
IntelliVue Clinical Network

Installation and Service Manual

Part Number M3185-91909
Printed in the U.S.A. August 2003
Edition 1

PHILIPS

About this Manual

Proprietary Information

This document contains proprietary information, which is protected by copyright. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

Philips Medical Systems
3000 Minuteman Road
Andover, MA 01810-1085
(978) 687-1501

Publication number
M3185-91909
Printed in USA

Warranty

The information contained in this document is subject to change without notice.

Philips Medical Systems makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties or merchantability and fitness for Philips Medical Systems shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Copyright

Copyright © 2003 Philips Electronics North America Corporation

Windows NT, Windows 98, and Windows 2000 are registered Trademarks of Microsoft Corporation.

Printing History

New editions of this document incorporate all material updated since the previous edition. Update packages may be issued between editions and contain replacement and additional pages to be merged by a revision date at the bottom of the page. Pages that are rearranged due to changes on a previous page are not considered revised.

The documentation printing date and part number indicate its current edition. The printing date changes when a new edition is printed. (Minor corrections and updates that are incorporated at reprint do not cause the date to change.) The document part number changes when extensive technical changes are incorporated.

First Edition..... August 2003
IntelliVue Clinical Network Release E.01.xx

Text Conventions

The following conventions for Notes, Cautions, and Warnings are used in this manual.

Note A **Note** calls attention to an important point in the text.

Caution A **Caution** calls attention to a condition or possible situation that could damage or destroy the product or the user's work.

Warning A **Warning** calls attention to a condition or possible situation that could cause injury to the user and/or patient.

Explanation of Symbols

Symbols on products and packaging mean the following:



Defibrillator-proof type CF equipment



Caution: Consult accompanying documents.



Signal (ECG) Input



Signal (ECG) Output



Data input/output



Alternating Current



Direct Current



Protective earth



Equipotential grounding post



Temperature



Humidity



Altitude or atmospheric pressure



Contains parts to be recycled



Contains parts that may not be put into normal waste disposal but must be recycled or dealt with as chemical waste



Fragile, handle with care



Keep dry



Consult instructions for use



Date of manufacture



Serial number



Catalog number



Batch code

About this Document

This document contains Service and Installation information for the IntelliVue Clinical Network, (hereinafter called the Clinical Network). Other products referenced are the IntelliVue Information Center, IntelliVue Information Center Client, IntelliVue Database Server, IntelliVue Small Database Server, and the IntelliVue Application Server.

Document- ation CD

The **Service and User Documentation CD** contains the following IntelliVue documentation:

- Clinical Network Installation and Service Manual
- Database Server Installation and Service Manual
- Information Center Installation and Service Manual
- Information Center Instructions for Use
- Information Center Installation Notes
- Information Center, Clinical Network, and Database Server Quick Reference Guides
- Application Notes
- Service Documentation for the PC Workstation, NetServer, LaserJet Printer, and other hardware devices

Table of Contents

About this Manual	1-2
Proprietary Information	1-2
Warranty	1-2
Copyright	1-2
Printing History	1-2
Text Conventions	1-3
Explanation of Symbols	1-3
About this Document	1-5
Document-ation CD	1-5
Introduction	1-1
Overview	1-1
Philips Patient Care System	1-2
Patient Monitors	1-2
Clinical Network Connected Operation	1-3
Information Center Client	1-3
Networks	1-4
Philips CareNet	1-4
Clinical Network	1-5
Patient Care Systems	1-7
Clinical Network Without a Database Server	1-7
Clinical Network With IntelliVue Database Server	1-7
Clinical Network With IntelliVue Small Database Server	1-9
M3185 Clinical Network	1-9
Switches	1-9
Network Connections	1-10
Extended Distances	1-10
Components and Options	1-12

Active Components	1-12
Purchased Options	1-12
Cabling Installation Materials.....	1-12
Mounting Options	1-13

Hardware Description.....2-1

Overview.....2-1

System Components.....2-2

Core/Edge Switches	2-3
Extension Switch/Repeater	2-4
Wireless Access Points	2-5
Access Points Mount Kit	2-6
Access Point Controller	2-7
Remote Power System	2-8
AP Power Over LAN	2-9
Wireless Bedside Adapter	2-10
Media Translators	2-11
Printer	2-14
Uninterruptible Power Supply	2-15
Operation	2-16
M3185 Cables and Installation Materials.....	2-17
UTP Cable.....	2-17
Fiber Optic Cable	2-19
Wall Boxes	2-20
Patch Panels.....	2-21

