fixed through the web interface, on the System config screens (“FILTERS” tab).
General Rules	No checks.

Primary APC	• Check that each filter setting matches the default. Warning: Non-default [filter] configuration
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…]

Table 64: PARAM/FILTER.TLV warnings and errors

Item/Rule	Description
Comments	• Authorization details for specific Patient Monitors. • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • Errors on the secondary can be corrected automatically; errors on the primary can be fixed through the web interface System config screens (“AUTHORIZATION TABLE” tab).
General Rules	No checks.
Primary APC	• Check that the authorization table is unused and has no entries Error: Authorization table is in use.
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though) Error: Secondary and primary files have differing contents [details…]

Table 65: PARAM/AUTHTBL.TLV warnings and errors

Item/Rule	Description
Comments	• DHCP Server IP address assignment information. • This file may not be present if no DHCP assignments have been made. • This file will be checked if the Smart Hopping only option is selected. • Errors on the secondary can be corrected automatically; errors on the primary can be fixed through the web interface System config screens (“BOOTP/DHCP” tab, click to view allocations, “Purge allocations”).
General Rules	No checks.
Primary APC	• Check that the file header is correct. Error: Primary DHCP file header incorrect • Check that all entries have Philips or Proxim MAC addresses Warning: unrecognized MAC address in DHCP table • Check that all entries for AP MAC addresses have unique ten low bits of IP address (cross checked against manually configured APs in the WTMS.TLV file) Error: AP x:x:x:x:x:x and AP x:x:x:x:x:x have duplicate low ten bits of IP address
Secondary APC	• The file headers on the primary and secondary files must match. Error: DHCP File headers do not match • The file must contain the same set of DHCP entries on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…]

Table 66: CONFIG/DHCP.TLV warnings and errors

Item/Rule	Description
Comments	• Group configuration information for Smart Hopping AP groups • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • Errors on the secondary file can be corrected automatically; errors on the primary can be fixed through the web interface, Group config screens.
General Rules	No checks.
Primary APC	• APs have default group basic configuration. Warning: APs have non-default group basic [specific item] configuration • APs have default group alert configuration. Warning: APs have non-default group alert [specific item] configuration • APs have default group radio configuration. Warning: APs have non-default group radio [specific item] configuration • APs have default advanced group configuration. Warning: APs have non-default advanced [specific item] group configuration. • Group configuration has default check boxes checked for enabling items on configuration screen. Warning: Non-default configuration: [specific item] on [specific group config screen], enable checkbox should be [set / unset]
Secondary APC	• The file must contain the same set of Groups on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…] • Each Group must contain the same set of Group TLVs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have different group configurations [details…] • Each Group must contain the same set of AP TLVs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have different AP configurations [details…]

Table 67: CONFIG/TABLE/GRPSWMTS.TLV warnings and errors

Item/Rule	Description
Comments	• AP configuration information for Smart-hopping APs • This file may not be present if no Smart-hopping APs are configured on the system. • This file is checked if the Smart-hopping only option is selected. • Errors on the secondary file can be corrected automatically; errors on the primary can be fixed through the web interface, individual AP configuration screens.
General Rules	No checks.
Primary APC	• All APs on same subnet. Error: APs are not all on same subnet • All entries for AP MAC addresses have unique ten low bits of IP address (cross checked against manually configured APs in the DHCP.TLV file). Error: AP x:x:x:x:x:x and AP x:x:x:x:x:x have duplicate low ten bits of IP address • WMTS systems only: All APs have same WMTS channel configuration. Error: APs do not all have same WMTS channel configuration • ROW Z.nn.nn systems only: All APs have same ISM area configuration. Error: APs do not all have same ISM area configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Radio Regulation Code configuration. Error: APs do not all have same ISM Radio Regulation Code configuration

	• ROW B.00.03 and onwards systems only: All APs have same ISM Frequency Plan configuration. Error: APs do not all have same ISM Frequency Plan configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Zigbee Channel configuration. Error: APs do not all have same ISM Zigbee Channel configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Advanced Channel configuration • Error: APs do not all have same ISM Advanced Channel configuration • APs have been set up with a preferred partner. Warning: APs have been configured with no preferred partner • APs are not disabled. Warning: AP has been disabled • APs have default RF Access code configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart Hopping Group settings (warning), and APs own group settings (error). Warning/Error: RF Access Code enable: AP is [set / unset], [AP Default / Default Smart-hopping Group / AP Group] is [unset / set] APs have default WMTS Channels configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart-hopping Group settings (warning), and APs own group settings (error). Warning/Error: WMTS Channels: AP has [channels] enabled, [AP Default / Default Smart-hopping Group / AP Group] has [channels] enabled • ROW Z.nn.nn systems only: APs have default ISM area code configuration - cross- check each entry in AP file against AP template defaults (warning), default Smart- hopping Group settings (warning), and the AP group settings (error) Warning/Error: ISM area code: AP is [area], [AP Default / Default Smart Hopping Group / AP Group] is [area] • ROW B.00.03 and onwards systems only: APs have default ISM Radio Regulation Code configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart-hopping Group settings (warning), and the AP group settings (error). Warning/Error: ISM Radio Regulation Code: AP has [code], [AP Default / Default Smart-hopping Group / AP Group] has [code] • ROW B.00.03 and onwards systems only: APs have default ISM Advanced Channels configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart-hopping Group settings (warning), and the AP group settings (error). Warning/Error: ISM Advanced Channels: AP has [channels] enabled, [AP Default / Default Smart-hopping Group / AP Group] has [channels] enabled
Secondary APC	• The file must contain the same set of APs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…] • Each AP must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…]

Table 68: CONFIG/TABLE/WMTS.TLV warnings and errors

Item/Rule	Description
Comments	• Default AP configuration for Smart-hopping APs • This file may not be present if no changes have been made to the default template settings. • This file will be checked if the Smart-hopping only option is selected. • Errors on the secondary can be fixed automatically; errors on the primary can be fixed through the web interface, Access Point Default settings.
General Rules	No checks.
Primary APC	• APs have default basic configuration. Warning: APs have non-default basic [specific item] configuration • APs have default alert configuration. Warning: APs have non-default alert [specific item] configuration • APs have default radio configuration. Warning: APs have non-default radio [specific item] configuration
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though). Error: Secondary and primary files have differing contents [details…]
General Rules	No checks.

Table 69: CONFIG/TEMPLATE/WMTS.TLV warnings and errors

7.8 Restore the APC configuration files

You must perform this task on the Primary APC. To restore the APC configuration, select the Restore this APC Config Files menu option and enter the option number for yes. To return to the menu without restoring the configuration files, press the option for no or press Esc.

Restoring APC configuration files works with the following requirements:

- Recovery only functions if a valid backup configuration file exists on the Primary APC.
- The restore function must be run on the Primary APC.
- If no backup is stored, the restore has no effect and keeps the APC configuration unchanged.
- The restore takes effect only after the user resets the Access Point Controller.
- When a configuration is restored on the Primary APC, the configuration is then propagated to all Secondary APCs, in order to make sure all APC configurations synchronize with the Primary APC.

7.9 Tools for troubleshooting

7.9.1 AP/APC Upgrade Tool

The AP/APC Upgrade Tool is used to ensure that all devices are at a compatible revision of code, there are no serious configuration errors (like having APs with different RF Access Codes or different channels), and that all of the Secondary APCs have the same configuration as the Primary APC.

7.9.2 Coverage assessment tools

The TRx4841A/4851A and MX40 have a coverage assessment mode which will report the received signal strength in Service Mode in the Instrument Telemetry Diagnostic screen. The MRx defibrillator will report the received signal strength in the “Network Settings” screen.

7.9.3 Wireless statistics

You can use Focal Point for troubleshooting the Smart-hopping Infrastructure. It relies on alerts and statistics gathered from the Smart-hopping access points, Patient Monitors, and access point controllers. These alerts and statistics are stored in a database in the Information Center server.

7.9.4 PIC iX displays inconsistent APC role information

What APC name is scanned into the PIC iX configuration depends on the PIC iX revision and if the APC is using http or https (see the example in table 71).

Since the APC role may change dynamically over time, it could be confusing to leave it as part of the name. The APC name can be edited to remove the role and priority in the PIC iX.

Web Browser	PIC iX B.xx, C.xx (or higher) Network Scan	PIC iX C.03.01 Network Scan	PIC iX C.03.01 Scan Using Export File	In PIC iX, edit name for consistency
Protocol	HTTP	HTTP	HTTPS	
B-0-APC2	B-0-APC2	B-0-APC2	APC2	APC2
P-0-APC1	P-0-APC1	APC1	APC1	APC1
S-2-APC3	S-2-APC3	S-2-APC3	APC3	APC3
S-2-APC4	S-2-APC4	S-2-APC4	APC4	APC4

Table 70: APC role information

7.10 Configuration errors after synchronization

If the Upgrade Tool displays error messages related to the configuration between the primary and secondary APC configuration files, do the following:

1. Run the Upgrade Tool with the following settings to correct the synchronization errors:
    a. APC – Do not upgrade
    b. Smart-hopping only, check and update configuration
    c. AP – Do not upgrade
2. Once this completes, wait three minutes and run the Upgrade Tool again, with the following settings, to confirm the errors are corrected:
    a. APC – Do not upgrade
    b. Only check configuration
    c. AP – Do not upgrade
3. If configuration errors still exist, do the following:
    a. Remove the APC that does not synchronize from the network (disconnect the RJ-45 cable connecting the APC to the switch or router).
    b. Using the serial port console menu, select the Reset APC to Factory Defaults option. This causes the APC to restart.
    c. Follow the instructions located in “Replacing an Smart-hopping APC” on page 123.

7.11 Downgrade D.02 software to version D.01

Note You need both the D.02 version and version D.01 (A.00.25) of the Upgrade Tool to downgrade from version D.02 to D.01.

To downgrade your Smart-hopping infrastructure from version D.02 to version D.01, follow these steps:

1. Before downgrading your APCs, make sure you disable HTTPS mode on all APCs (version D.01 software does not support HTTPS communication; HTTPS communication in a D.01 environment may corrupt the APCs).

a. To disable HTTPS mode on your APCs, connect a serial cable to your APC (“Using the APC Serial Menu Console” on page 171contains instructions for connecting a serial cable to your APC). This avoids communication issues between the APCs and APs during the downgrade.
b. From the main console menu, enable the Security and Advanced Parameters menu option.
c. Disable the Secure Communication Via SSL option from the main console menu.

2. Using the D.02 version of the Upgrade Tool, run the Upgrade Tool using the following configuration options, to make sure there are no configuration errors:
   a. APC - Do not upgrade
   b. Only check configuration
   c. AP - Do not upgrade

3. Make sure the Upgrade Tool reports no errors. If error messages point to synchronization issues with the APCs, run the upgrader.exe program using the following configuration options to resolve the errors:
   a. APC - Do not upgrade
   b. Smart-hopping only, check and update configuration
   c. AP - Do not upgrade
   Wait three minutes for all devices to synchronize. If you still encounter errors, follow the instructions found in “Configuration Errors After Synchronization” on page 136.

Caution In the event of monitoring loss after downgrading the APC to a version lower than D.02, make sure the Acquire Gateway Physical Address menu option is enabled (APC vD.02 software automatically enables this feature).

4. Export a copy of the system configuration file. Run the Upgrade Tool using the following configuration options, to export a copy of the version D.02 configuration file:
   a. APC - Do not upgrade
   b. Only check configuration
   c. AP - Do not upgrade
   d. Under Configuration, select Export

Note Downgrade the primary APC first.

5. Using the D.01 version of the Upgrade Tool, run the Upgrade Tool using the following configuration options to downgrade the APCs:
   a. APC - Force Upgrade
   b. Ignore configuration
   c. AP - Do not upgrade

6. Run the Upgrade Tool using the following configuration options to downgrade the APs:
   a. APC - Do not upgrade
   b. Ignore configuration
   c. AP - Force Upgrade

7. Connect a serial cable to the primary APC and open the serial port console menu. From the Advanced Configuration menu, clear the web browser user ID and password (make sure the fields are blank before pressing Enter). You only need to do this on the primary APC - it propagates the change to the other APCs.

8. Using the D.01 version of the Upgrade Tool, run the Upgrade Tool using the following configuration options, to make sure there are no configuration errors:
   a. APC - Do not upgrade
   b. Only Check configuration
   c. AP - Do not upgrade
   The downgraded APCs ought to synchronize properly, producing no errors or warnings. If you encounter errors, follow the instructions found in “Configuration Errors After Synchronization” on page 136.

9. Export a copy of the system configuration file. Run the Upgrade Tool using the following configuration options, to export a version D.01 configuration file:
    a. APC - Do not upgrade
    b. Only check configuration
    c. AP - Do not upgrade
    d. Under Configuration, select Export

7.12 Verify the configuration of APCs and APs using the Smart-hopping 1.0 Upgrade Tool

The Smart-hopping 1.0 Upgrade Tool can verify that APCs on your network are configured correctly and display warning and error messages that you may use to troubleshoot any configuration errors that may exist on your Smart-hopping network.

Follow these steps to verify the configuration of the Smart-hopping Access Point Controllers and Access Points using the Upgrade Tool:

1. Run the Upgrade Tool on your Service PC by double-clicking the Upgrader.exe file: The Upgrade Tool splash screen appears.

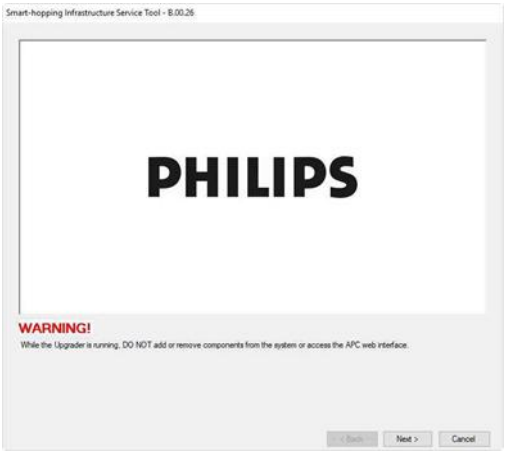


Figure 59: Upgrade Splash Screen

2. Click Next to continue. The APC/AP firmware selection screen appears.

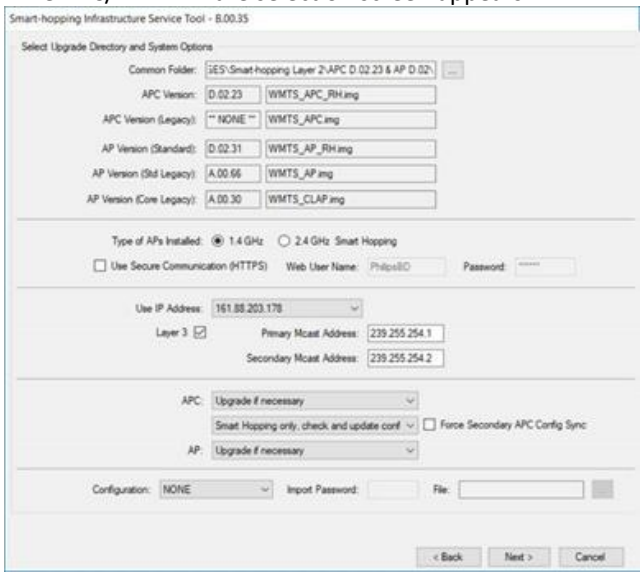


Figure 60: APC/AP Firmware Selection Screen

3. Complete the settings on the APC/AP firmware selection screen:
    a. Click and then browse to the directory (e.g., C:\TelemetryUpgrader\AP and APC Images\) in which you have installed the APC and AP firmware files.
    b. Specify what type of APs you have installed by marking the appropriate radio button, 1.4 GHz Smart Hopping or 2.4 GHz Smart Hopping.
    c. Verify that the correct firmware versions are displayed in the APC Version, AP Version (Standard), and AP Version (Cluster) fields.
    d. Select the ICN IP address (e.g., 172.31.240.4) you have configured for the support PC on which you are running the Upgrade Tool from the Use IP Address drop-down menu. The menu lists the IP addresses of all Ethernet NICs configured on the PC.
    e. For the upgrade options in the firmware selection dialog box, choose these specific options for each respective selection. See table 72 below.

Label	Option	Information
APC	Do Not Upgrade	Do not allow each APC to be upgraded
	Only Check Configuration	Verify the APC configuration
AP	Do Not Upgrade	Do not allow each AP to be upgraded

Table 71: Upgrade options

4. Click Next to verify the Smart-hopping configuration.
   After the Upgrade Tool has verified the configuration on all APCs and APs, review the Upgrade Tool Report screen to verify that there are no Smart-hopping configuration errors present.

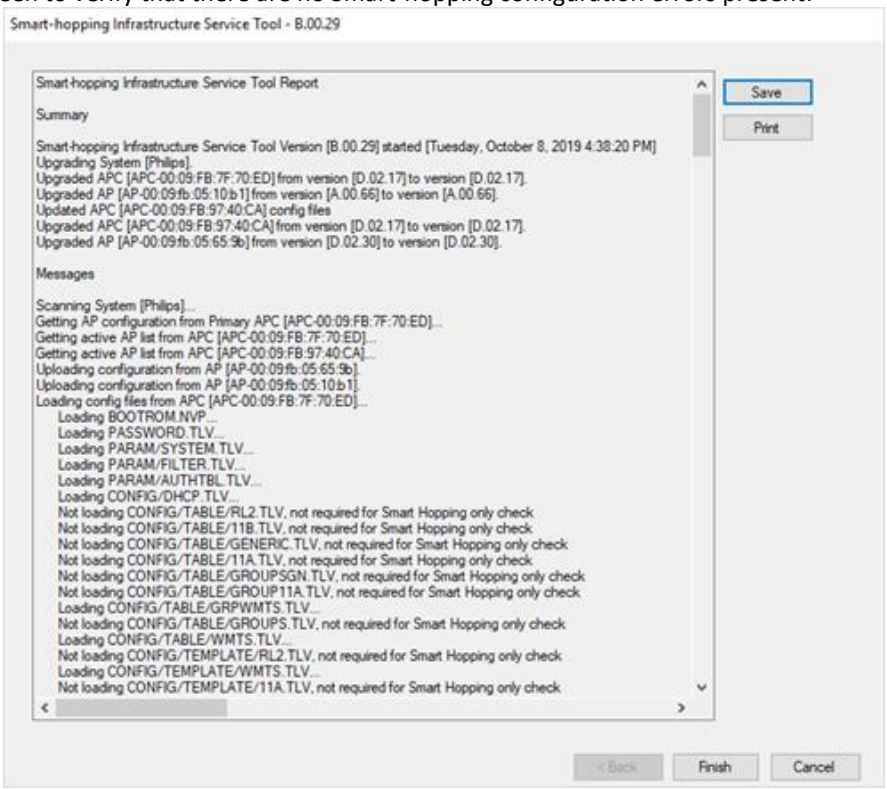


Figure 61: Upgrade Tool Report

5. Click Save to save the Upgrade Tool report to a disk file on your service PC.
   After saving the Upgrade Tool Report to a disk file, you should open the text file in Notepad and execute a find for the strings “error” and “warning.” All errors must be corrected and all warnings be reviewed. See “Upgrade Tool Warning and Error Messages” on page 138 for descriptions of possible error and warning messages.

6. Click Finish to close the Upgrade Tool.
   Note the Upgrade Tool automatically creates a log file, logfile.txt, in the directory from which it was run.

7.13 Exporting and importing APC configuration files

You can export a system configuration from an Access Point Controller to a disk file and import a previously exported configuration file to an Access Point Controller by running the Upgrade Tool.

Note Before exporting any configuration files, you must run through the Upgrade Tool configuration checking process and correct any errors that are found. If you do not correct errors prior to exporting the configuration, the exported archive will contain errors.

To export the Smart-hopping configuration to a file in both human- and machine-readable formats:

Export a Configuration File

1. Run the Upgrade Tool on your Service PC by double-clicking the Upgrader.exe file located in the folder you copied the Upgrade Tool.
   The Upgrade Tool splash screen appears.

2. Click Next> to continue.
   The APC/AP firmware selection screen (Figure 63) appears.

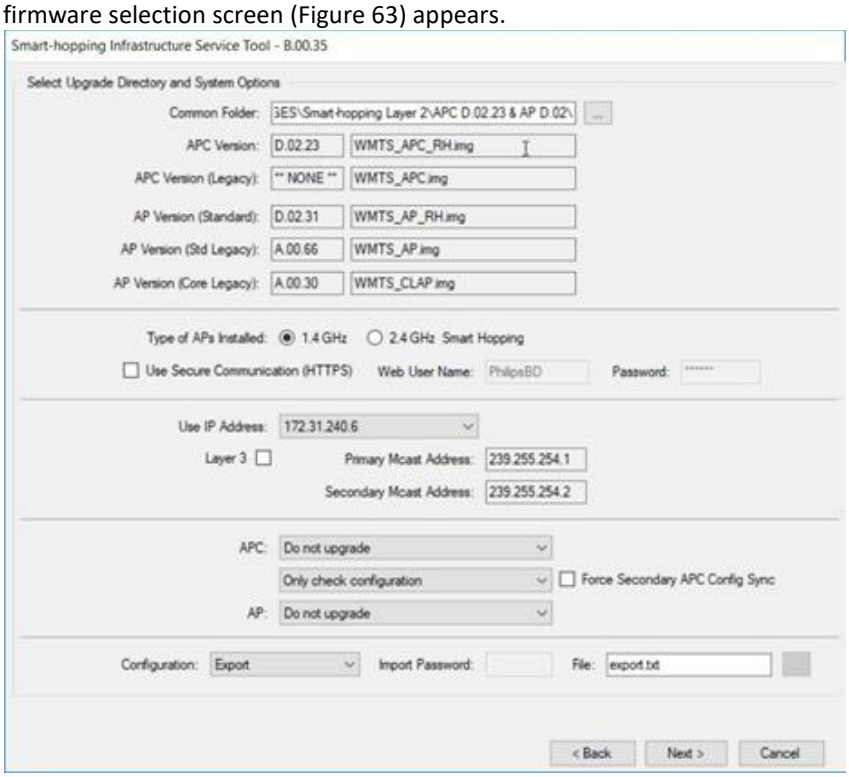


Figure 62: Exporting an Smart-hopping Configuration

   a. Specify what type of APs you have installed by marking the appropriate radio button - 1.4 GHz Smart Hopping or 2.4 GHz Smart Hopping.
   b. Deselect the Layer 3 check box for Layer 2 operation. If operating in Layer 3 mode, select the Layer 3 check box, and enter the Primary and Secondary Multicast Addresses.

c. For the upgrade options in the firmware selection dialog box, choose these specific options for each respective selection. See table 73 below.

Label	Option	Information
APC	Do Not Upgrade	Do not allow each APC to be upgraded
	Only Check Configuration	Verify the APC configuration
AP	Do Not Upgrade	Do not allow each AP to be upgraded

Table 72: Upgrade options

d. In the Configuration drop-down box, select Export.
e. The file name is export.txt. Do not change the file name.

3. Click Next to create the specified Smart-hopping configuration file.
   a. When you export files using the Upgrade Tool, the process places the following files and folders into the exports folder (located in the same directory as the upgrader.exe file:
      i. The APC configuration file (export_YYYYMMDD-HHMMSS.txt)
      ii. An additional file (export_YYYYMMDD-HHMMSS.CSV), an equipment inventory list
      iii. A folder (YYMMDD-HHMMSS), that contains copies of the configuration files (in binary format), used for importing Smart-hopping devices into the PIC iX system Network Scan

   The exported file containing the configuration archive is stored on the service PC (in the exports folder on the directory from which you run the Upgrade Tool). All configuration items on the APC are archived to the specified file. A sample exported APC configuration file is shown in Figure´64.

```
########################################
#    SMART HOPPING SYSTEM EXPORT FILE     #
########################################
System {  APC MAC 00:09:FB:97:00:DA {    File String  "BOOTROM.NVP" {      MAC 00:09:FB:97:00:
    File String  "PASSWORD.TLV" {      Tag Word 1700      {        Bytes { 00 00 00 00 }
    File String  "PARAM/SYSTEM.TLV" {      Tag Word 1310      #Possible tag names:
      #SYS_WEB_USERNAME_TAG
      {        String  "PhilipsBD"        Bytes { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      #SYS_WEB_PASSWORD_TAG
      {        Bytes { 2C 38 2C E2 A2 9A A4 9A F0 5A 84 DF A6 07 44 E3 }        Bytes { F6 C2
      #SYS_WEB_PORT_TAG
      {        Bytes { 00 00 00 50 }      }      Tag Word 1320      #Possible tag names:
      #SYS_WEB_ENABLED_TAG
      {        Byte 01      }      Tag Word 1322      #Possible tag names:
      #SYS_MCAST_ENABLED_TAG
      {        Bytes { 00 00 00 00 }      }      Tag Word 1324      #Possible tag names:
      #SYS_TRAP_CFG_MASTER_RESOLUTION_ENABLE_TAG
      {        Byte 01      }      Tag Word 1325      #Possible tag names:
      #SYS_TRAP_CFG_TUNNELED_STATION_THRESHOLD_TAG
      {        Bytes { 00 00 00 32 }      }      Tag Word 1326      #Possible tag names:
      #SYS_TRAP_CFG_TUNNELED_AP_THRESHOLD_TAG
      {        Bytes { 00 00 00 1E }      }      Tag Word 1327      #Possible tag names:
      #SYS_TRAP_CFG_MANAGED_AP_THRESHOLD_TAG
      {        Bytes { 00 00 00 32 }      }      Tag Word 1328      #Possible tag names:
      #SYS_TRAP_CFG_SYSTEM_UTILIZATION_THRESHOLD_TAG
      {        Bytes { 00 00 00 50 }      }      Tag Word 1303      #Possible tag names:
      #PROXIM_TAG_APC_NAME2
      {        String  "APC-CL115"      }      Tag Word 1304      #Possible tag names:
      #SYS_SYSTEM_NAME_TAG
      #PROXIM_TAG_AP_SYSTEM_NAME
      {        String  "Philips"      }      Tag Word 1305      #Possible tag names:
      #SYS_AP_ADD_ENABLED_TAG
      {        Byte 01      }      Tag Word 1311      #Possible tag names:
      #SYS_WCS_REPEATING_ENABLED_TAG
      {        Byte 00      }      Tag Word 1307      #Possible tag names:
      #SYS_CONFIGURATION_KEY_TAG
      {        Bytes { 00 00 B7 68 }      }      Tag Word 1308      #Possible tag names:
```

Figure 63: Sample Exported APC Configuration File

4. Click Finish to close the Upgrade Tool.
   Note the Upgrade Tool automatically creates a log file, logfile_YYYYMMDD-HHMMSS.txt, in the logs folder.

5. Locate the Smart-hopping export files, the Upgrade Tool report, and the Upgrade Tool log file, and move these files to an archive folder on your service PC for safekeeping. The files and folders you want

to move contain the following (**note** you are starting from the same directory in which the Upgrade Tool executable file is located). See table 74.

The relevant APC configuration files and an overview of their content is provided in Chapter 3.

exports\ (folder)			
	export_YYYYMMDD-HHMMSS.CSV (a Comma Separated Value file, most commonly opened in Excel, that contains the current device inventory list)		
	export_YYYYMMDD-HHMMSS.TXT (a text file containing the configuration information of the primary APC)		
	YYYYMMDD-HHMMSS\ (a folder that contains the configuration files [in binary form])		
		APC -<MAC Address> (Primary)\ (where <MAC Address> is the MAC Address [in 00:00:00:00:00:00 form] - folder containing Primary APC configuration files	
			BOOTROM.NVP
			PARAM_SYSTEM.TLV
			CONFIG_DHCP.TLV
			CONFIG_TABLE_GROUPS.TLV
			CONFIG_TABLE_WMTS.TLV
			COMBINED_SYSTEM.TLV (only for the Primary APC)
		APC<MAC Address>\ (where <MAC Address> is the MAC Address [in 00:00:00:00:00:00 form] - folder containing APC configuration files)	
			BOOTROM.NVP
			PARAM_SYSTEM.TLV
			CONFIG_DHCP.TLV
			CONFIG_TABLE_GROUPS.TLV
			CONFIG_TABLE_WMTS.TLV

Table 73: Folder structure of APC configuration export files

7.13.1 Importing Smart-hopping configuration files

The Upgrade Tool can import an APC/AP configuration file (for the purposes of restoring a configuration).

Note The configuration file import process should only be done by a Phillips-trained service person who is familiar with the Smart-hopping installation and only in the case of system disaster recovery (i.e., the Smart-hopping monitoring is completely not working).

An APC configuration file is MAC address-specific and can only be imported back into the system from which it was originally exported.

This import process must not be done on active clinical systems.

To ensure that the configuration import works properly, you must follow these steps:

1. Ensure that all APCs that were online when the export file was created are online before the file import is initiated.

2. Remove all APs from the network by powering down the appropriate PoE Units.

3. To import a configuration to the primary APC, run the Upgrade Tool.
    a. After the Upgrade Tool starts, make the following settings as appropriate for your network:

i. Select the appropriate AP type, 1.4 GHz or 2.4 GHz when the Upgrade Tool starts.
ii. For the upgrade options in the firmware selection dialog box, choose these specific options for each respective selection. See table 75.

b. In the Configuration drop-down box, select Import include Pri APC.
c. Enter the password to import the configuration file.
d. Click to select the configuration file.
e. Click Next to start running the Upgrade Tool.

Label	Option	Information
APC	Do Not Upgrade	Do not allow each APC to be upgraded
	Ignore Configuration	
AP	Do Not Upgrade	Do not allow each AP to be upgraded

Table 74: Upgrade options

After the import process is complete, you must:

1. After the Upgrade Tool has verified the configuration on all APCs and APs, review the Upgrade Tool Report screen to verify that there are no configuration errors present. If there are any configuration errors present, you must correct the errors before modifying the Smart-hopping infrastructure. For more information on verifying the system configuration with the Upgrade Tool, see “Verify the Configuration of APCs and APs Using the Smart-hopping 1.0 Upgrade Tool” on page 147.

2. Add the APs back onto the network:
   a. Add up to 24 APs back onto the network by powering up a PoE Unit or PoE Switch.
   b. Verify that newly added APs appear in the APC web interface and then run the Upgrade Tool again. For the upgrade options in the firmware selection dialog box, choose these specific options for each respective selection. See table 76 below.

   Note Do NOT keep refreshing your web browser while waiting for the newly added APs to appear in the APC web interface. Refreshing the APC web interface too frequently will only slow down communications on the entire Smart-hopping infrastructure.

   c. Repeat Steps a and b until all APs have been added back to the network.

   Note that all configuration files are imported in full except for the following:

   d. SYSTEM.TLV - This file is imported tag by tag, except for the following data which is ignored: APC Name, System Name, Configuration Key info, Web username/password/config info, AP_CFG_PRESIDE.
   e. BOOTROM NVP - This file contains the APC MAC address and static IP address/subnet mask/ default gateway. These settings should only be edited using the bootloader serial menu on the APC.

Label	Option	Information
APC	Do Not Upgrade	Do not allow each APC to be upgraded
	Only Check Configuration	Verify the APC configuration
AP	Do Not Upgrade	Do not allow each AP to be upgraded

Table 75: Upgrade options

8 Appendix A: Installing multiple smart-hopping systems at a single hospital site

You can install independent Smart-hopping systems at a given installation site if you follow the configuration rules and guidelines given in this appendix. This appendix includes:

- General Requirements for Installing Multiple Smart-hopping systems at a Site
- Patient Monitor Installation Requirements for Multiple Smart-hopping systems
- Sync Network Requirements for Multiple Smart-hopping systems

8.1 General requirements for installing multiple smart-hopping systems at a site

You can install independent Smart-hopping systems in a hospital.

The basic design rules for using multiple Smart-hopping systems at a single installation site are:

- Each Smart-hopping system must use a different RF Access Code (1 - 254) to ensure that every wireless client connects to the correct AP.
- Every Patient Monitor in the hospital needs a unique Equipment Label (no duplication of labels).
- A common Sync Network is required if the Smart-hopping systems are on adjacent floors, or if the linear distance between access points on the same floor is less than 300 feet.
- The Smart-hopping systems do not have to be synchronized to each other if they are separated by two or more floors, or if the linear distance between access points on the same floor is greater than 300 feet.
- If there are multiple Layer 3 Smart-hopping systems in operation at a site, the systems need to use a unique pair of Multicast addresses (Primary APC Multicast Address, Secondary APC Multicast Address) for proper communication between the APCs and APs.
- Each PIC iX subnet can have a single isolated Smart-hopping system (non-routed) or be connected by a router to a single Smart-hopping system (routed).
- Each PIC iX Clinical Unit may be associated with a single Smart-hopping system or Zone.

8.2 Patient monitor installation requirements for multiple smart-hopping systems

New installations or replacement of a 1.4/2.4 GHz Patient Monitor requires an association process to establish a connection with the Smart-hopping infrastructure and the IntelliVue Network Central Station to get an equipment label assigned. Normal monitoring cannot proceed until the Patient Monitor has been assigned an equipment label.

8.2.1 Patient monitors

When an Patient Monitor is shipped from the factory, it is shipped with an Equipment Label of “New Device” and an RF Access Code of “0”. This allows it to connect to any access point (AP). However, a new Patient Monitor will connect to the first access point it detects—not necessarily the AP that is closest.

If you do not see the MAC address appear in the Label Assignment screen, then it is possible that the Patient Monitor is connected to an access point associated with a different network. You can try to reboot the Patient Monitor and then click the Refresh key until you see the MAC address appear in the Label Assignment Screen., or you can manually change the RF Access Code on the device to ensure it connects to the desired system.

If the systems are so close that it is likely that an Patient Monitor will connect to another system during the installation process, then it is likely that you will see extra MAC addresses in the Label Assignment screen. These are IPMs from the other system that connected, but were not assigned a label because they connected to the wrong system.

If a user wants to move an Patient Monitor to a new area with a different RF Access Code, then the Patient Monitor must be re-configured as a ‘new device’ with no equipment label assigned, then assign the Patient Monitor to the new AP group and Clinical care unit.

8.3 Sync network requirements for multiple Smart-hopping systems

The design rules for synchronization of multiple Smart-hopping Systems:

- A common Sync Network is required if the Smart-hopping systems are on adjacent floors, or if the linear distance between system access points on the same floor is less than 300 feet.

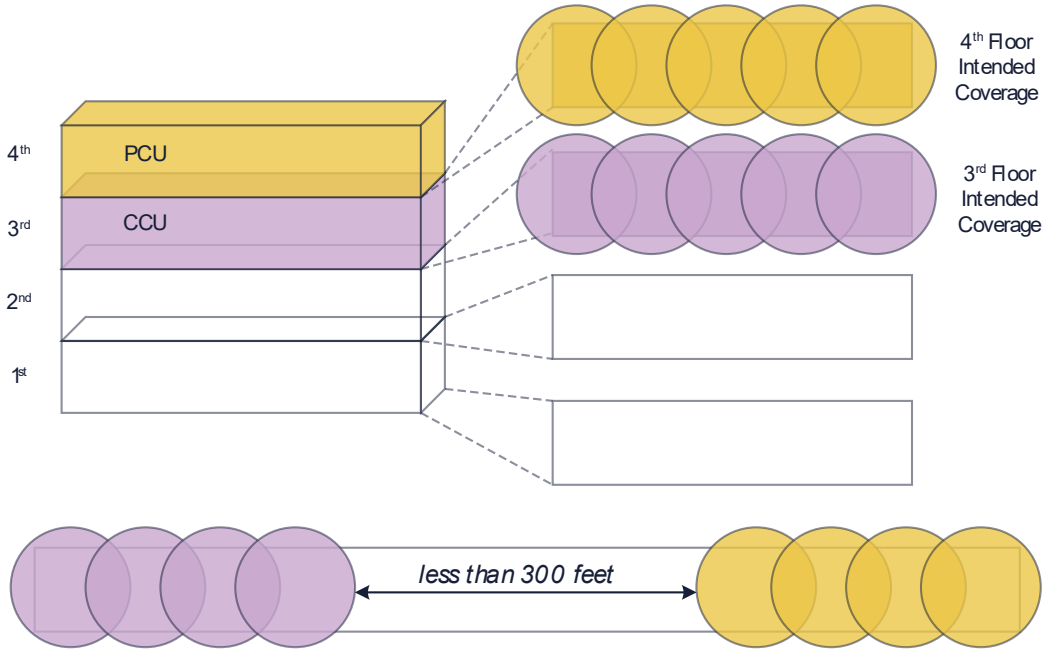


Figure 64: Common Sync Network Required

- The Smart-hopping systems do not have to be synchronized to each other if they are not on adjacent floors, or if the linear distance between system access points on the same floor is greater than 300 feet.

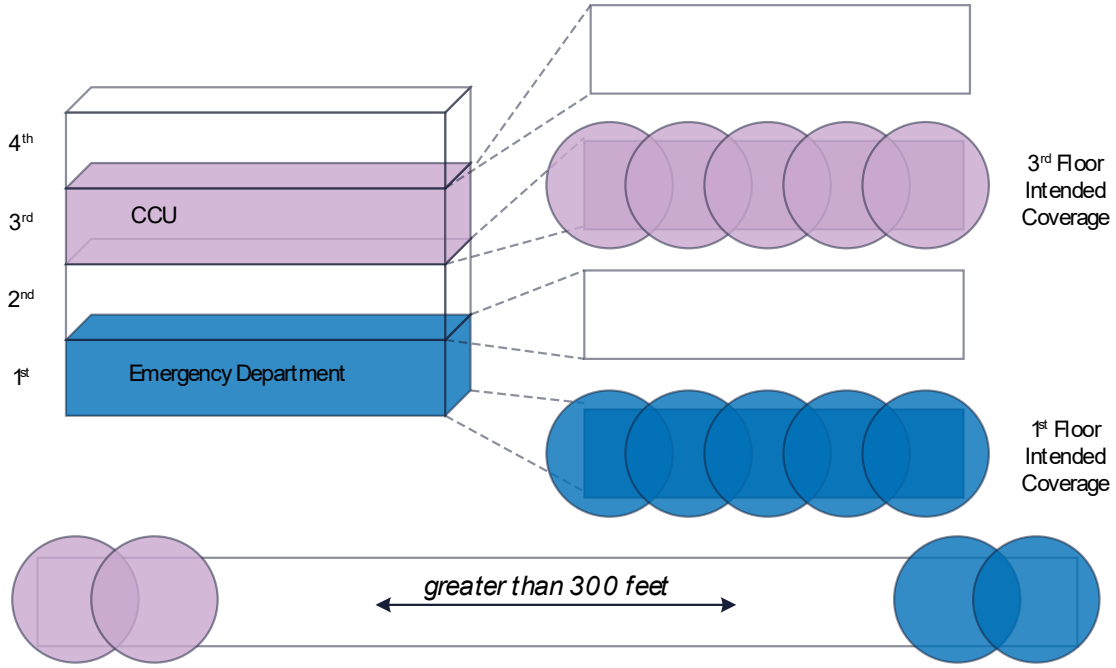


Figure 65: Common Sync Network Not Required

Consider an example (Figure 67) where a hospital wants three different Smart-hopping systems to provide wireless coverage to three units located on different floors.

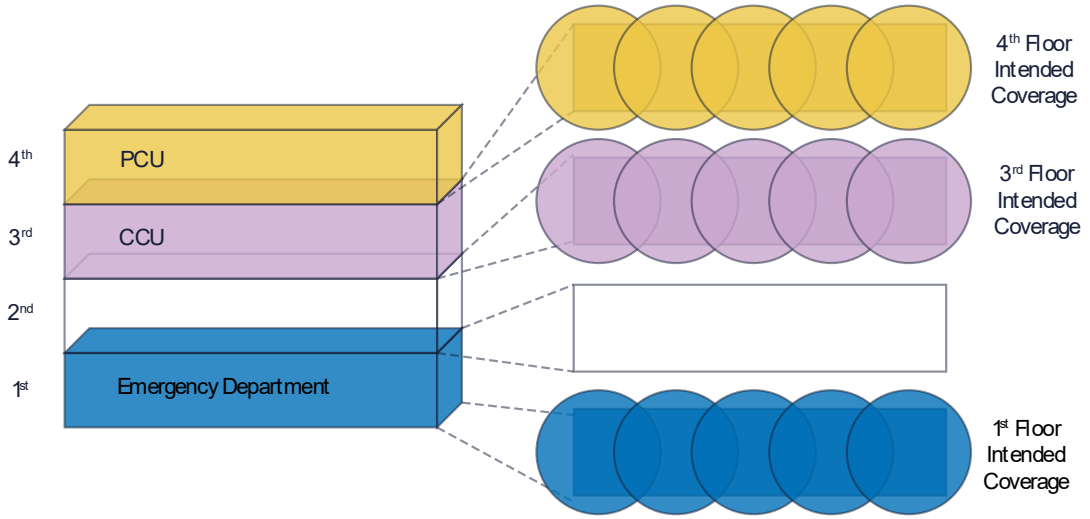


Figure 66: Sample Multiple Smart-hopping system Coverage Requirements

In this example, because the PCU and CCU are on adjacent floors, but the Emergency Department (ED) is further away, the Smart-hopping systems in the PCU and CCU must be synchronized to each other, but the ED system does not need to be synchronized to them.

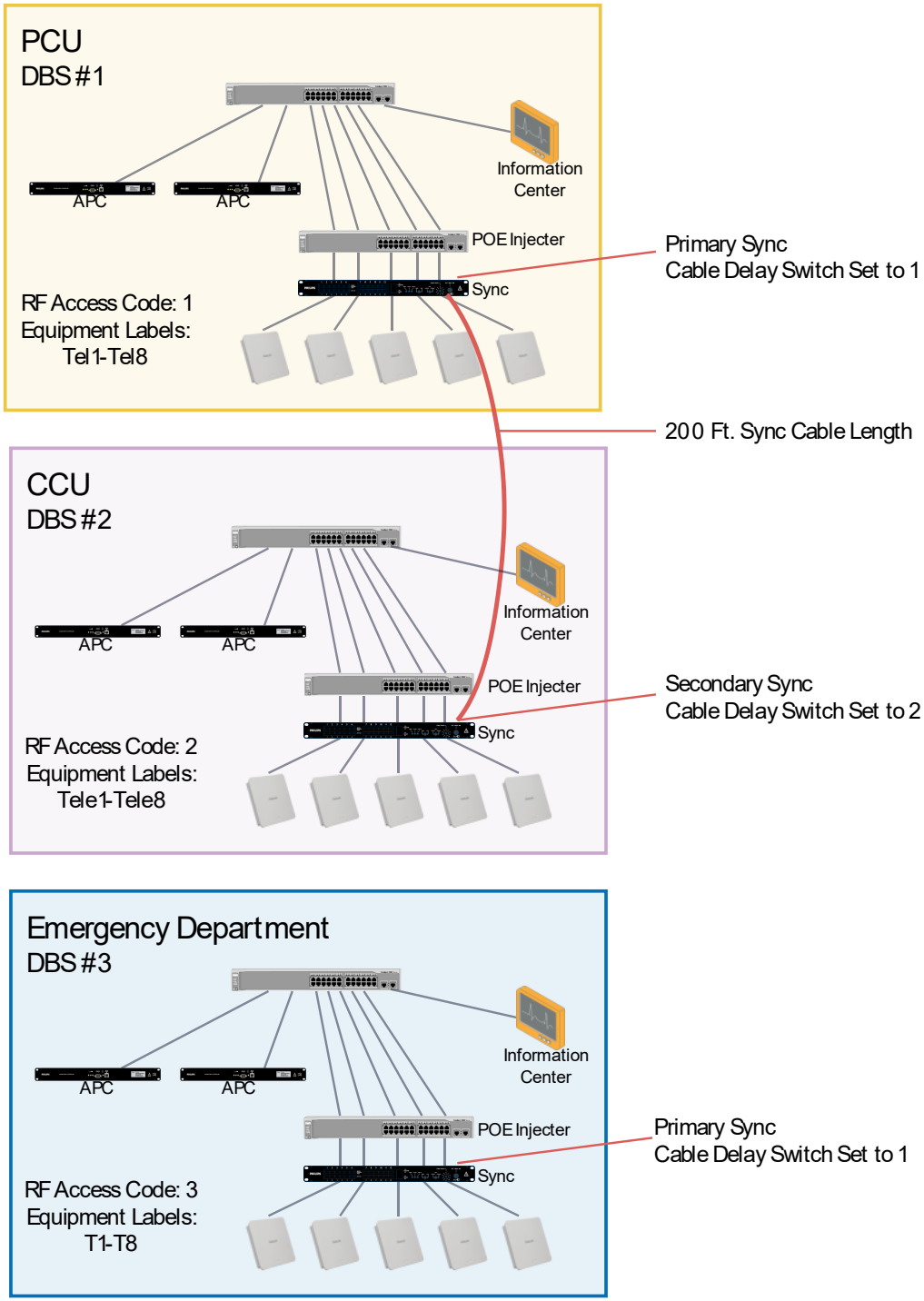


Figure 67: Sample Multiple Smart-hopping system Sync Network and Equipment Label Requirements

Note All three Smart-hopping systems must have different RF Access Codes configured and unique Equipment Labels assigned.

9 Appendix B: Routed topology configuration information

This appendix provides important information to help you configure a routed ring Smart-hopping infrastructure topology including:

- IntelliVue Network and Smart-hopping Infrastructure Subnet Device IP Addresses
- Sample Routed Topology

9.1 IntelliVue Network and Smart-hopping infrastructure subnet device IP addresses

Device Types (with Routed Subnet)	IntelliVue Network Subnet IPs Mask: 255.255.248.0	Default Gateway	Smart-hopping infrastructure Wireless Subnet IPs Mask: 255.255.240.0	Smart-hopping infrastructure Default Gateway
Network Subnet Address (Used in Config Wizard for Router)	172.31.n.0		172.31.240.0	
Gateway Address	172.31.n.1		172.31.240.1	
Router A – <used for Smart-hopping Wireless Subnet Router>	172.31.n.2		172.31.240.2	172.31.240.1
Router B – <used for Smart-hopping Wireless Subnet Router>	172.31.n.3		172.31.240.3	172.31.240.1
Reserved for Service PC	172.31.n.4 - 9	172.31.n.1	172.31.240.4-9	172.31.240.1
Network Switches and Remote Client Infrastructure	172.31.n.10 - 102	172.31.n.1	172.31.240.10 – 20	172.31.240.1
Reserved for Future Use	172.31.n.103 - 255		172.31.240.21 – 172.31.240. 255	
Smart-hopping APCs			172.31.241.0 – 127	172.31.240.1
IntelliVue 802.11 Devices	172.31.(n+1).0 - 63	172.31.n.1		
IntelliVue 802.11 Devices and legacy Proxim (RangeLAN2/Harmony) APs. Note: Proxim devices are not supported on PIC Release J (or higher).	172.31.(n+1).64 - 127	172.31.n.1		
Reserved for Future Use	172.31.(n+1).128 - 255		172.31.241.128 - 255	
Smart-hopping AP Static Range (1.4/2.4 GHz)			172.31.242.0 – 172.31.244.127	
Smart-hopping APC Bootp/DHCP Server Range 2 for 1.4/2.4 GHz APs			172.31.244.128 - 172.31.246.255	172.31.240.1
Database Server (NIC 1)	172.31.(n+3).0 - 15	Default blank		
Application Server (NIC 1)	172.31.(n+3).16 - 31	172.31.n.1		
Information Centers (NIC 1)	172.31.(n+3).32 - 63	172.31.n.1		
Information Center Clients	172.31.(n+3).64 - 95	172.31.n.1		
Printers (Set by BootP)	172.31.(n+3). 96 - 127			
Reserved	172.31.(n+3).128 - 255		172.31.247.0 - 255	
Bedside Monitors/Devices (Wired & ISM 2.4GHz) (Set By BootP)	172.31.(n+4).0 - 255			

Reserved for Future Use	172.31.(n+5).0 - 255			
Smart-hopping APC Bootp/DHCP Server Range 1 for Patient Monitors			172.31.248.0 – 172.31.253.255	172.31.240.1
Reserved for Future Use	172.31.(n+7).0 - 254		172.31.254.0 – 172.31.255.254	
Network Broadcast Address	172.31.(n+7).255		172.31.255.255	

Table 76: Routed IntelliVue Network Subnet and Smart-hopping infrastructure wireless subnet device IP addresses

Refer to table 77 for a list of the device IP address assignments used in a routed IntelliVue Network configuration where the Smart-hopping infrastructure is installed as a separate subnet to which up to 22 subnets have access via routers.

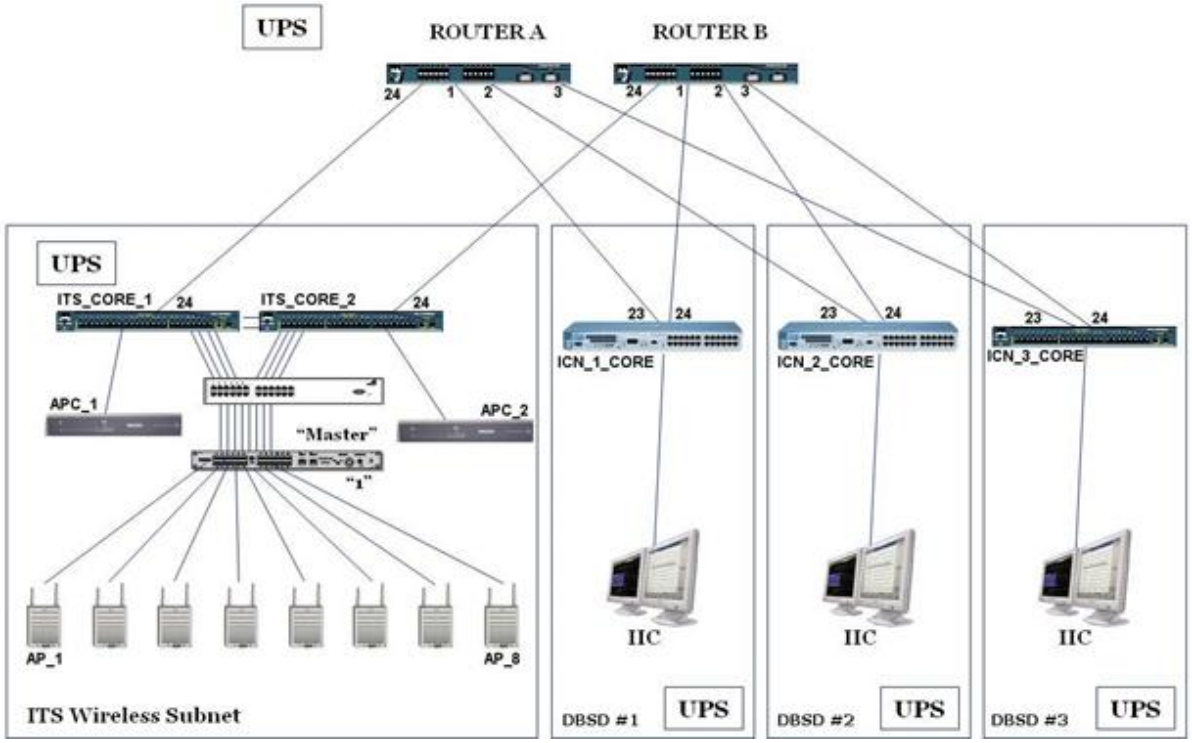
Note the following regarding table 77:

- "n" represents the network number and starts at 0 for single IntelliVue Network subnets. This variable increments by 8 from there for additional IntelliVue Network subnet. For example, for subnet 2, "n" equals 8, for subnet 3, "n" equals 16, and so on.

- Route statements are generated (in instances with a Router and without) at the completion of the Config Wizard.

9.2 Sample routed topology

Figure 69 shows a sample routed ring topology.



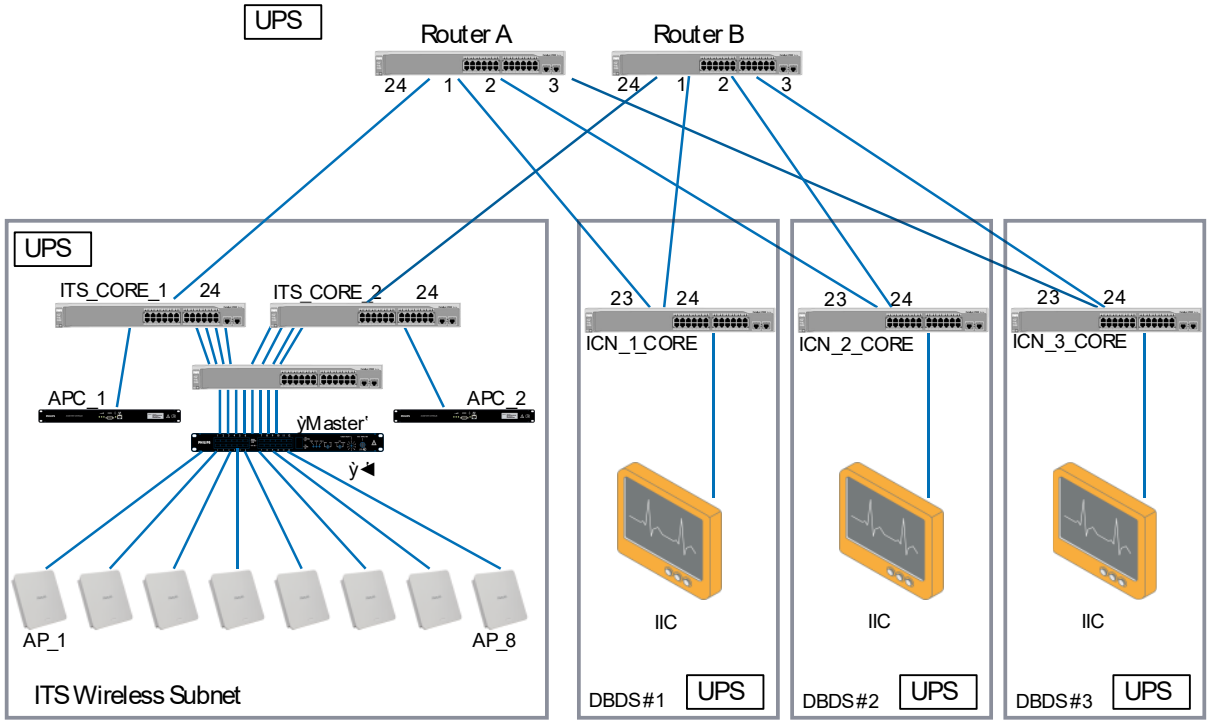


Figure 68: Sample Routed Smart-hopping infrastructure Topology

In a routed ring IntelliVue Network configuration, the Smart-hopping infrastructure is installed as a separate subnet to which multiple IntelliVue Network deployments have access using routers. Note the following general guidelines for installing the Smart-hopping infrastructure within a routed IntelliVue Network topology:

- An Smart-hopping infrastructure subnet can be connected up to 22 IntelliVue Network subnets using routers.
- Up to 600 Smart-hopping Access Points may be installed on a routed IntelliVue Network topology.
- The 1.4 GHz Smart-hopping infrastructure or 2.4 GHz Smart-hopping infrastructure may be installed within a routed IntelliVue Network topology.

Note the following possible port connections and device IP address assignments for this sample topology shown in Figure 63:

Smart-hopping infrastructure Wireless Subnet

- The Smart-hopping infrastructure devices reside on the Smart-hopping infrastructure wireless subnet which has a subnet address of 172.31.240.0.
- Router A is configured with an IP address of 172.31.240.2.
- Router B is configured with an IP address of 172.31.240.3.
- ITS_CORE_1 is configured with an IP address of 172.31.240.10 and connects to port 24 on Router A from port 24.
- ITS_CORE_2 is configured with an IP address of 172.31.240.11 and connects to port 24 on Router B from port 24.
- ITS_CORE_1 and ITS_CORE_2 have redundant connections to each other using their uplink ports.
- APC_1 is configured with an IP address of 172.31.241.0.

- APC_2 is configured with an IP address of 172.31.241.1.

Since there is only one Sync Unit on the Smart-hopping infrastructure, it is considered to be the Primary Sync Unit and its front-panel Cable Delay Switch is set to 1.

There are eight 1.4 GHz Access Points on the Smart-hopping infrastructure. They are named AP_1 to AP_8. The Access Points are assigned IP addresses ranging from 172.31.242.0 (AP_1) to 172.31.242.7 (AP_8).

SUBNET 1
IntelliVue Network_1_CORE is configured with an IP address of 172.31.0.10 and connects to Port 1 on Router A from Port 23 and to Port 1 on Router B from Port 24. The standalone PIC on IntelliVue Network subnet 1 is configured with an IP address of 172.3.1.3.32.

SUBNET 2
IntelliVue Network_2_CORE is configured with an IP address of 172.31.8.10 and connects to Port 2 on Router A from Port 23 and to Port 2 on Router B from Port 24. The standalone PIC on IntelliVue Network subnet 2 is configured with an IP address of 172.3.1.11.32.

SUBNET 3
IntelliVue Network_3_CORE is configured with an IP address of 172.31.16.10 and connects to Port 3 on Router A from Port 23 and to Port 3 on Router B from Port 24. The standalone PIC on IntelliVue Network subnet 3 is configured with an IP address of 172.3.1.19.32.

10 Appendix C: Upgrade Tool warning and error messages

This appendix describes the warning and error messages generated by the Philips Upgrade Tool and includes:

- Overview
- Configuration Synchronization
- Configuration Errors After Synchronization
- Message Descriptions

Additional troubleshooting information is available in “Troubleshooting System Issues” on page 132.

10.1 Overview

The Upgrade Tool will upload the APC system configuration and check that it conforms to the system requirements and installation rules, and verify that the Secondary APC configuration matches the Primary APC configuration.

Configuration update is done by normal APC update processing, so the APC does not need to be rebooted, and data flow is not interrupted, while configuration update is performed.

If an installation rule is broken, a Warning Message is generated and written to the summary report. If a system requirement is broken, an Error Message is generated and written to the summary report, and the upgrade is aborted. If the Primary and Secondary configuration are mismatched, the Upgrade Tool attempts to force the Secondary APC to upload a copy of the Primary APC configuration.

You should take the appropriate response to a warning or error message as follows:

- Warning Message - A warning allows you to continue with the APC upgrade.
  Issue: If the system is not configured properly, or if a Primary or Backup Primary APC has failed, service personnel are notified with this warning:

  ```
  WARNING: System installation requires APC Priority setting to be 0 for either
  all APCs or exactly 2x APC (Primary and 1x Backup APC)
  ```

  Solution: To properly use the backup primary feature, see “APC Roles” on page 137 for more information.

- Error Message - An error must be corrected before the upgrade can be completed. To correct an error, it may be necessary to take the APC down. Appropriate notification will be given under these circumstances.
  You can fix errors on the primary APC through the web interface or the APC serial console menu.
  Examples:

  ```
  *** ERROR: All APs do not have same WMTS channel configuration,
  00:09:FB:15:D7:67 has [1 2 3 4 ] enabled, 00:09:FB:25:40:81 has [1 2 3 4 5 6]
  enabled
  ```

  ```
  *** ERROR: RF Access Code: AP is 1, AP's Group is 92
  ```

- Errors on the secondary APC file can be corrected by running the Upgrade Tool using the Smart-hopping Only, Check and Update Configuration option. Errors in the Secondary APC configuration are corrected automatically when possible by forcing the Secondary APC to synchronize with the Primary APC. For example:

  ```
  *** ERROR: Tag in Secondary, not present in Primary: 0x1102 (Possible tag
  names: PROXIM_TAG_WCS_MANUAL_PART, PROXIM_TAG_FILTER_NETBEUI_ENABLE_TAG)
  length 1, value 1 (0x1)
  ```

The Upgrade Tool generates warning and error messages based on the presence of and content of a number of configuration files resident on the APC.

This section lists and describes the possible warning and error messages generated by the Upgrade Tool in the context of their associated configuration file.

Note If the Upgrade Tool displays an error message stating that a file is missing on a particular APC, then you can ignore any other warning or error messages related to that missing file on that APC.

This section lists and describes the possible warning and error messages generated by the Upgrade Tool in the context of their associated configuration file.

The following tables document APC configuration files and their associated warning and error messages. The following information is provided for each configuration file:

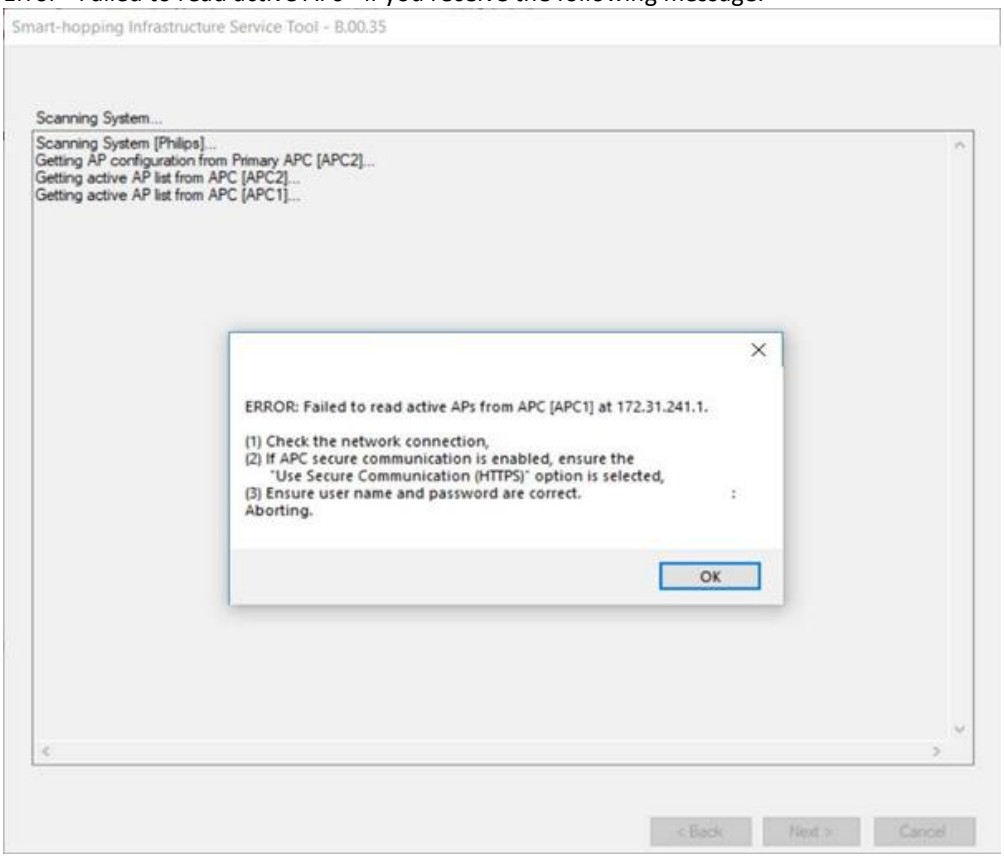
- file name
- file content
- whether the file is required to be present (some files are optional), and whether it will be checked if the Smart hopping-only option is selected
- what general rules are applied to both Primary and Secondary APCs for this file
- what rules are applied to the Primary APC only for this file
- what rules are applied to the Secondary APCs for this file
- whether a failure results in a warning or an error for each rule

The APC configuration rules are applied in the following order:

- Primary APC
    - File 1 general rules
    - File 1 master-specific rules
    - File 2 general rules
    - File 2 master-specific rules
    - [… etc., for each file, in the order given in the table below]
- Slave APC 1
    - File 1 general rules
    - File 1 slave-specific rules
    - File 2 general rules
    - File 2 slave-specific rules
    - [… etc., for each file, in the order given in the table below]
    - [… etc., for each slave APC]

10.1.1 Error messages

- Error - Failed to read active APs - if you receive the following message:



When you click OK, the Upgrade Tool fails and closes. This indicates there are potential network connection issues, user ID and password mismatches, or communication mode (HTTP or HTTPS) mismatches.

To resolve this issue, make sure your service PC is connected to the same subnet or VLAN as the APCs, make sure the Secure Communication via SSL menu option, user ID, and password are configured identically on all APCs in your Smart-hopping network. Once verified, restart the Upgrade tool.

- Upgrade Tool Error: When you have APCs running D.02 software and you add an APC running D.01 software, upgrading the new APC to D.02 software using the Upgrade Tool causes a synchronization error that displays in the Upgrade tool. This is due to changes in password storage and synchronization between versions D.01 and D.02 APC software. Philips recommends upgrading the APC to the D.02 software version running on the other APCs before installing it into the Smart-hopping network.

- Tag 0x1103 Error Message: During an upgrade or the APC configuration synchronization process, the APs are temporarily roamed away from their preferred APC partner, and then are roamed back. This activity results in configuration changes to Tag 0x1103. After 3 minutes, the APs renew their registration which ought to eliminate any mismatches associated with this tag.

- After the Upgrade Tool completes an upgrade or synchronization process, you must wait for at least three minutes for the APs to renew their registration. After waiting three minutes, run the Upgrade Tool with the following settings to confirm that all of the errors have been corrected:
    - APC – Do not upgrade
    - Only check configuration
    - AP – Do not upgrade

10.2 Configuration synchronization

If the Upgrade Tool displays error messages related to the configuration between the primary and secondary APC configuration files, do the following:

1. Run the Upgrade Tool with the following settings to correct the synchronization errors:
    a. APC – Do not upgrade
    b. Smart-hopping only, check and update configuration
    c. AP – Do not upgrade

2. After the Upgrade Tool completes the synchronization process, you must wait for at least three minutes for the APs and APCs to complete synchronizing. If you do not wait three minutes, the Upgrade Tool displays new Tag 0x1103 error messages. After waiting 3 minutes, run the Upgrade Tool with the following settings to confirm that all of the errors have been corrected:
    a. APC – Do not upgrade
    b. Only check configuration
    c. AP – Do not upgrade

10.3 Configuration errors after synchronization

If the Upgrade Tool displays error messages related to the configuration between the primary and secondary APC configuration files, do the following:

1. Run the Upgrade Tool with the following settings to correct the synchronization errors:
    a. APC – Do not upgrade
    b. Smart-hopping only, check and update configuration
    c. AP – Do not upgrade

2. Once this completes, wait three minutes and run the Upgrade Tool again, with the following settings, to confirm the errors are corrected:
    a. APC – Do not upgrade
    b. Only check configuration
    c. AP – Do not upgrade

3. If configuration errors still exist, do the following:
    a. Remove the APC that does not synchronize from the network (disconnect the RJ-45 cable connecting the APC to the switch or router).
    b. Using the serial port console menu, select the Reset APC to Factory Defaults option. This causes the APC to restart.
    c. Follow the instructions located in “Replacing an Smart-hopping APC” on page 122.

10.4 Message description

Item/Rule	Description
Comments	• APC specific information such as MAC address and IP address settings. • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • To fix errors or warnings in this file, use the APC serial menu to correct the settings.
General Rules	• Check that the file itself is not corrupt (correct length, all fields given below are present). Error: APC boot file length is incorrect Error: [Data item] not found in boot file • Check that last 3 bytes of MAC address are non-zero. Warning: APC MAC address is default • Check that the MAC address is either Philips (00:09:FB:xx:xx:xx) Error: MAC address is corrupt • Check that the APC has a static IP address. Warning: DHCP flag set • Check that the static IP address is not class D or E. Error: Class D/E IP addresses are illegal • Check that the subnet mask is non-zero. Error: Subnet mask must not be zero • Check that the default gateway is either zero or on the same subnet as the APC. Error: Gateway and IP address are on different subnets
Primary APC	No checks
Secondary APC	Check that the secondary APC is on the same subnet as the primary APC. Error: Secondary and primary are not on same subnet

Table 77: BOOTROM.NVP warnings and errors

Item/Rule	Description
Comments	• User and password info for logging in to the APC web interface. • This file must be present. This file will be checked if the Smart Hopping only option is selected.
General Rules	No checks.
Primary-specific	No checks.
Slave-specific	• The file must contain the same set of TLVs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…]

Table 78: PASSWORD.TLV warnings and errors

Item/Rule	Description
Comments	• System specific information. • This file must be present. • This file is checked if you select the Smart Hopping only option. • Errors on the secondary file can be corrected by running the Upgrade Tool (using the Smart-hopping Only, Check and Update Configuration option). Errors on the primary can be fixed through the web interface, on the System config screens (“BOOTP/DHCP” and “SUBNET TABLE” tabs). System type on the APC can be configured through the APC serial menu.

General Rules	No checks.
Primary APC	• Check that the System Type (1.4 GHz or 2.4 GHz) stored in the APC matches the selection made on the Upgrade Tool UI. Error: System type on APC is [type], tool has been configured to verify a [type] system • Check that the DHCP configuration matches the default. Warning: Non-default System DHCP Table configuration • Check that the subnet table configuration matches the default. Warning: Non-default subnet table configuration • Check that any ranges in the DHCP configuration that would match AP MAC addresses would not allow two APs to have duplicate ten low bits of IP address. Error: Range n in DHCP table is invalid: duplicate FMIDs could result. Low ten bits of AP IP addresses must be guaranteed unique
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though); except the APC name TLV. Error: Secondary and primary files have differing contents [details…]

Table 79: PARAM/SYSTEM.TLV warnings and errors

Item/Rule	Description
Comments	• Filter configuration information. • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • Errors on the Secondary file can be corrected automatically; errors on the Primary can be fixed through the web interface, on the System config screens (“FILTERS” tab).
General Rules	No checks.
Primary-specific	• Check that each filter setting matches the default. Warning: Non-default [filter] configuration
Slave-specific	• The file must contain the same set of TLVs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…]

Table 80: PARAM/FILTER.TLV warnings and errors

Item/Rule	Description
Comments	• Authorization details for specific Patient Monitors. • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • Errors on the secondary can be corrected automatically; errors on the primary can be fixed through the web interface System config screens (“AUTHORIZATION TABLE” tab).
General Rules	No checks.
Primary APC	• Check that the authorization table is unused and has no entries Error: Authorization table is in use.
Secondary APC	• The file must contain the same set of TLVs on the primary and the secondary (not necessarily in the same order, though) Error: Secondary and primary files have differing contents [details…]

Table 81: PARAM/AUTHTBL.TLV warnings and errors

Item/Rule	Description
Comments	• DHCP Server IP address assignment information. • This file may not be present if no DHCP assignments have been made. • This file will be checked if the Smart Hopping only option is selected. • Errors on the Secondary can be corrected automatically; errors on the Primary can be fixed through the web interface System config screens ("BOOTP/DHCP" tab, click to view allocations, "Purge allocations").
General Rules	No checks.
Primary-specific	• Check that the file header is correct. Error: Primary DHCP file header incorrect • Check that all entries have Philips or Proxim MAC addresses Warning: unrecognized MAC address in DHCP table • Check that all entries for AP MAC addresses have unique ten low bits of IP address (cross checked against manually configured APs in the WTMS.TLV file) Error: AP x:x:x:x:x:x and AP x:x:x:x:x:x have duplicate low ten bits of IP address
Slave-specific	• The file headers on the Primary and Secondary files must match. Error: DHCP File headers do not match • The file must contain the same set of DHCP entries on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…]

Table 82: CONFIG/DHCP.TLV warnings and errors

Item/Rule	Description
Comments	• Group configuration information for Smart Hopping AP groups • This file must be present. • This file will be checked if the Smart Hopping only option is selected. • Errors on the Secondary file can be corrected automatically; errors on the Primary can be fixed through the web interface, Group config screens.
General Rules	No checks.
Primary-specific	• APs have default group basic configuration. Warning: APs have non-default group basic [specific item] configuration • APs have default group alert configuration. Warning: APs have non-default group alert [specific item] configuration • APs have default group radio configuration. Warning: APs have non-default group radio [specific item] configuration • APs have default advanced group configuration. Warning: APs have non-default advanced [specific item] group configuration. • Group configuration has default check boxes checked for enabling items on configuration screen. Warning: Non-default configuration: [specific item] on [specific group config screen], enable check box should be [set/unset]

Slave-specific	• The file must contain the same set of Groups on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…] • Each Group must contain the same set of Group TLVs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have different group configurations [details…] • Each Group must contain the same set of AP TLVs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have different AP configurations [details…]

Table 83: CONFIG/TABLE/GRPSWMTS.TLV warnings and errors

Item/Rule	Description
Comments	• AP configuration information for Smart Hopping APs • This file may not be present if no Smart Hopping APs are configured on the system. • This file will be checked if the Smart Hopping only option is selected. • Errors on the Secondary file can be corrected automatically; errors on the Primary can be fixed through the web interface, individual AP configuration screens.
General Rules	No checks.
Primary-specific	• All APs on same subnet. Error: APs are not all on same subnet • All entries for AP MAC addresses have unique ten low bits of IP address (cross checked against manually configured APs in the DHCP.TLV file). Error: AP x:x:x:x:x:x and AP x:x:x:x:x:x have duplicate low ten bits of IP address • WMTS systems only: All APs have same WMTS channel configuration. Error: APs do not all have same WMTS channel configuration • ROW Z.nn.nn systems only: All APs have same ISM area configuration. Error: APs do not all have same ISM area configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Radio Regulation Code configuration. Error: APs do not all have same ISM Radio Regulation Code configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Frequency Plan configuration. Error: APs do not all have same ISM Frequency Plan configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Zigbee Channel configuration. Error: APs do not all have same ISM Zigbee Channel configuration • ROW B.00.03 and onwards systems only: All APs have same ISM Advanced Channel configuration Error: APs do not all have same ISM Advanced Channel configuration • APs have been set up with a preferred partner. Warning: APs have been configured with no preferred partner • APs are not disabled. Warning: AP has been disabled • APs have default RF Access code configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart Hopping Group settings (warning), and AP's own group settings (error). Warning/Error: RF Access Code enable: AP is [set/unset], [AP Default/ Default Smart Hopping Group/AP's Group] is [unset/set] APs have default WMTS Channels configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart Hopping Group settings

	(warning), and AP's own group settings (error). Warning/Error: WMTS Channels: AP has [channels] enabled, [AP Default/ Default Smart Hopping Group/AP's Group] has [channels] enabled • ROW Z.nn.nn systems only: APs have default ISM area code configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart Hopping Group settings (warning), and AP's own group settings (error) Warning/Error: ISM area code: AP is [area], [AP Default/Default Smart Hopping Group/AP Group] is [area] • ROW B.00.03 and onwards systems only: APs have default ISM Radio Regulation Code configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart Hopping Group settings (warning), and AP's own group settings (error). Warning/Error: ISM Radio Regulation Code: AP has [code], [AP Default/Default Smart Hopping Group/AP's Group] has [code] • ROW B.00.03 and onwards systems only: APs have default ISM Advanced Channels configuration - cross-check each entry in AP file against AP template defaults (warning), default Smart Hopping Group settings (warning), and AP's own group settings (error). Warning/Error: ISM Advanced Channels: AP has [channels] enabled, [AP Default/Default Smart Hopping Group/AP's Group] has [channels] enabled
Slave-specific	• The file must contain the same set of APs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…] • Each AP must contain the same set of TLVs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…]

Table 84: CONFIG/TABLE/WMTS.TLV warnings and errors

Item/Rule	Description
Comments	• Default AP configuration for Smart Hopping APs • This file may not be present if no changes have been made to the default template settings. • This file will be checked if the Smart Hopping only option is selected. • Errors on the Secondary can be fixed automatically; errors on the Primary can be fixed through the web interface, Access Point Default settings.
General Rules	No checks.
Primary-specific	• APs have default basic configuration. Warning: APs have non-default basic [specific item] configuration • APs have default alert configuration. Warning: APs have non-default alert [specific item] configuration • APs have default radio configuration. Warning: APs have non-default radio [specific item] configuration
Slave-specific	• The file must contain the same set of TLVs on the Primary and the Secondary (not necessarily in the same order, though). Error: Secondary and Primary files have differing contents [details…]

Table 85: CONFIG/TEMPLATE/WMTS.TLV warnings and errors

11 Appendix D: Using the APC serial console

This appendix describes how to configure the menu options contained in the APC serial port console:

11.1 Using the APC serial menu console

11.1.1 Connecting to the APC serial port menu

To configure your terminal client (using the serial port on the APC) to connect to the APC, use the following settings:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

Caution The default APC serial console password is a strong password. If you change the password and do not have the new password, Philips cannot recover the APC. You must then replace the APC, either by purchasing a new APC or replacing it with a spare APC.

11.1.2 Access Point Controller serial port menu

Highlights of the APC serial port menu. Use the APC serial port menu to configure the APC for your environment.

```
Philips AP Controller                    Main                                    D.02.23
Built date: Oct 23 2020 14:15:17.

Selection   Description                              Current Value
---------   -----------                              -------------
1           Static TCP/IP and APC Priority Settings
2           Enable 1.4/2.4GHz Smart Hopping
3           Advanced Configuration
4           APC Error Logging
5           CLIENT CI MULTICAST Spoof                disabled
6           APC MULTICAST Layer 3                    disabled
7           APC Client Gratuitous ARP                disabled
8           This APC for Primary Contention          enabled
9           Security and Advanced Parameters         disabled
10          Check APC network interface periodically disabled
11          BACKUP this APC config files
12          RESTORE this APC config files
13          Reset Configuration to Factory Defaults
14          Reset Access Point Controller
15          Snapshot PRIMARY APC current running config
16          SAFE Reset PRIMARY Access Point Controller

Enter a selection number ->
```

Figure 69: APC Serial Port Menu

Click the links in this section for more information on each of the APC serial port menu options:

Check the APC firmware version displayed on the APC serial interface Main Menu and verify that the APC is running firmware which is compatible with all components of the system. If the APC is not running a compatible version of the firmware, use the Upgrade Tool to update the APCs with the latest version of the firmware.

11.1.3 Serial port menu options

Smart-hopping APCs running version D.02 software display the following items on the main console menu:

Note When you enable the Security and Advanced Parameters menu option, three additional items appear on the console menu— Secure Communication Via SSL, Engineering Support Parameters, and Reset Webserver Password to factory default.

Option Number	Option (Security and Advanced Parameters Enabled)	Option (Security and Advanced Parameters Disabled)
1	Static TCP/IP and APC Priority Settings	Static TCP/IP and APC Priority Settings
2	Enable 1.4/2.4 GHz Smart-hopping	Enable 1.4/2.4 GHz Smart-hopping
3	Advanced Configuration	Advanced Configuration
4	APC Error Logging	APC Error Logging
5	Client CI MULTICAST Spoof	Client CI MULTICAST Spoof
6	APC Multicast Layer 3	APC Multicast Layer 3
7	APC Client Gratuitous ARP	APC Client Gratuitous ARP
8	This APC for Primary Contention	This APC for Primary Contention
9	Security and Advanced Parameters	Security and Advanced Parameters
10	Secure Communication Via SSL	Check APC Network Interface Periodically
11	Engineering Support Parameters	Backup this APC Config Files

12	Check APC Network Interface Periodically	Restore this APC Config Files
13	Backup this APC Config Files	Reset Configuration to Factory Defaults
14	Restore this APC Config Files	Reset Access Point Controller
15	Reset Configuration to Factory Defaults	Snapshot Primary APC Running Config
16	Reset Access Point Controller	Safe Reset Primary Access Point Controller
17	Snapshot Primary APC Running Config	
18	Safe Reset Primary Access Point Controller	
19	Reset Webserver Password to factory default	

Table 86: Console main menu options

11.1.4 Static TCP/IP and APC priority settings

How to configure APC IP address information, Multicast connection information, and a backup APC priority.

```
Philips AP Controller Static TCP/IP and APC Priority Settings              D.01.02

Selection   Description                              Current Value
---------   -----------                              -------------
1           Static IP Address                        172.20.121.0
2           Static Subnet Mask                       255.255.248.0
3           Static Default Gateway Address           172.20.120.1
4           Client Current CI Multicast Address      224.0.23.63
5           Client New CI Multicast Address          224.0.23.173
6           Master APC Multicast Address             239.255.254.1
7           Slave APC Multicast Address              239.255.254.2
8           Backup APC Priority Level(0,1,2; default=0=highest)  0
9           Network Logging IP Address               0.0.0.0

Enter a selection number or <ESC> for previous menu ->
```

Figure 70: Static TCP/IP and APC Priority Settings

The menu options allow you to set IP address information (IP address, subnet mask, default gateway) for this APC, Multicast connection information, backup APC priority. To change any of the menu items, select the option number and enter the updated information.

Enter the number of the menu option you wish to change. To commit changes, press Enter. To return to the menu without changing any settings, press Esc.

1. Static IP Address — Sets the IP address of this APC. Enter the IP address in octet form (for example — 172.31.241.1)
2. Static Subnet Mask — Sets the subnet of this APC. Enter the IP address in octet form (for example — 255.255.240.0). The subnet mask determines the number of devices in a subnet (for example, 255.255.240.0 [also known as /20 CIDR] allows for 4096 hosts in a subnet.).
3. Static Default Gateway Address — Sets the default gateway of this APC. Enter the IP address in octet form (for example — 172.31.240.1)
4. Client Current CI Multicast Address — Sets the IP address of the CI (Connect Indication) service (located on a Surveillance iX system in the Multicast zone) to which the Smart-hopping wireless clients currently connect. Keep the default IP address (224.0.23.63).
5. Client New CI Multicast Address — Sets the IP address of a new CI (Connect Indication) service to which this APC connects. Keep the default IP address (224.0.23.173).
6. Primary APC Multicast Address — Configures the APC to recognize the Multicast IP address of the primary APC. Enter the IP address in octet form (for example — 239.255.254.1)

7. Secondary APC Multicast Address — Configures the APC to recognize the Multicast IP address of the secondary APC. Enter the IP address in octet form (for example — 239.255.254.2)
8. Backup APC Priority Level (0 or 2; the default is 0 [highest]) — This entry allows you to set if this APC becomes the next Primary APC if the original Primary APC is disabled or stops working. If you set this option to 0, this APC is the highest priority backup APC. The higher the number (0– 2), the lower this APC becomes in the backup APC hierarchy.

Note The Backup Primary APC feature is only available in systems with 3 or more APCs.If all of the APCs in a system are set to a priority level of 0 (factory default), the Backup Primary APC feature is disabled. The system operates like a D.01 or C.00 system.

11.1.5 Enable 1.4/2.4 GHz Smart-hopping

This topic contains information on setting the System Name and type of Smart-hopping (1.4 GHz or 2.4 GHz).

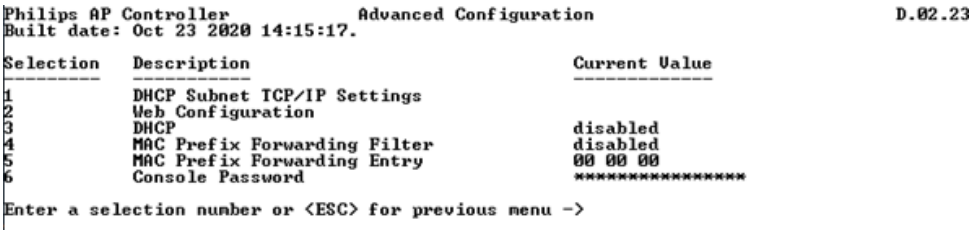


Figure 71: Enable 1.4/2.4 GHz Smart-hopping Menu

This menu option allows you to change the system name and select which type of Smart-hopping you want to use (1.4 or 2.4 GHz). Select the option and either manually enter the data or select your choice from the list.

1. System Name — Leave the system name at the default (Philips).
2. System Type — When the list appears, enter 1 for 1.4 GHz Smart-hopping or 2 for 2.4 GHz Smart-hopping. The change automatically saves.
3. Press Esc to exit without saving an option change or to return to the main menu.

11.1.6 Advanced configuration

Warning Do not change any settings in Advanced Configuration unless directed to do so by Philips support.

Configure advanced APC settings, such as: web configuration and console password.

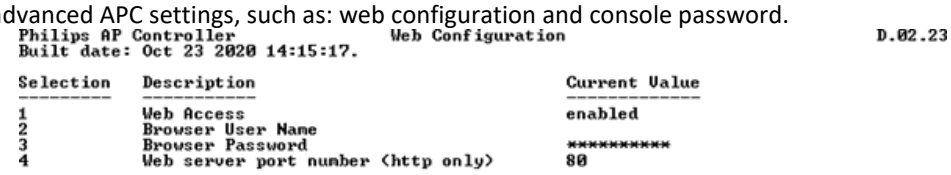


Figure 72: Advanced Configuration Menu

This menu option allows you to change the DHCP subnet TCP/IP settings, configure web access, enable/disable DHCP, change the console password, and edit MAC prefix forwarding information. Select the option and either manually enter the data or select your choice from the list. Press Enter to commit changes or press Esc to exit without saving an option change or to return to the main menu.

1. DHCP Subnet TCP/IP Settings — When you select this option, another menu appears. You configure options 1-5 using the web interface.

2. Web Configuration — A web server configuration menu appears.

```
Philips AP Controller                Web Configuration                    D.02.23
Built date: Oct 23 2020 14:15:17.

Selection    Description                                  Current Value
---------    -----------                                  -------------
1            Web Access                                   enabled
2            Browser User Name
3            Browser Password                             **********
4            Web server port number (http only)           80

Enter a selection number or <ESC> for previous menu ->
```

a. Leave option 1 enabled (default).
b. Enter 2 to change the Browser User Name. When prompted, enter a user name (for example, PhilipsBD).
c. Enter 3 to change the Browser Password. When prompted, enter a password.
d. Leave option 4 at the default (port 80).

Note This option only applies when connecting to the APC web interface over traditional HTTP (not HTTPS).

3. Console Password — Allows you to set or change the password the APC uses for serial port connections.
   Press Esc to exit without saving an option change or to return to the main menu.

11.1.7 APC error logging

```
Philips AP Controller                APC Error Logging                    D.02.23
Built date: Oct 23 2020 14:15:17.

Selection    Description                                  Current Value
---------    -----------                                  -------------
1            Serial based logging                         disabled
2            Network based logging                        disabled
3            Flash based Error logging                    enabled
4            Display Flash based Error logs

Enter a selection number or <ESC> for previous menu ->
```

How to enable or disable system logging to the serial port, over the LAN, or to the system flash. The APC Error Logging menu option allows you to send APC error logs to any or all of the following:

- Serial based logging - A console attached to the APC serial port
- Network based logging - This is unsupported. Do not enable this option.
- Flash based Error logging - The system flash memory (enabled by default)
- Display Flash based Error logs - Displays any system errors

To enable or disable an option, do the following:

1. Select the item from the menu.
2. Enter the option number to either enable or disable this option.
3. Press Esc to exit the menu without changing the setting or after changing the setting to commit changes.

11.1.8 Client CI MULTICAST spoof

How to configure which Multicast address to select for the CI Multicast message.
The CI Multicast Spoof menu option supports selecting which Multicast address to use for the CI (Connection Indication) Multicast message. When disabled (default), the client CI uses the IP address 224.0.23.63. When enabled, the client CI uses the IP address 244.0.23.173. To enable or disable this option, do the following:

1. Select the CI Multicast Spoof from the APC serial port menu.
2. Enter the option number to either enable or disable this feature.
3. Press Esc to exit the menu without changing the setting or after changing the setting to commit changes.

11.1.9 APC multicast layer 3

How to enable or disable Multicast data transmission over a Layer 3 network.
In a Layer 3 Smart-hopping deployment, critical communication messages are sent via Multicast. To change to this type of implementation, you must enable the APC MULTICAST Layer 3. The Multicast addresses used for communication between the Smart-hopping infrastructure devices are configured using the "Static TCP/IP and APC Priority Settings" on page 172 menu option.

To enable or disable the APC Multicast Layer 3 feature, do the following:

1. Select the APC Multicast Layer 3 from the APC serial port menu.
2. Enter the option number to either enable or disable this feature. This feature is disabled by default.
3. Press Esc to exit the menu without changing the setting or after changing the setting to commit changes.

11.1.10 APC client gratuitous ARP

How to enable or disable transmission of gratuitous ARP messages from the APC to client devices.

Some networks are sensitive to excessive ARP messages, which can impact switches and create network problems. The APC provides a configuration option to disable the Gratuitous ARP messages that APC creates for client devices. The default is disabled, which does not send the gratuitous ARP messages.

This menu option allows you to enable or disable the gratuitous ARP messages sent by the APC (the default setting is disabled). Select the option from the list that appears and press Enter to commit changes.

1. When the Enable/Disable option appears, enter 1 to enable Gratuitous ARP and enter 2 to disable Gratuitous ARP. The change automatically saves.
2. Press Esc to exit without saving an option change or to return to the main menu.

11.1.11 This APC for primary contention

How to configure the APC to contend for primary APC status.

When disabled, the APC does not take on mastership and prevents an APC added to the system from taking control. Set to enable for normal operation.

This menu option allows you to enable or disable this APC from primary APC contention. This option is enabled by default. Select the option from the list that appears and press Enter to commit changes.

1. When the Enable/Disable option appears, enter 1 to enable the This APC for Primary Contention and enter 2 to disable This APC for Primary Contention. The change automatically saves.
2. Press Esc to exit without saving an option change or to return to the main menu.

11.1.12 Security and advanced parameters

How to enable security and advanced parameters on the APC.

This menu option allows you to enable or disable security and advanced parameters for HTTP or HTTPS communication to the APC using a web browser. Select the option from the list that appears and press Enter to commit changes.

1. When the Enable/Disable option appears, enter 1 to enable the Security and Advanced Parameters and enter 2 to disable Security and Advanced Parameters. The change automatically saves.
2. Press Esc to exit without saving an option change or to return to the main menu.

11.1.12.1 New menu items

```
Philips AP Controller                    Main                                D.02.23
Built date: Oct 23 2020 14:15:17.

Selection   Description                                 Current Value
---------   -----------                                 -------------
1           Static TCP/IP and APC Priority Settings
2           Enable 1.4/2.4GHz Smart Hopping
3           Advanced Configuration
4           APC Error Logging
5           CLIENT CI MULTICAST Spoof                   disabled
6           APC MULTICAST Layer 3                       disabled
7           APC Client Gratuitous ARP                   disabled
8           This APC for Primary Contention             enabled
9           Security and Advanced Parameters            disabled
10          Check APC network interface periodically    disabled
11          BACKUP this APC config files
12          RESTORE this APC config files
13          Reset Configuration to Factory Defaults
14          Reset Access Point Controller
15          Snapshot PRIMARY APC current running config
16          SAFE Reset PRIMARY Access Point Controller

Enter a selection number -> 9

Security and Advanced Parameters  [disabled]
        1. enabled
        2. disabled
Enter a selection number or <ESC> -> 1


Philips AP Controller                    Main                                D.02.23
Built date: Oct 23 2020 14:15:17.

Selection   Description                                 Current Value
---------   -----------                                 -------------
1           Static TCP/IP and APC Priority Settings
2           Enable 1.4/2.4GHz Smart Hopping
3           Advanced Configuration
4           APC Error Logging
5           CLIENT CI MULTICAST Spoof                   disabled
6           APC MULTICAST Layer 3                       disabled
7           APC Client Gratuitous ARP                   disabled
8           This APC for Primary Contention             enabled
9           Security and Advanced Parameters            enabled
10          Secure Communication Via SSL (default = disable)disabled
11          Engineering Support Parameters (default = disable)disabled
12          Check APC network interface periodically    disabled
13          BACKUP this APC config files
14          RESTORE this APC config files
15          Reset Configuration to Factory Defaults
16          Reset Access Point Controller
17          Snapshot PRIMARY APC current running config
18          SAFE Reset PRIMARY Access Point Controller
19          Reset Webserver Password to factory default

Enter a selection number ->
```

When you enable the Security and Advanced Parameters menu option, the main console displays three additional menu options. The additional menu options are:

Secure communication via SSL
Select this option to enable or disable SSL (Security Socket Layer) encryption between a web client and the APC when using a web browser to communicate with the APC. This option is disabled by default.

- When disabled, web communication with the APC uses HTTP.
- When enabled, web communication with the APC uses HTTPS.

For more information on installing an SSL certificate, see the SSL/TLS Certificate Installation Instructions in the Microsoft Windows online help.

Engineering Support Parameters
This option is disabled by default. Enable this option only when asked by Philips Support.

Reset Webserver Password to factory default
Select this option to reset the web browser user name and password.

11.1.13 Check APC network interface periodically

Configure whether the APC network interface periodically pings the default gateway.

This option allows you to enable or disable a periodic ICMP ping from the APC to its default gateway. If enabled and the APC does not receive a reply from the default gateway, it logs an error. To enable or disable this option, do the following:

1. Enter the number of the Check APC Network Periodically menu option to enable or disable this feature.
2. To commit changes, press Enter. To return to the menu without changing any settings, press Esc.

11.1.14 Backup this APC config files

The Backup this APC Config Files option stores a copy of the configuration files to the APC flash. At the completion of system configuration, run this function to save a backup up copy of the system configuration. You must perform this task on the Primary APC. To backup the APC configuration, select the Backup this APC Config Files menu option and enter the option number for yes. To return to the menu without backing up the configuration files, press the option for no or press Esc.

11.1.15 Restore this APC config files

The Restore this APC Config Files option replaces copies of the configuration files to the APC flash with previously backed up files. This is useful in the event of corruption of the running configuration file or in event a system recovery. You must perform this task on the Primary APC. To restore the APC configuration, select the Restore this APC Config Files menu option and enter the option number for yes. To return to the menu without restoring the configuration files, press the option for no or press Esc.

Restoring APC configuration files works with the following requirements:

- Recovery only functions if a valid backup configuration file exists on the Primary APC.
- The restore function must be run on the Primary APC.
- If no backup is stored, the restore has no effect and keeps the APC configuration unchanged.
- The restore takes effect only after the user resets the Access Point Controller.
- When a Configuration is restored on the Primary APC, the configuration is then propagated to all Secondary APCs if the APC configuration key is different, in order to make sure all APC configurations synchronize with the Primary APC. To ensure the primary APC has the highest configuration key, use the serial port console menu on all other APCs and select the Reset Configuration to Factory Defaults option and confirm the reset. This resets the configuration key on all other APCs.

11.1.16 Reset configuration to factory defaults

How to reset the APC to the factory settings. This preserves the latest version of installed software and removes some user- configured details.

To reset the APC configuration to its factory defaults (preserves the latest version of installed software, system name, and IP address details). do the following:

Warning When you reset an APC to factory defaults, wait two minutes until attempting to access the APC. The two minutes allows the configuration to save properly.

1. Select the option for Reset Configuration to Factory Defaults from the main menu and press Enter.
2. Enter 1 to confirm the reset; enter 2 or Esc to cancel the factory reset.
3. Once you confirm the factory reset, the APC restarts.

11.1.17 Reset access point controller

Resetting the APC is the equivalent of a power cycle restart. All configurations are preserved. To perform a simple restart of your primary APC without affecting the Smart-hopping network operation, select the Reset Primary Access Point Controller menu option and enter the option number for yes. To return to the menu without restarting, press the option for no or press Esc.

11.1.18 Snapshot primary APC running config

This feature preserves a copy of the current Primary APC running configuration. This feature helps avoid disruption when restarting the primary APC. It saves sufficient secondary APC info on the primary APC to prevent AP re- registration activities after restarting the primary APC.

To create a snapshot of the APC current running configuration, do the following:

1. Select the option from the main menu and press Enter.
2. Enter 1 to confirm the snapshot; enter 2 or Esc to cancel the snapshot.

11.1.19 Safe reset primary Access Point Controller

The Safe Reset of the APC copies the current running configuration (performs a Snapshot Primary APC Running Config) to other APCs to prevent any disruption to the network as the APC restarts. To perform a simple restart of your primary APC without affecting the Smart- hopping network operation, select the Safe Reset Primary Access Point Controller menu option and enter the option number for yes. To return to the menu without restarting, press the option for no or press Esc.

12 Appendix E: Smart-hopping network deployments: layer 2, layer 3, routed, and non-routed explained

This appendix explains how the terminology Layer 2, Layer 3, Non-Routed, and Routed are used in the context of the Smart-hopping infrastructure user interfaces and this documentation.

Layer 2 and Layer 3 in the Smart-hopping Infrastructure context - specifically when used in this documentation, the APC serial console user interface and Smart-hopping Infrastructure Service Tool (a.k.a. Philips AP and APC Upgrade Tool), refer to how the Smart-hopping infrastructure devices communicate with each other. It is not referencing how data gets from the Smart-hopping devices to the Information Center.

A Layer 2 Smart-hopping network deployment indicates that all Smart-hopping APCs, APs, and wireless clients all reside on the same VLAN or subnet (typically VLAN 124). Certain critical messages between the infrastructure devices are transmitted across the subnet as broadcast messages.

A Layer 3 Smart-hopping network deployment indicates that all the Smart-hopping APCs and wireless clients reside on the same VLAN or subnet, but the associated APs reside on different VLANs or subnets. In this type of system, the critical messages between the infrastructure devices are transmitted between the VLANs as multicast messages.

The terms non-routed and routed, in the Smart-hopping Infrastructure context (specifically when used in the BootP/ DHCP Server Configuration web view), refer to how data transmits from the Smart-hopping devices to the Information Center.
A non-routed Smart-hopping deployment is a clinical network where the APs, APCs, Smart-hopping Wireless Clients, and the Information Centers that monitor them are all on the same VLAN or subnet. Data from the Smart-hopping devices to the Information Center does not need to be routed since all of the devices are on the same subnet.

A routed Smart-hopping deployment is a clinical network where the Smart-hopping devices (APs, APCs, and Smart- hopping Wireless Clients) are not on the same VLAN or subnet as the Information Centers; therefore routing is required to get the data from the Smart-hopping devices to the Information Centers.

The illustrations in this section explain (from a topology perspective) how Layer 2 and Layer 3, and routed and non- routed deployments appear, and potential VLANs you might use when deploying the Smart-hopping devices and monitors.

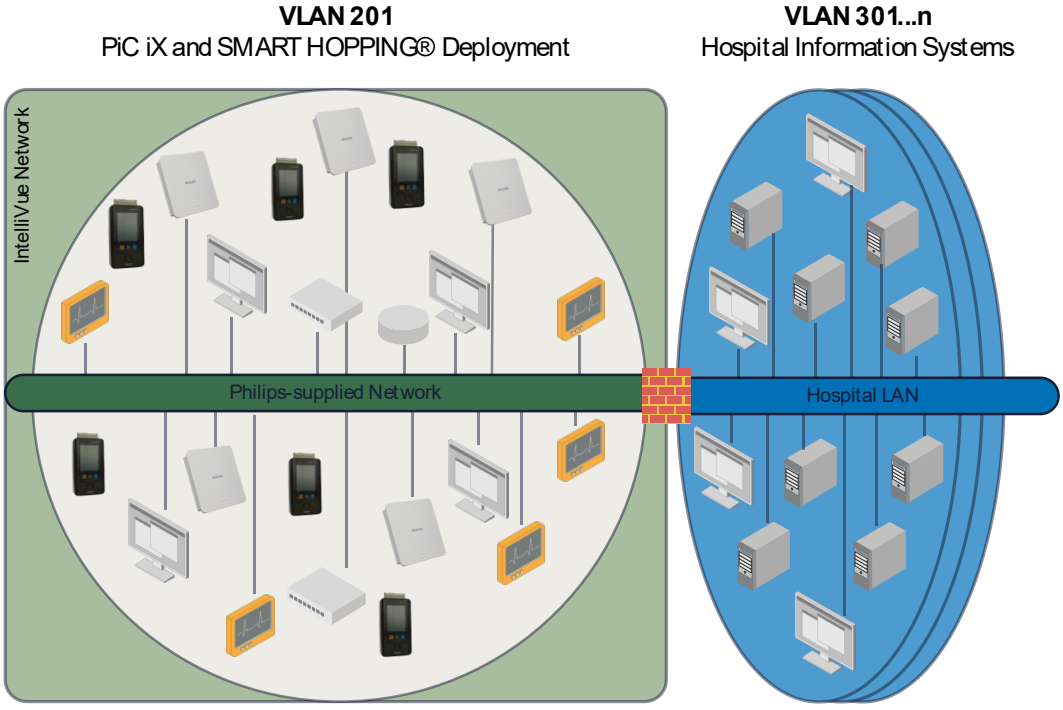


Figure 73: Layer 2 Non-routed Deployment on a Philips-Supplied Network

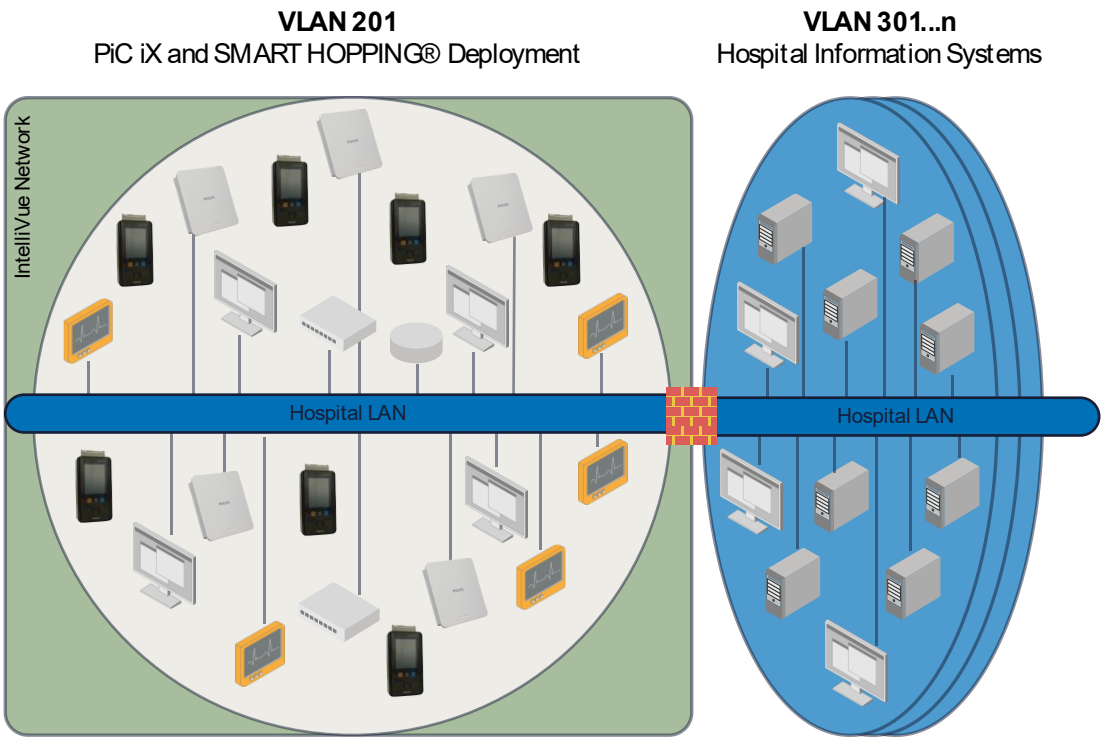


Figure 74: Layer 2 Non-routed Deployment on a Customer-Supplied Network

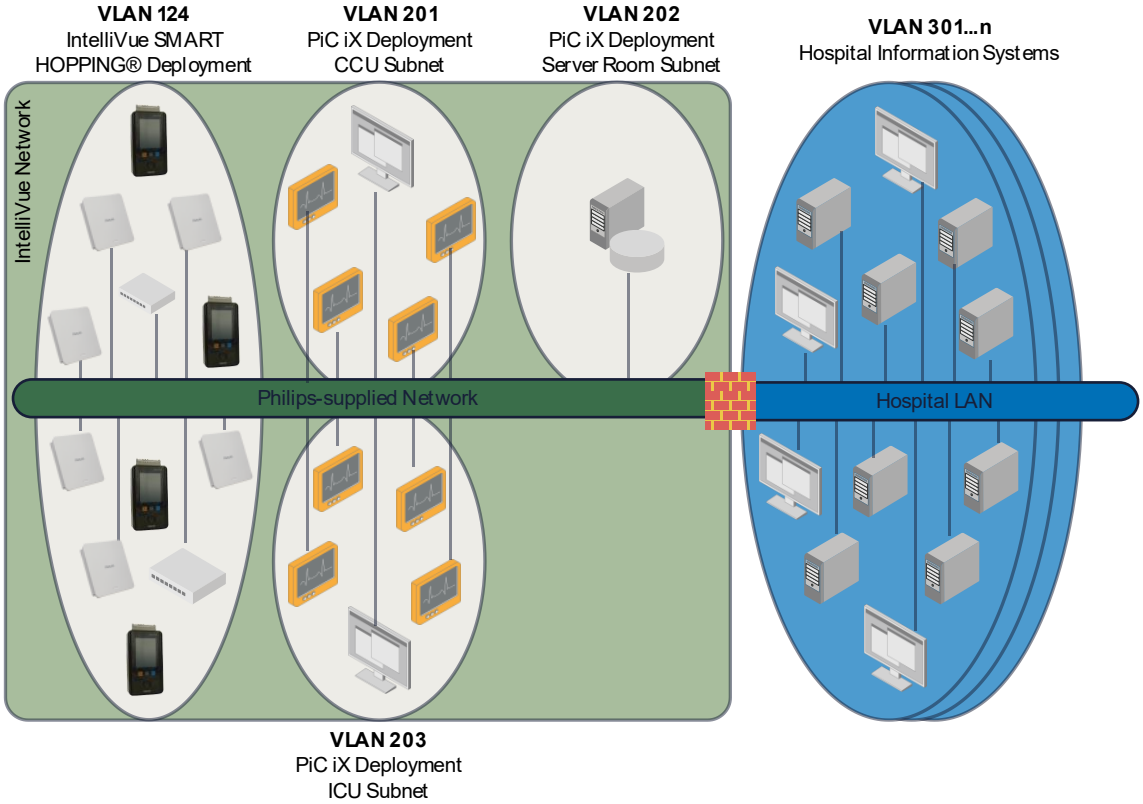


Figure 75: Layer 2 Routed Deployment on a Philips-Supplied Network

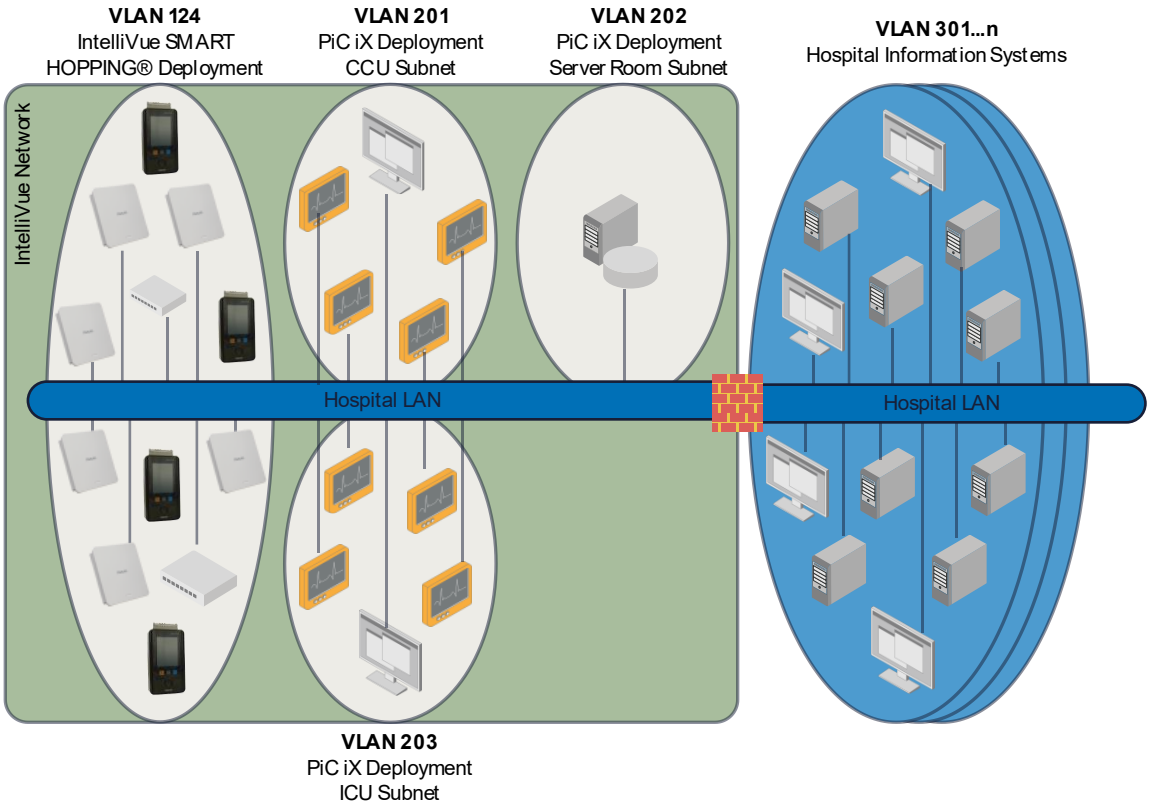


Figure 76: Layer 2 Routed Deployment on a Customer-Supplied Network

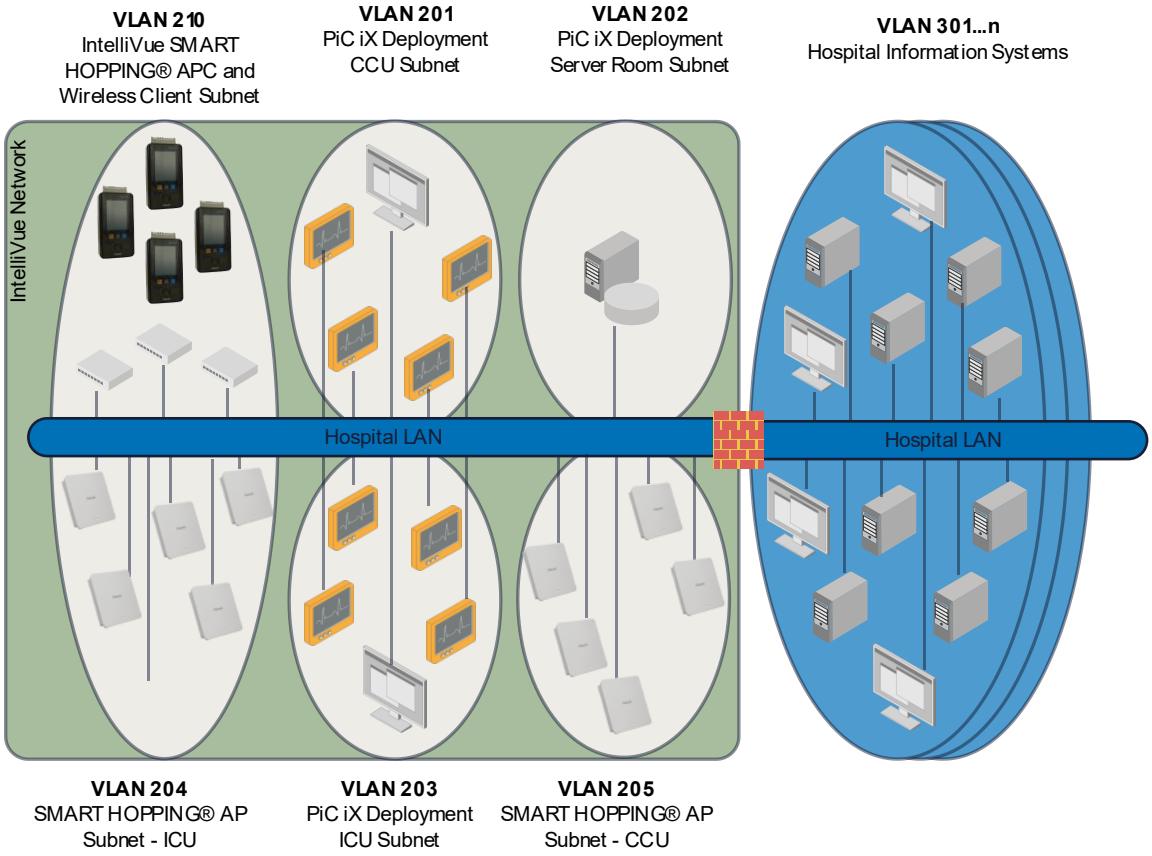


Figure 77: Layer 3 Routed Deployment on a Customer-Supplied Network (Example 1)

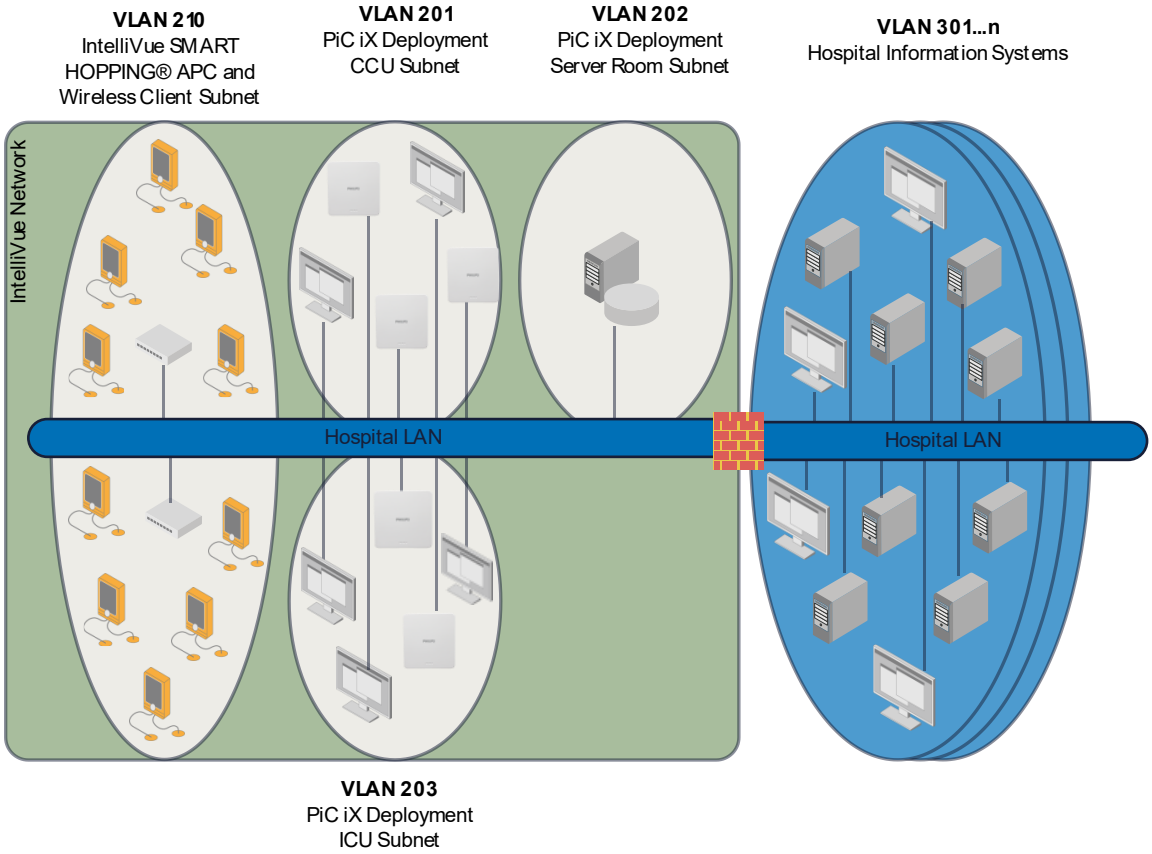


Figure 78: Layer 3 Routed Deployment on a Customer-Supplied Network (Example 2)

13 Appendix F: DHCP option 43

When deploying a PIC iX server, support for Layer 3 or routed functionality for Smart-hopping Access Points in a remote subnet needs to obtain its IP address, subnet mask, default gateway and 2 Multicast IP addresses dynamically from a customer supplied DHCP server.

The Access Point joins the supplied Multicast IPs using Internet Group Management Protocol (IGMP) and uses them to discover and register with the Access Point Controller serving those groups.
In large CSCN environments with multiple Smart-hopping networks, each Smart-hopping network must be configured to use different pairs of Multicast IP addresses.

13.1 Background

The DHCP protocol defines each option with an option code which is a number between 0 and 255. To avoid conflicts between options, new options must be registered with a standards body and be published as an RFC.

The number of official options is limited and the process to get a new option recognized is difficult. For this reason, a new mechanism was introduced to make it easier for vendors to distribute their own proprietary information without clashing with other vendors and without having to register new options each time one is needed. This is achieved through the DHCP option 43 (Vendor Specific Information).

Each vendor has a private table of DHCP options which is kept separately by the DHCP server. These options are numbered similarly to the main DHCP options but the numbers refer to the private option table for each vendor. The numbers used for global options can be reused for private options with a completely different meaning. Each vendor is identified by a Vendor Class Identifier. When a DHCP Client asks for vendor specific options it makes a request with Option 60 using the predefined Vendor Class Identifier string. The DHCP server replies with Option 43, including the vendor code corresponding to the Vendor Class string supplied by the Access Point during the DHCP request and the options configured for that specific scope.

To correctly support Option 43, the DHCP server must have the ability to manage multiple option tables, one table for the global options and one table for each Vendor for the vendor specific options.

13.2 DHCP option 43 implementation

The majority of DHCP Servers do not support multiple vendor definitions for Option 43. Only a single vendor definition is supported for Option 43. Furthermore, once Option 43 is defined at the DHCP Server Option level which means it is applied to all DHCP scopes (all subnets) globally, it is impossible to define different multicast IP addresses for different zones.

It is crucial that configurable Multicast IP addresses are used by Smart-hopping Access Points on a subnet by subnet basis, per DHCP Scope.

It is recommended that IP addresses be assigned a lease time of eight days. If APs are powered off for longer than the lease time:

- Device location performance will be impacted.
- Statistics will not be gathered.
- The status indicated in the status log of the Philips IntelliVue Information Center will not be accurate.
- All devices should be rescanned into the database server.
- Define a PHILIPS AP Vendor Class.
- The Smart-hopping AP sends a DHCP discover using Option 55 (Parameter Request List) to list all options for which the Smart-hopping AP is expecting a response. The Parameter list will include:
    - Subnet mask (1)
    - Default gateway (3)
    - Domain Name Server (6)
    - Broadcast Address (28)
    - Static Route (33)

- Vendor-Specific Information (43)

- The Smart-hopping AP includes DHCP Option 60 (Vendor Class Identifier) using PHILIPS AP as its Vendor Class Identifier.
- The DHCP Server will use the supplied Parameter List and Vendor Class string to determine which options to return to the Access Point in the DHCP offer.

13.2.1 Configure a DHCP scope for each subnet

The following procedure describes how to configure a DHCP Scope for each subnet using the most common options:

1. Open the DHCP administrative console by clicking on Administrative Tools > DHCP.

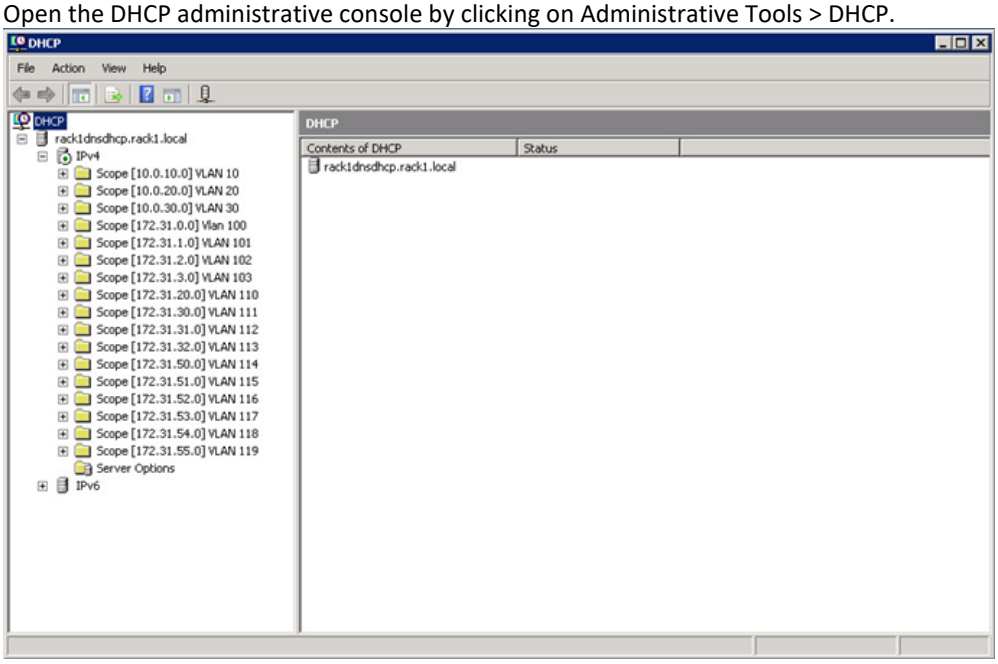


Figure 79: DHCP Administrative Console

2. Right-click on the IPv4 item and select New Scope from the list.

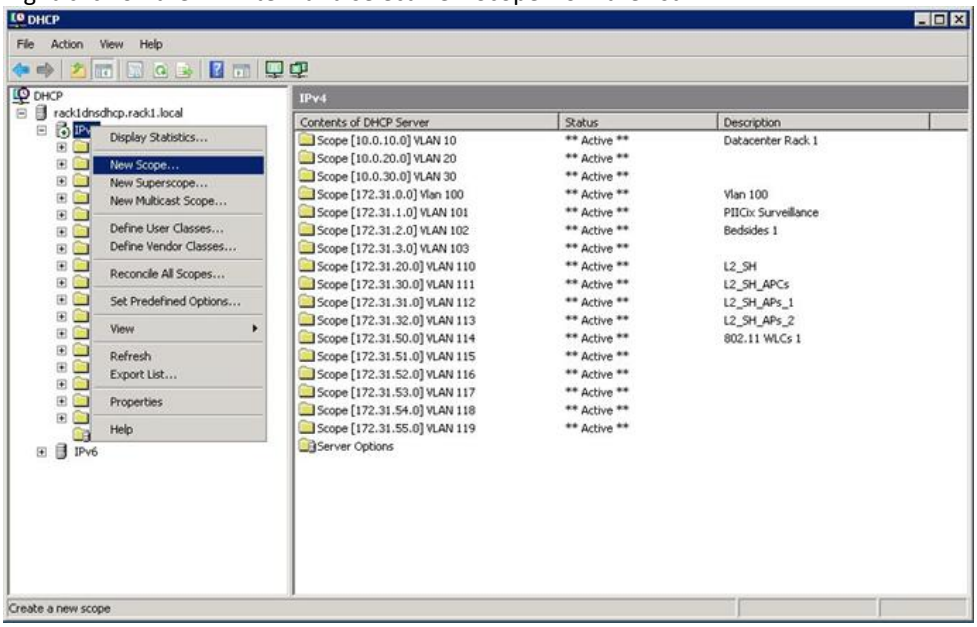


Figure 80: New Scope

3. Enter a Name and Description for the new scope. Click Next.

Figure 81: Name and Description

4. Enter the Start IP Address and End IP Address for the new scope. Adjust the range to meet your specific network needs. Click Next.

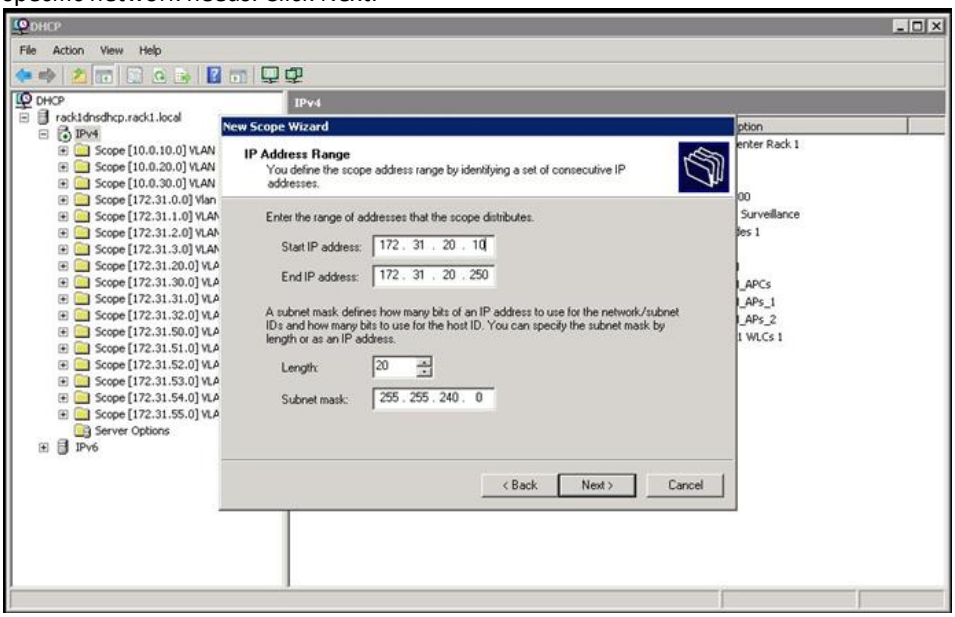


Figure 82: Start and End IP Addresses

5. Do not enter any exclusions in the Add Exclusions dialog. Click Next.

6. Enter a lease duration of eight days (the default value). Click Next.

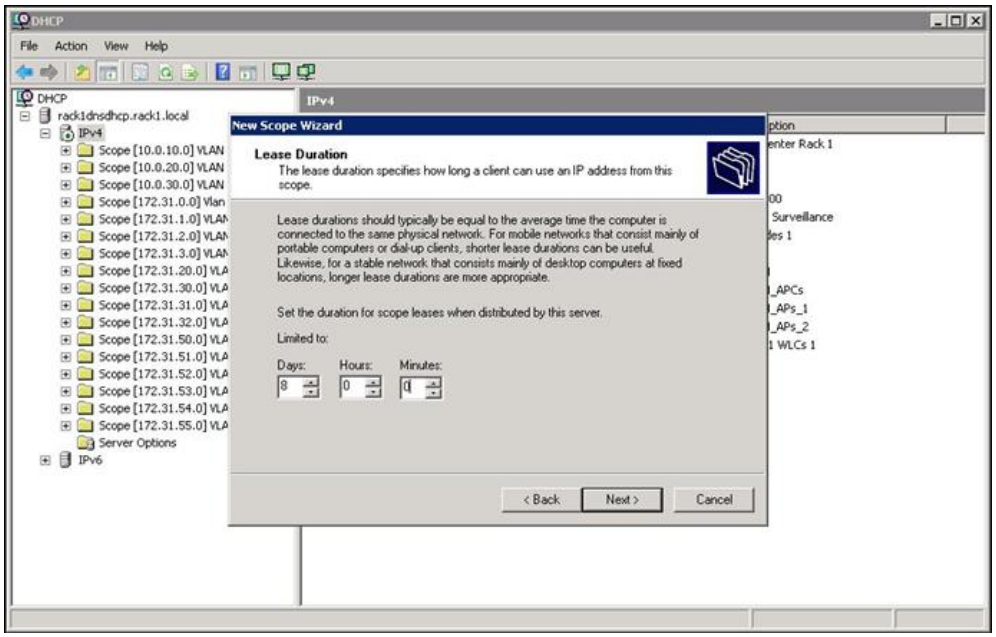


Figure 83: Lease Time

7. Select the Yes radio button to configure the DHCP options now. Click Next.

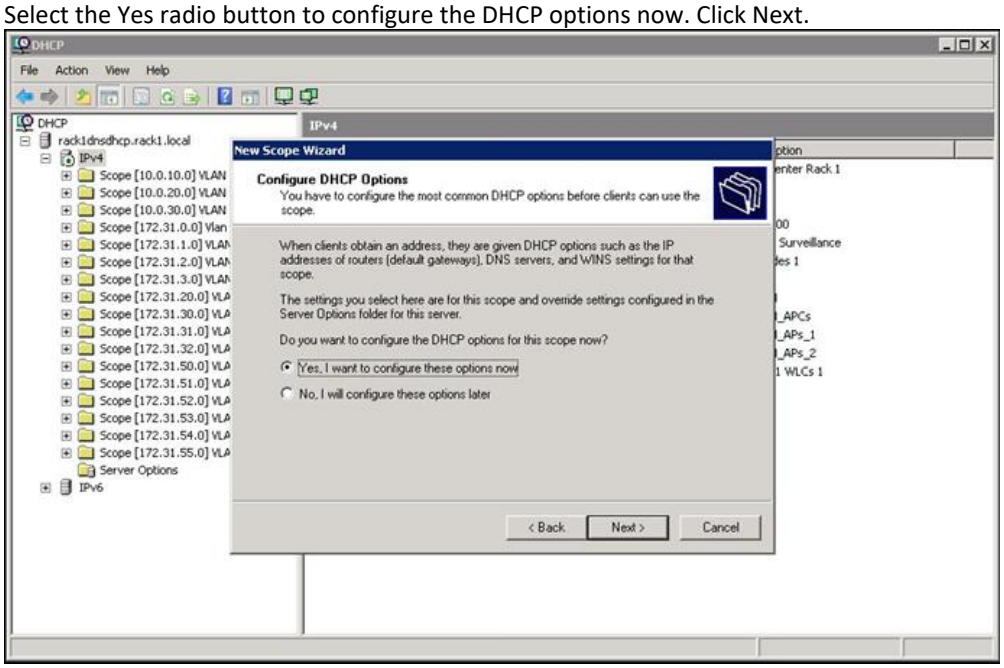


Figure 84: DHCP Options

8. Enter the IP Address for the Router (Default Gateway). Click Add. Click Next.

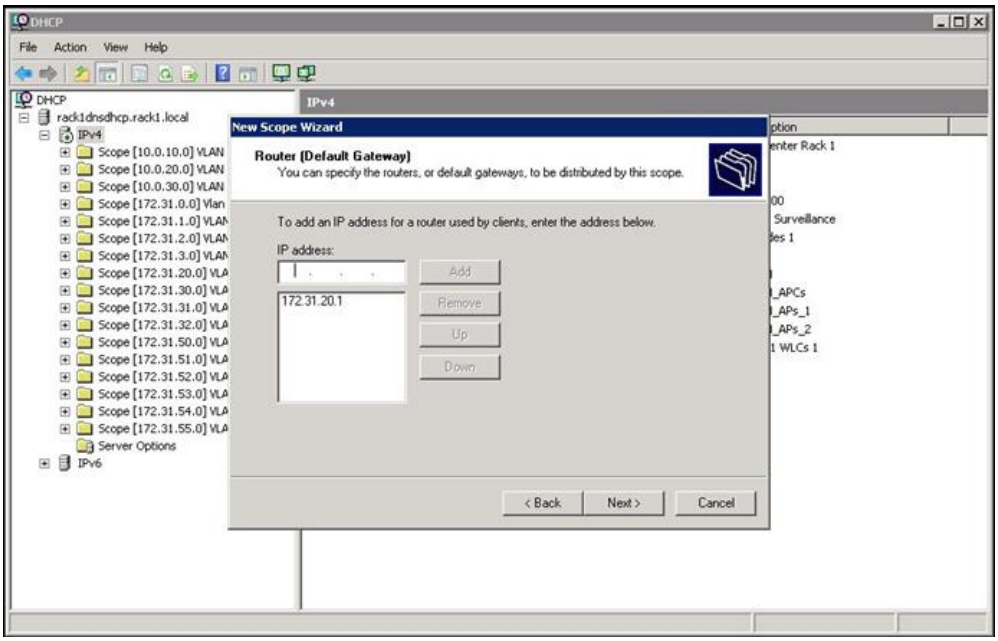


Figure 85: Router (Default Gateway)

9. Enter the Domain Name and DNS Servers IP Address. Click Add. Click Next.

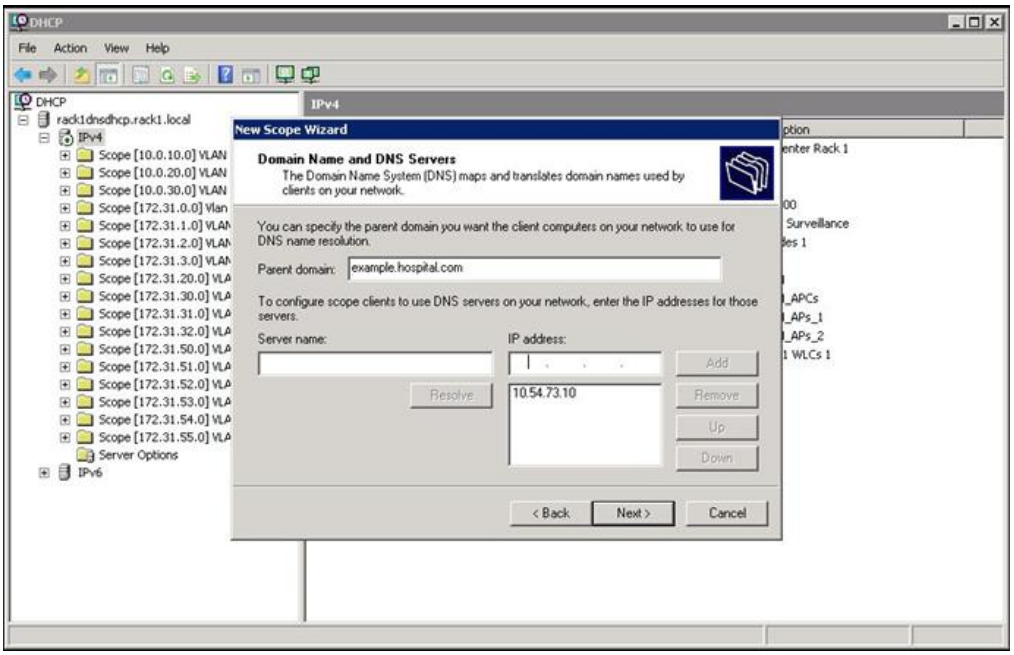


Figure 86: Domain Name and DNS Servers

10. Leave the WINS Server field blank. Click Next.

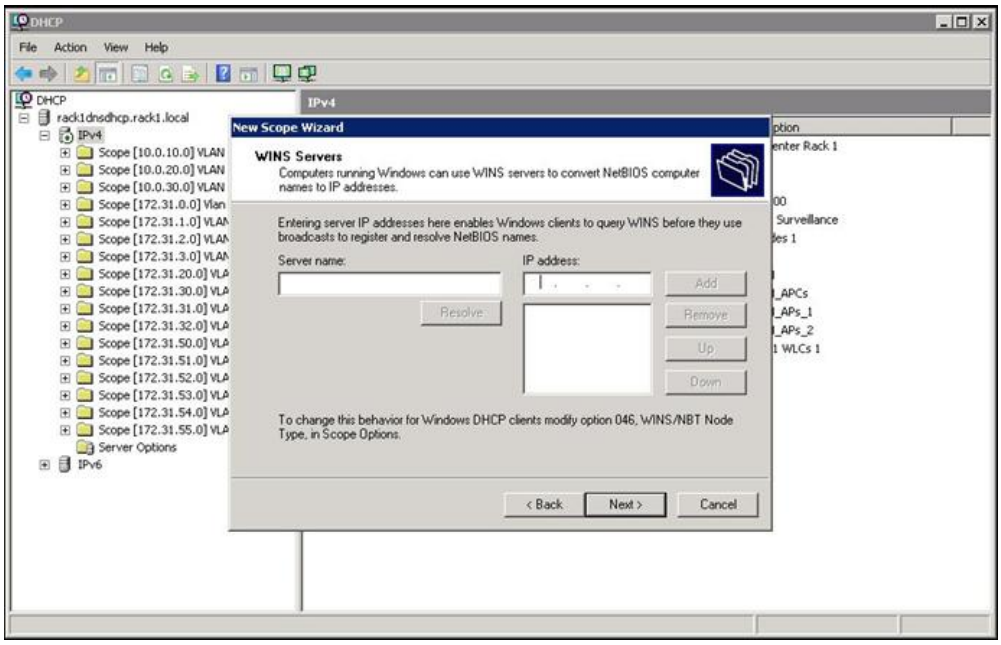


Figure 87: WINS Server

11. Select the Yes radio button to activate the scope. Click Next. Click Finish.

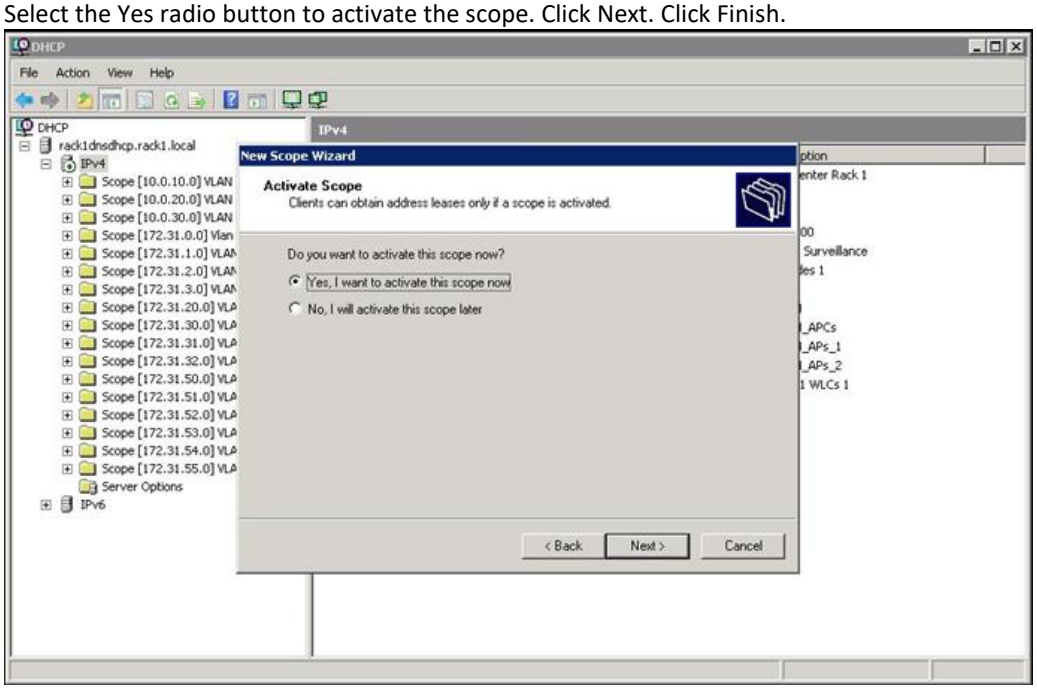


Figure 88: Activate the Scope

12. Select the Scope Options to verify that all settings are entered correctly.

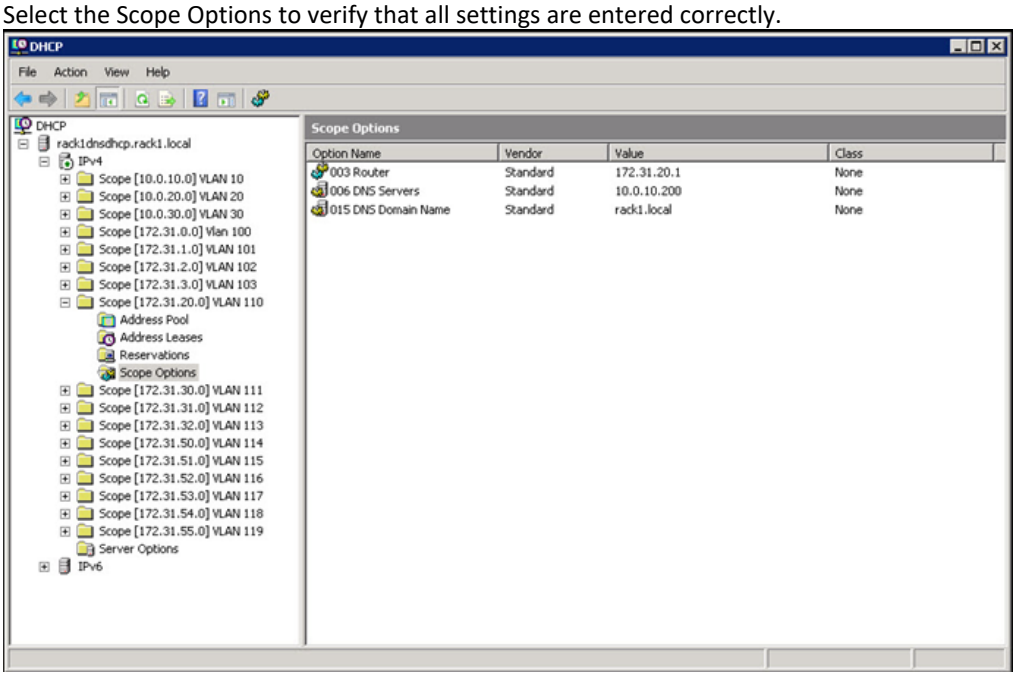


Figure 89: Scope Options

13.2.2 Windows 2008 server or windows 2003 server example

1. Define a Philips Vendor Class.
    a. Open Start > Programs > Administrative Tools > DHCP.
    b. Expand the contents of the server.
    c. Right click under IPv4 and choose Define Vendor Classes.

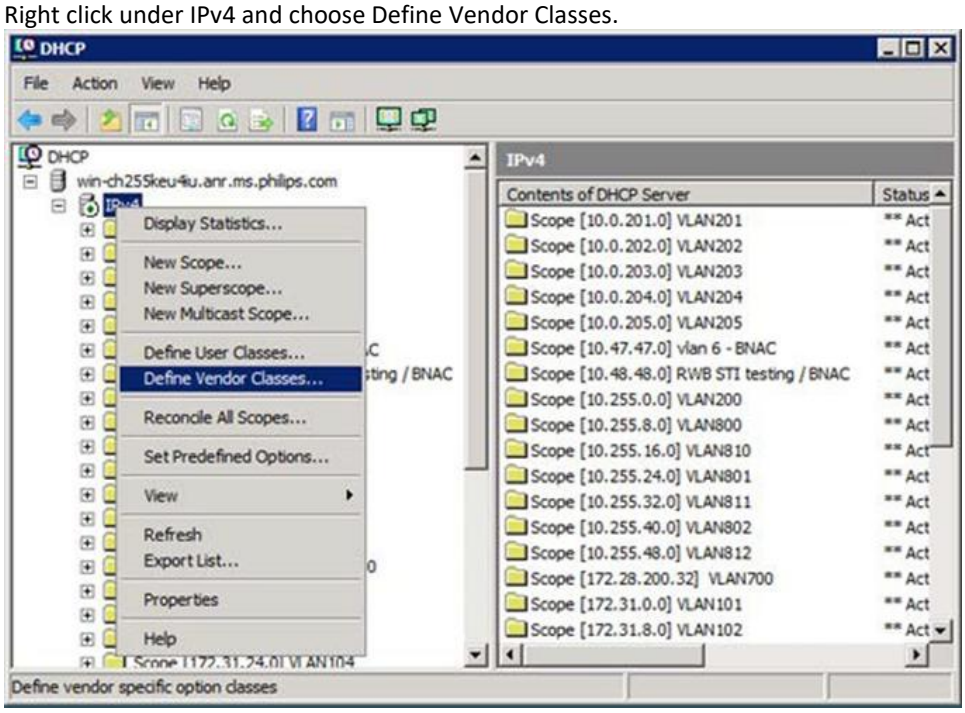


Figure 90: Define New Vendor Class

    d. Click on the Add button.
    e. Enter PHILIPS AP as the Display Name and Philips SH AP Vendor Class in the Description Field of the New Class dialog box.
    f. Place your cursor under the ASCII field of the dialog box and left click your mouse to enter PHILIPS AP in the ASCII field.

Note In this ASCII field the syntax must match exactly. The entry must be all capitals with a space between “PHILIPS” and “AP.”

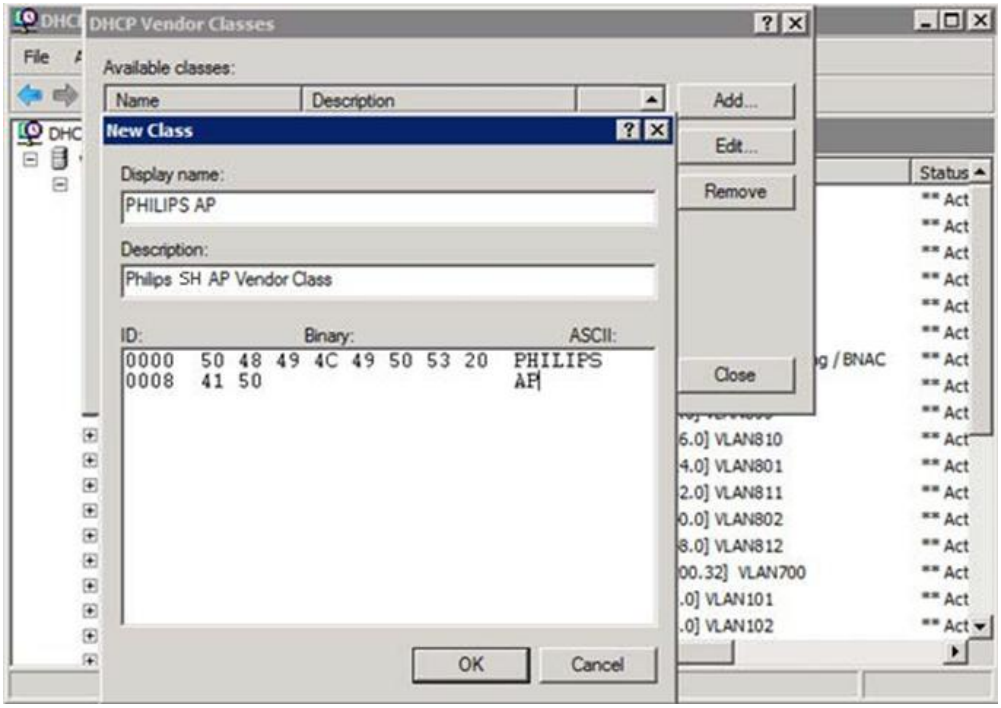


Figure 91: New Class dialog box

g. Click the OK button to exit New Class dialog. Click on the Close button to exit the DHCP Vendor Classes dialog box.

2. Right click IPv4 and choose Set Predefined Options.

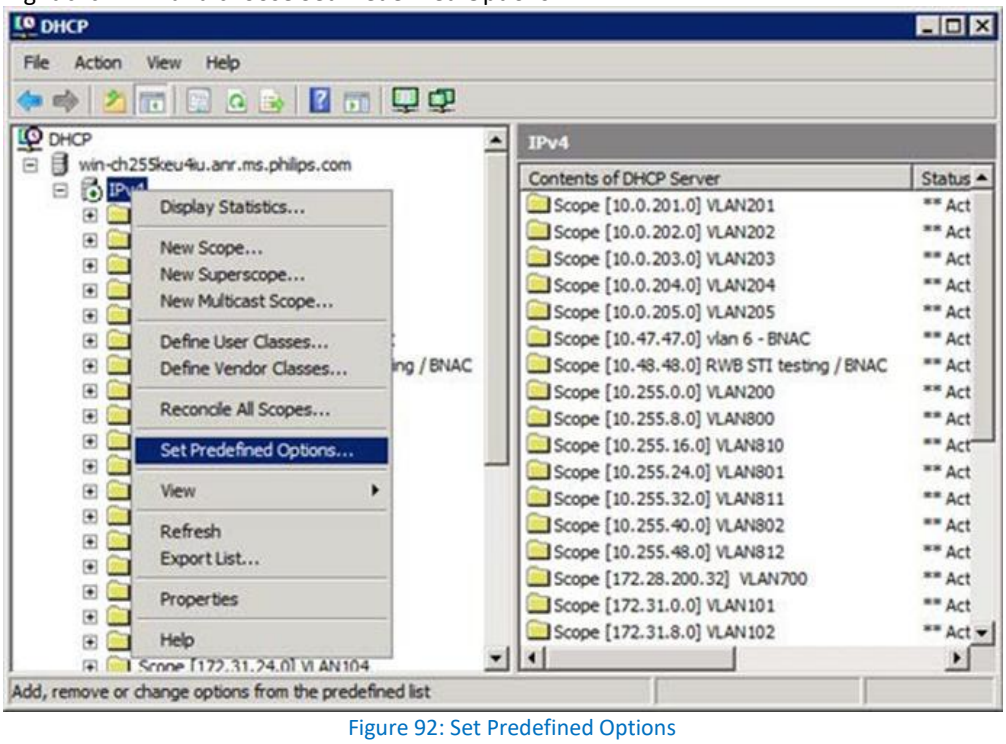


Figure 92: Set Predefined Options

a. In the Predefined Options and Values dialog box, select PHILIPS AP in the Option Class drop down box.
Note that this is the PHILIPS AP Vendor Class that you created.

b. Since this is the first Predefined Option for this Vendor Class the Option Name drop down box is empty. Click on the Add button, to add a New Option Type.

c. Enter Philips AP Multicast IPs under Name, select IP Address under Data Type drop down box and then click on the Array check box.

d. In the Code text box, enter 224 (if available) and in the Description, enter a short description such as Philips SH AP Multicast Addresses.

e. Click OK to exit the Option Type dialog box. Click OK to exit the Predefined Options and Values dialog box.

Note Do not enter any default values under the Edit Array check box. You will specify these on a per scope basis.

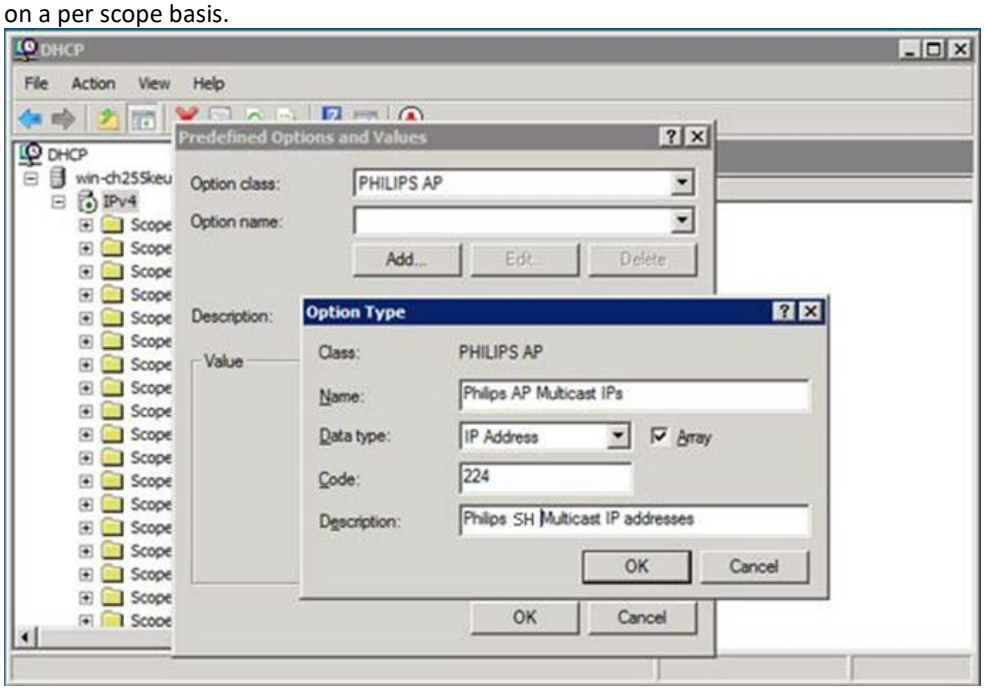


Figure 93: Option Type dialog box

3. Configure Scope Options.

a. After defining a DHCP Scope, expand the Scope, right click on the Scope Options and select Configure Options.

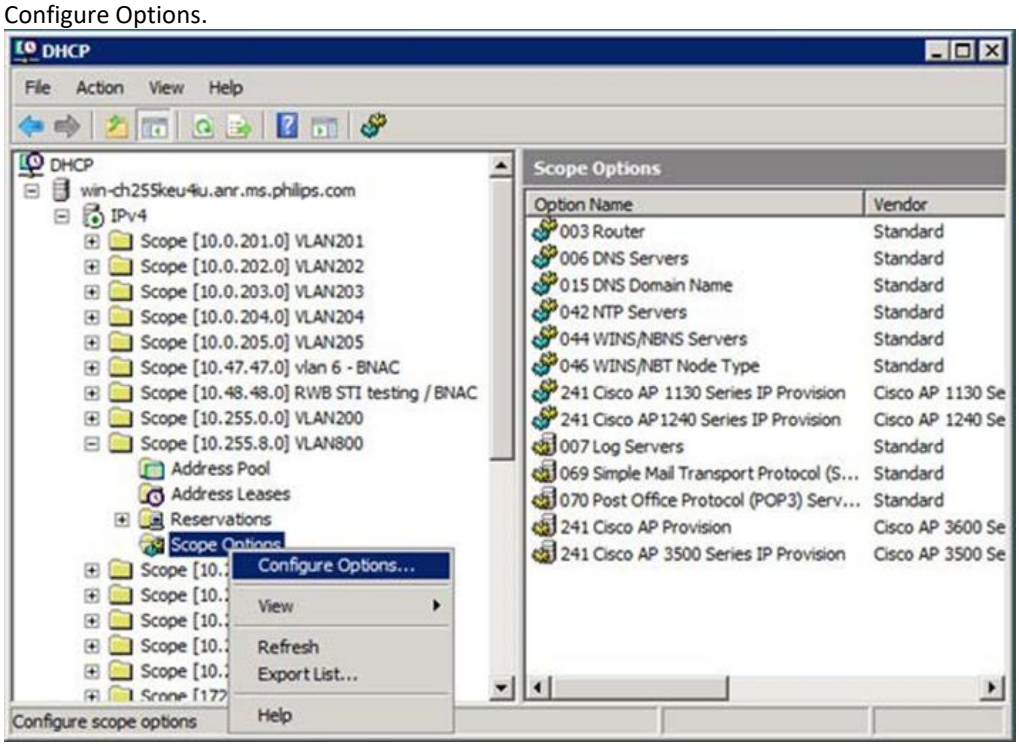


Figure 94: Configure Scope Options

b. Click on the Advanced tab and under Vendor class, select PHILIPS AP. A list of predefined options will appear below the Available Options text box.
c. Select the 224 Philips AP Multicast IPs option.
d. In the Data Entry section of the dialog box, leave the Server name blank. In the IP address section, type the Primary APC Multicast IP address you want to configure for this DHCP scope and click on the Add button. Then type the Secondary APC Multicast IP address and click on the Add button.
e. Click on the Apply button.
f. Click on the OK button to exit the Scope Options dialog box.

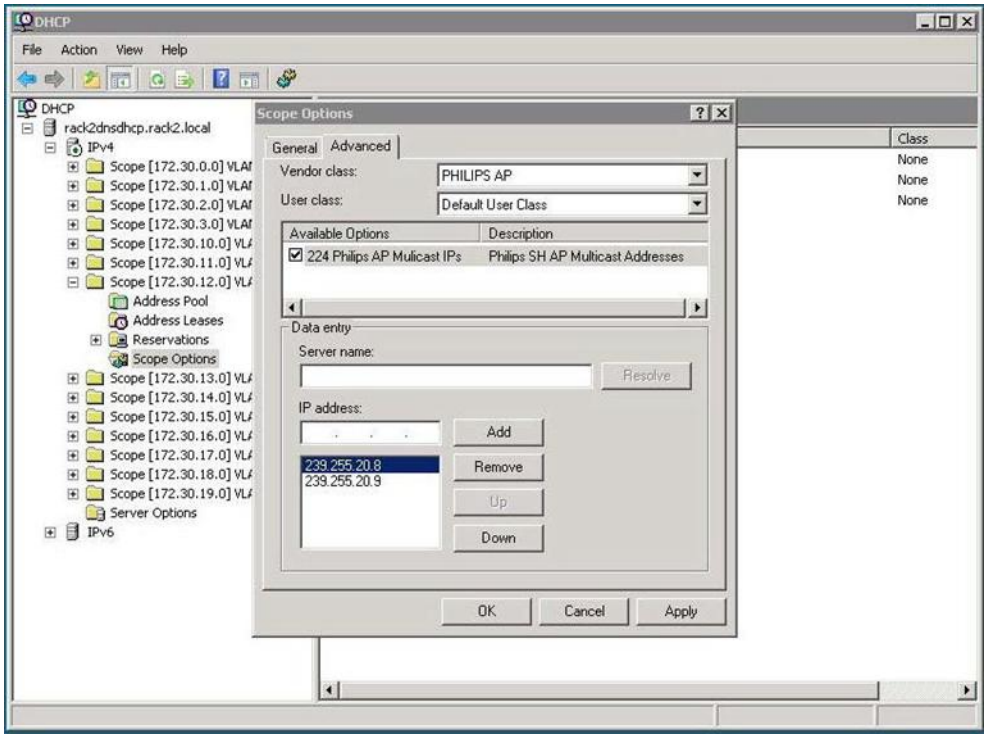


Figure 95: Scope Options dialog box

g. Verify the scope options are configured correctly by looking at the multicast IP address under the Vendor column for the item PHILIPS AP.

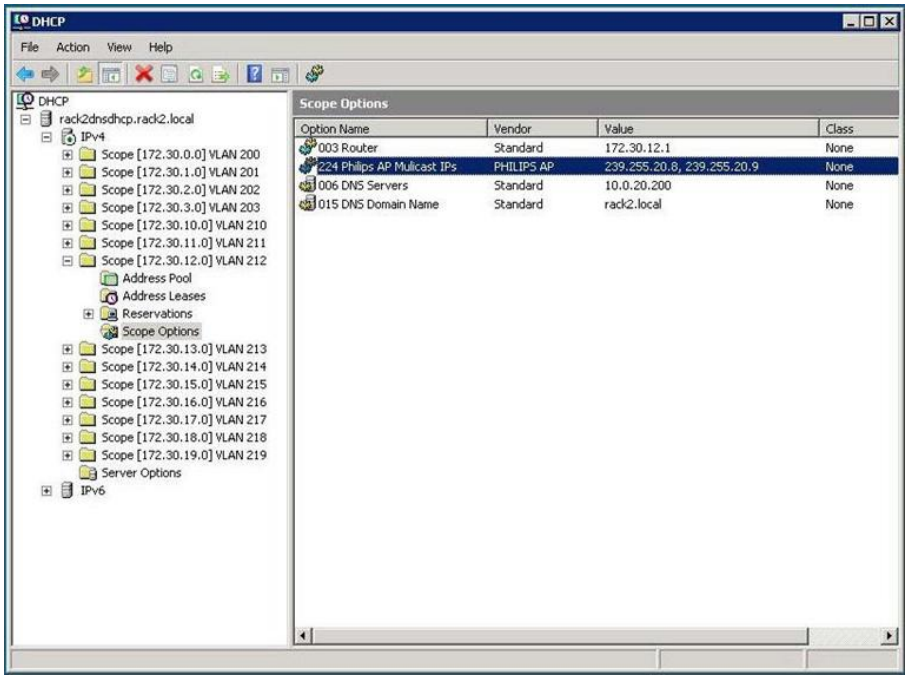


Figure 96: Multicast IP values

h. The changes take effect immediately. Exit the DHCP Administrative tool.

13.2.3 Wireshark captures: Philips layer 3 Access Point DHCP request

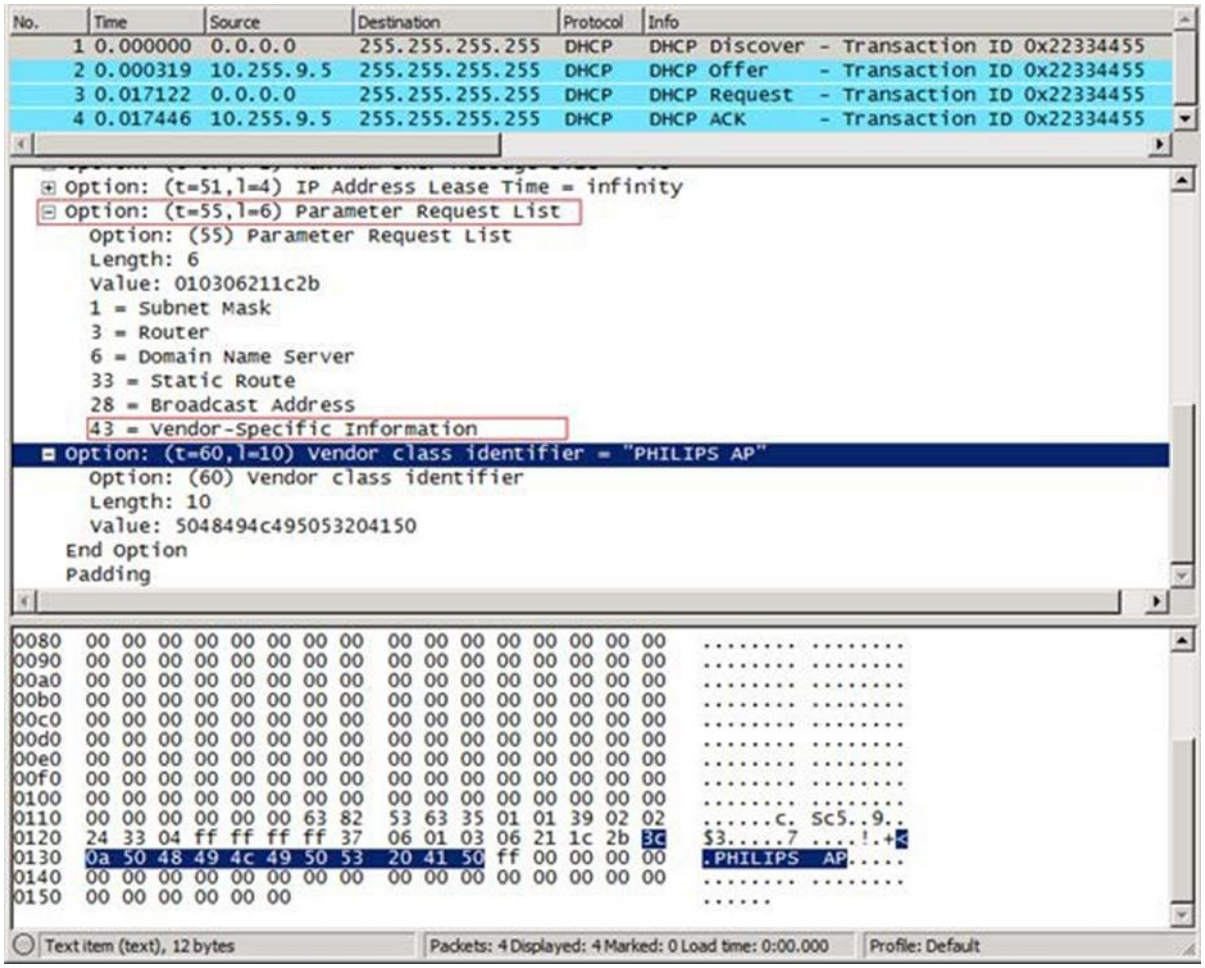


Figure 97: Parameter Request List

The DHCP Client includes Option 43 in the Option 55 Parameter Request List and also includes Option 60 supplying its Vendor Class identifier, in this case PHILIPS AP.

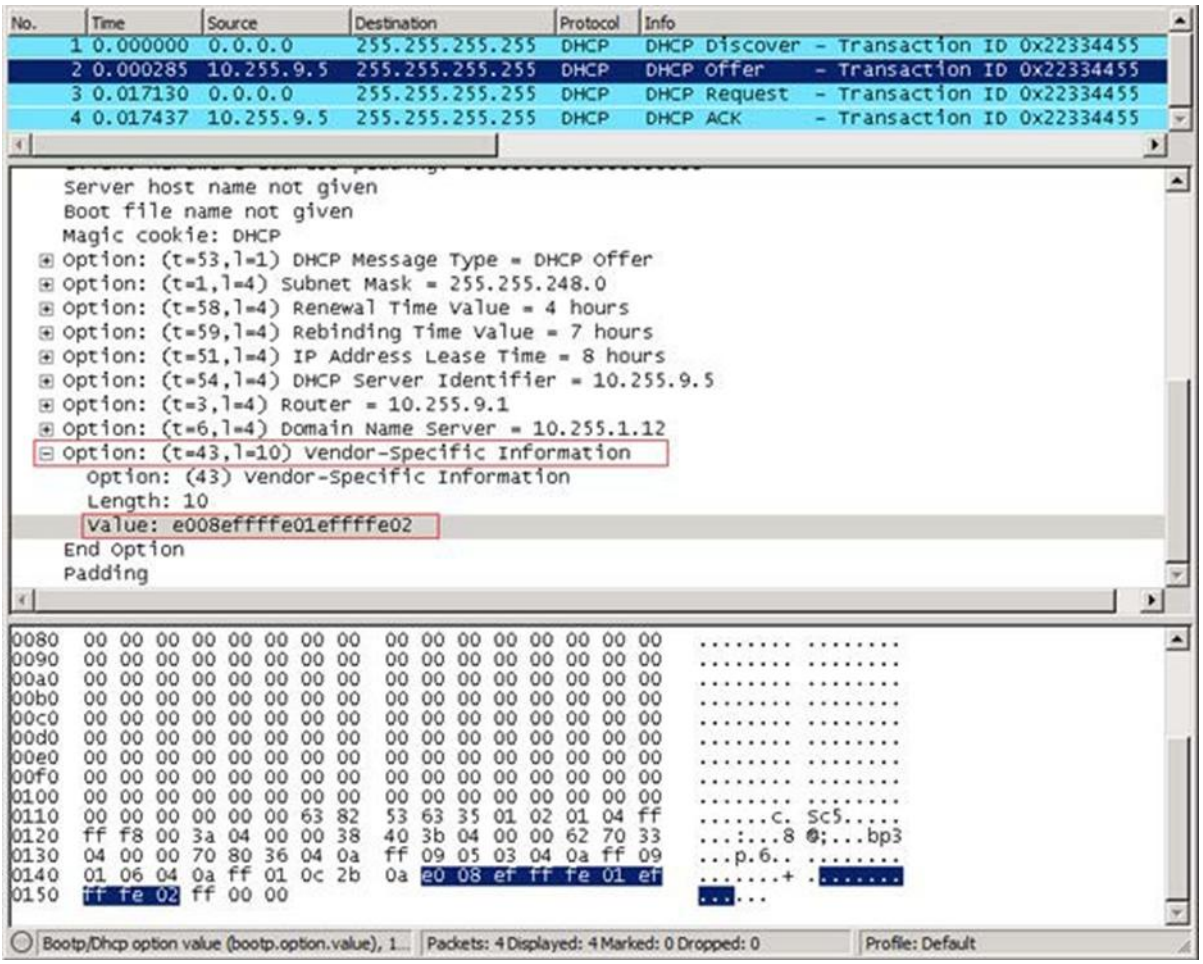


Figure 98: Option 43 values

The DHCP Server responds with the following DHCP Option 43 based on the client supplied Vendor Class: The highlighted values in the option 43 Field of e0 08 ef ff fe 01 ef ff fe 02 translates to:

e0 = Philips AP Vendor Option code = 224

08 = Number of Bytes in the array

ef ff fe 01 = 1st Multicast IP address 239.255.254.1

ef ff fe 02 = 2nd Multicast IP address 239.255.254.2

14 Appendix G: Configuring layer 3 option on each AP

This appendix describes how to configure the Layer 3 option on each AP:

- Smart-hopping 1.0
- Smart-hopping 2.0

14.1 Smart-hopping 1.0

Philips recommends that Customer-supplied Clinical Networks use the DHCP Option 43. For more information on DHCP Option 43, refer to Appendix F, DHCP Option 43. If not using DHCP Option 43, you must manually configure each AP using the following procedure:

1. Power up the AP from the PoE switch.

2. Open a terminal session from your service PC.

3. Configure the terminal session:
    a. Enter a name for the New Connection. Click OK.
    b. Select an available COM port from the Connect Using drop-down menu, and then click OK.
    c. Set the serial port settings as follows:
        i. Bits per second: 115200
        ii. Data bits: 8
        iii. Parity: None
        iv. Stop bits: 1
        v. Flow Control: None
    d. Click Apply, then OK.

4. Connect a serial cable between an available COM port on your service PC and the AP serial interface port. The following prompt is displayed:

```
781F  halLedSetSyncStatus:  Status  is  0092
7FE7 CCLmenu
```

5. At the prompt enter CCLmenu then hit return. The following menu is displayed:

```
91AB
91AB  CCL  debug  menu
91AC Versions:
91AC  Hardware  Revision:   HW59111037
91AD Firmware:                C.99.07
91AF  Secondary  boot  loader:   C.99.04
91B0 Primary boot loader:      C.00.08
91B1 DECT firmware (d/m/y): 15/06/2012  17:16
91B2 AP has been up:            93599s
91B3   1) Ethernet options
91B4   2)  Set  debug  level
91B5   3) Application menu
91B6   4)  Run  test  engine
91B6   5) Memory menu
91B7   6) Dect menu
91B8  7)  Slot  services  menu
91B8  8)  Debug  display  menu
91B9  9)  PSKEY menu
91BA  A)  Unit  test  menu
91BB  B)  Chip  test  menu
91BB  C)  Profile menu
91BC  D)  Generate  software  fault
91BD  0)  Return  to  previous  menu
91BE
91BE Enter command required: 1
```

6. At the prompt enter the number 1. The following menu is displayed:

```
9C73
9C73
9C73 Ethernet options
9C74 Current Ethernet settings: 100BASE-T, full duplex, Force speed
switch off
9C76 Proxim packets Rx:                          35819
9C78 Other packets Rx:                           38652
9C79 Rx errors:                                      0
9C7B   1) Set transmit display options
9C7C   2) Run Ethernet sniffer
9C7D   3) Set Ethernet MAC address
9C7E   4)  Set  default  IP  address
9C7F   5)  Display  Ethernet  chip
9C80   6) Stop Ethernet chip
9C80   7)  Start  Ethernet  chip
9C81   8) Display PIC settings
9C82   9) Show Ethernet descriptors
9C83   A) Suspend the Ethernet chip
9C84   B)  Resume  the  Ethernet  chip
9C85   C) Display EEPROM
9C86   D) Set EEPROM word
9C87   E) Reset AP
9C87   F) Print TX Descriptors
9C88   G) Print RX Descriptors
9C89   H) Restart Ethernet Controller
9C8A   I) Set Multicast Filter
9C8B  J)  Toggle  Auto-negotiation
9C8C  0)  Return  to  previous  menu
9C8D
9C8D Enter command required: I
```

7. At the prompt enter the letter I and hit return. The following prompt is displayed:

```
A5BF Enter Primary Multicast IP address: 239.255.200.100
```

8. At the prompt enter the Multicast IP address of the Primary/Secondary APC[4] and hit return. The following prompt is displayed:

```
CC1A Enter Secondary Multicast IP address: 239.255.200.101
```

[4] The default values for the Primary and Secondary Multicast IP addresses are 239.255.254.1 and 239.255.254.2 respectively. The values shown here are only for example purposes; your network configuration may vary.

9. At the prompt enter the Multicast IP address of the Secondary APC and hit return. The following menu is displayed:

```
D7D2
D7DB
D7DB Ethernet options
D7DC Current Ethernet settings: 100BASE-T, full duplex, Force speed
switch off
D7DE Proxim packets Rx:                          35847
D7E0 Other packets Rx:                           38682
D7E1 Rx errors:                                      0
D7E3   1) Set transmit display options
D7E4   2) Run Ethernet sniffer
D7E5   3) Set Ethernet MAC address
D7E6   4) Set default IP address
D7E7   5) Display Ethernet chip
D7E8   6) Stop Ethernet chip
D7E8   7) Start Ethernet chip
D7E9   8) Display PIC settings
D7EA   9) Show Ethernet descriptors
D7EB   A) Suspend the Ethernet chip
D7EC   B) Resume the Ethernet chip
D7ED   C) Display EEPROM
D7EE   D) Set EEPROM word
D7EF   E) Reset AP
D7EF   F) Print TX Descriptors
D7F0   G) Print RX Descriptors
D7F1   H) Restart Ethernet Controller
D7F2   I) Set Multicast Filter
D7F3  J) Toggle Auto-negotiation
D7F4  0) Return to previous menu
D7F5
D7F5 Enter command required: 0
```

10. At the prompt enter the number 0 and hit return to return to the previous menu. The following menu is displayed:

```
E7EF
E7EF
E7EF  CCL  debug  menu
E7F0 Versions:
E7F0  Hardware  Revision:   HW59111037
E7F1 Firmware:                C.99.07
E7F2  Secondary  boot  loader:   C.99.04
E7F4 Primary boot loader:      C.00.08
E7F5 DECT firmware (d/m/y): 15/06/2012  17:16
E7F6 AP has been up:            93669s
E7F7   1) Ethernet options
E7F8   2)  Set  debug  level
E7F9   3) Application menu
E7F9   4)  Run  test  engine
E7FA   5) Memory menu
E7FB   6) Dect menu
E7FB  7)  Slot  services  menu
E7FC  8)  Debug  display  menu
E7FD  9)  PSKEY menu
E7FE  A)  Unit  test  menu
E7FF  B)  Chip  test  menu
E7FF  C)  Profile menu
E800  D)  Generate  software  fault
E801  0)  Return  to  previous  menu
E802
E802 Enter command required: 0
```

11. At the prompt enter the number 0 and hit return to return to the previous menu. The following output is displayed:

```
ECC4 ApcregSM TUNNELLING/MAPC_RESP_RX

ECC5 MAPC_RESP was from 172.31.241.1
ECC6 Leaving ApcregSM TUNNELLING
ECC7 AP run time is 26:1:13
ECC8 config state machine resetting radio
F16F Average ARQ retry: 0
F18E ApcregSM TUNNELLING/KEEPALIVE_TIMEOUT
F2CA version string from Hal: V29907.29904.20008
F2CB Version in reg request: 1.0-B211
F2CC Constructing TLV
F2CD Constructing TLV
F2CD Leaving ApcregSM TUNNELLING
F2CE ip2mac about to send_via_arp
F2CF halLedSetSyncStatus: Status is 0092
F2EA FMID State machine, state: STANDBY, event EXPIRY_TIMEOUT
F328 Requesting Subnet table
F339 Leaving FMID state machine: state WAITING_SUBNET_TABLE_UPDATE
F33B ip2mac about to send_via_arp
F33C ConfigGetSet: SET tag 0x1304
F33E Config: AP System Name: Philips
F33F ConfigGetSet: SET tag 0x1308
F340 ConfigGetSet: SET tag 0x1309
F341 Subnet table:
F341 subnet[0]: 172.31.240.0
F342 config state machine resetting radio
F343 FMID State machine, state: WAITING_SUBNET_TABLE_UPDATE, event
SUBNET_TABLE_
UPDATED
F346 Broadcasting FMID keepalive SUBNET BROADCAST
F356 Broadcasting FMID keepalive MULTICAST BROADCAST
F357 FMID table clear expired
F358 My FMID Table is now:
F359 Mac addr: 0:9:FB:25:10:A3; Ip addr: 172.31.242.3; fmid:
0x203; Expiry: 1440
2
F35B Leaving FMID state machine: state STANDBY
F35C ip2mac about to send_via_arp
F35D ETHMCAST enabled
F35E     ip_write_internal     IN_MULTICAST
EFFFFE02 F35F ip2mac about to send_via_arp
F360 ETHMCAST enabled
F361 send_arp enable Multicast MAC address
F362 halLedSetSyncStatus: Status is 0092
```

Once the prompt is returned the AP is configured. It is important to wait until the prompt is returned to provide enough time for the AP to save the new values entered.

12. Unplug the AP from the PoE.

13. Repeat all steps for each AP to be configured.

14.2 Smart-hopping 2.0

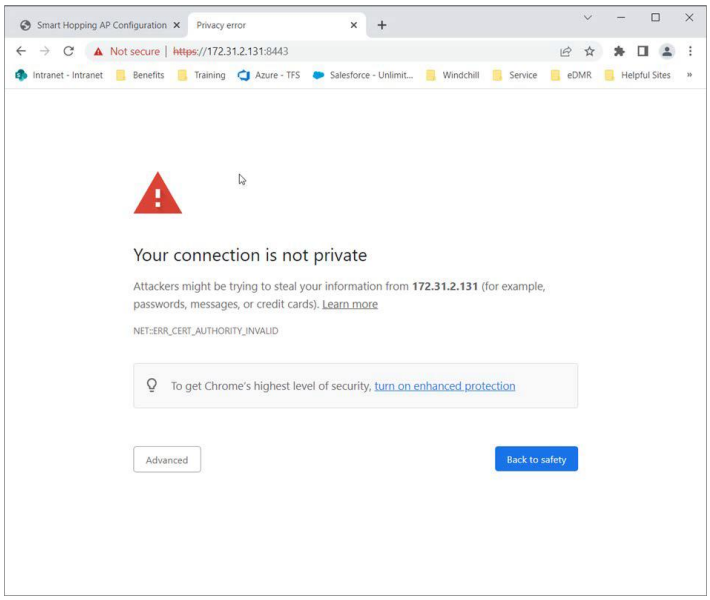
Philips recommends that Customer-supplied Clinical Networks use the DHCP Option 43. For more information on DHCP Option 43, refer to Appendix F, DHCP Option 43. If not using DHCP Option 43, you must manually configure each AP using the following procedure:

14.2.1 Connecting to the Access Point Web Interface

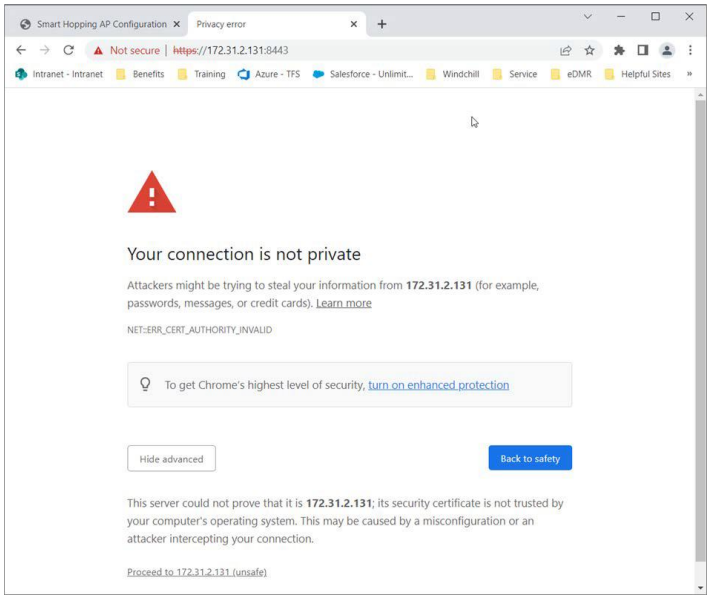
To connect to the Access Point web interface, do the following:

1. Open a browser and enter the IP address of the AP and connect to port 8443 (for example, http://172.31.2.131:8443).
   A warning displays to tell you that the security certificate is not valid. This is normal when connecting to the AP web interface.

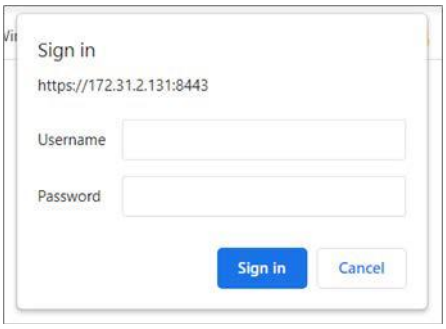
2. Select the Advanced button for the option to bypass this warning.



3. The Advanced Settings view displays. Select the Proceed to <IP Address> (unsafe) link to display the AP web interface.

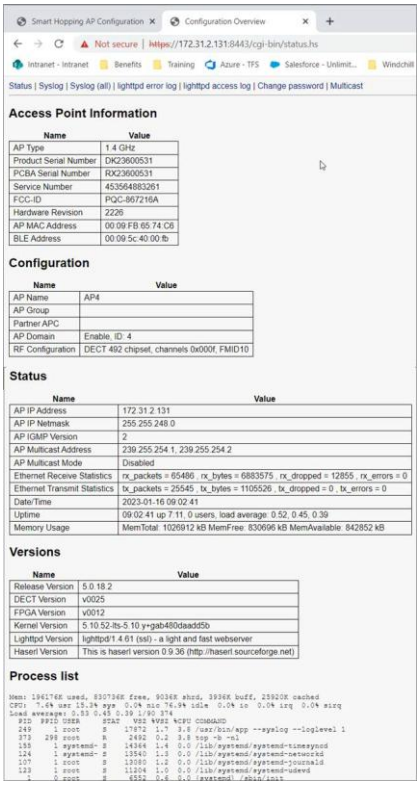


4. At the Sign In prompt, enter your user ID and password, and click Sign In.



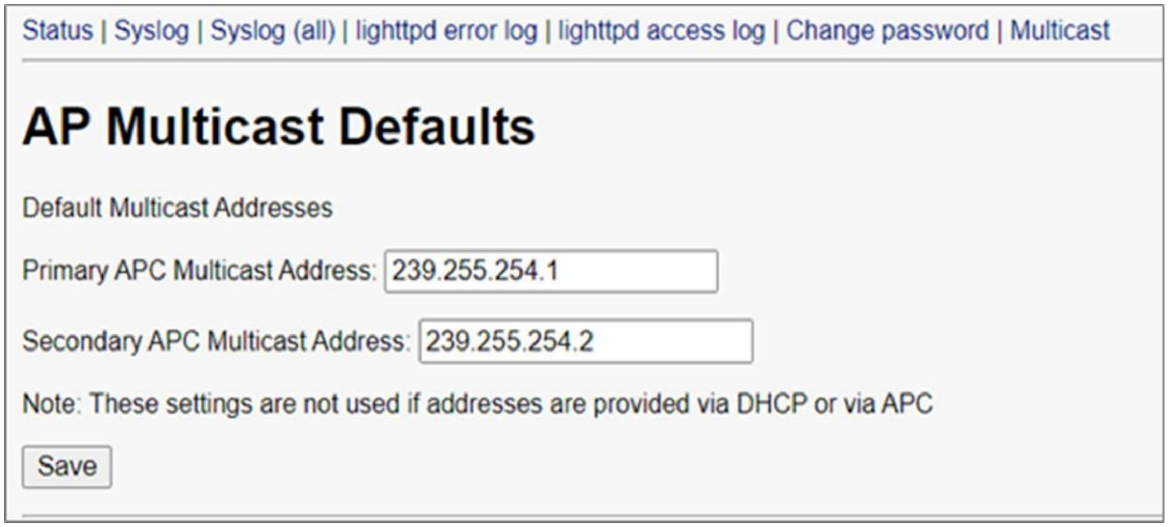
Note There is no timeout feature for the web interface. Make sure you close the web interface after completing the desired service action.

5. The AP Status tab displays.



6. The Status tab displays a variety of information related to the Access Point, as shown in the image.

7. Select Multicast from the options tab. This displays AP Multicast Defaults and allows you to configure Multicast information on your Access Point Controller.



8. If you want to change the Primary or Secondary Multicast IP address your APC uses, enter the IP address of your Multicast server in the appropriate address field. When you are done, click Save to save the new address configuration.
   Note If your APC provides the Multicast IP addresses or your DHCP server provides them, the settings in this tab are ignored.