Specifications.....2-22

Physical	2-23
Environmental	2-24
Electrical	2-25

Regulatory.....2-26

Philips Software.....	2-26
Philips Hardware	2-26

- Site Planning 3-1**
- Overview 3-1**
- Site Planning 3-2**
- Considerations 3-2
- Responsibilities 3-2
- Customer 3-2
- Philips Factory 3-3
- Philips Service Provider 3-3
- Location 3-3
- Wiring Closets 3-4
- Rack Mounting 3-4
- Switches 3-4
- Wireless Access Points 3-4
- Extension Switches & Media Translators 3-4
- UPSs 3-5
- Other 3-5
- Network 3-5
- Cabling 3-5
- Environmental Requirements 3-6
- Electrical Requirements 3-6
- Equipment Mounting 3-6
- Safety 3-6
- Medical Device Standards 3-6
- Philips Device Requirements 3-6
- Patient Environment 3-6
- Network Design 3-7**
- Clinical Requirements 3-7
- Number of Units and Beds 3-7
- Patient Monitor Type 3-7
- Central Monitoring Locations 3-7
- Patient Data Review Locations 3-7
- Type of Patient Data Access 3-8
- Future Capability 3-8
- Philips Hardware Capability 3-8
- Patient Monitors 3-9

CareNet	3-9
Clinical Network	3-9
Printers	3-10
Switch Function	3-10
Switch Firmware	3-10
Switch Rules	3-10
Upgraded Systems	3-11
Designing Clinical Network Systems	3-11
Connecting Devices	3-12
Specific Network Device Settings	3-13
Drawing the Design	3-13
Design Guidelines	3-13
Directed Messages	3-14
Broadcast and Multicast Messages	3-14
Example 1: Single Switch Network	3-14
Example 2: Multiple Switch Network	3-16
Wireless Network Systems	3-19
Frequency Management	3-19
Wireless Network Design Guidelines	3-19
Standard vs Non-Standard Systems	3-20
Standard System Design	3-21
Standard System Example	3-22
Non-Standard System Design	3-25
Non-Standard System Example	3-25
Channel Reuse-Example	3-26
RF Survey	3-27
Performing the RF Data Throughput Survey	3-27
Checking for Channel Reuse	3-30
Installing the Clinical Network.	4-1
Overview	4-1
Preparing for Installation	4-2
Cable Plant Installation	4-2
Installation Materials	4-2
Noise Immunity	4-2

UTP Cable Plant Installation	4-3
RJ-45 Connections	4-4
Fiber Optic Cable Plant Installation	4-4
Unpacking and Inspection	4-4
Philips Shipments	4-4
Unpacking Components	4-5
Checking Inventory	4-5
Inspection	4-5
Packaging Inspection	4-5
Mechanical Inspection	4-5
Electrical Inspection	4-6
Claims for Damage	4-6
Re-packaging for Shipment	4-6
Network Component Installation	4-7
Switch Firmware	4-7
Device Configuration	4-7
Using ConfigTool	4-8
Network Switches	4-11
RangeLAN2 Access Points	4-14
M3/M4 Monitors	4-16
Wireless Bedside Adapters	4-19
Access Point Controllers & Harmony Access Points	4-21
Configuration Troubleshooting	4-28
Using HyperTerminal Connection	4-29
Physical Installation	4-42
Switches	4-42
RangeLAN2 Wireless Access Points	4-42
Media Translators	4-44
Network Connections	4-45
Switch to Switch	4-48
Switch to 100 Mbps HALF Network Devices	4-48
Switch to 100 Mbps FULL Network Devices	4-48
Switch to 10 Mbps Network Devices	4-49
Clinical Network Devices: Names and IP Addresses	4-50
IP Address	4-50
Subnet Mask	4-51

Default Gateway	4-51
MAC Address	4-51
Host Name.	4-51
Device Name.	4-52
Setting Host Names and IP Addresses	4-52
Verifying Network Connectivity	4-52
Troubleshooting the Clinical Network	5-1
Overview	5-1
Maintenance	5-2
Routine Maintenance.	5-2
Air Intakes.	5-2
UPS.	5-2
Troubleshooting.	5-4
Troubleshooting Strategy	5-5
SDN Connectivity	5-6
Wireless Connectivity	5-6
.	5-7
Network Connectivity	5-8
Server Connectivity	5-9
System Trouble-shooting.	5-10
Network Statistics	5-13
Switches	5-13
HP 2524 Switch.	5-13
Cisco 1900 Switch	5-20
Access Points	5-22
Diagnostics.	5-26
Service Portal Support.	5-26
LED Diagnostics	5-28
LAN Interface Card	5-28
Harmony Access Point LED Diagnostics.	5-29
RangeLAN2 Access Point	5-30

Access Point Controller LED Diagnostics	5-32
Remote Power System LED Diagnostics	5-33
HP2524 Switch	5-33
Cisco Switch	5-35
Allied Telesyn AT-FS708 switch	5-36
LED Status Indicators	5-36
Ports 1 - 7	
LED Status Indications	5-37
Port 8MDI	
LED Status Indications	5-37
J3300 10Base-T Hub	5-38
10 Mbps Media Translator	5-39
100 Mbps Media Translator	5-40
Repair	5-42
Philips Hardware	5-42
UPS	5-42
UPS Configuration	5-44
Restoring Switch Firmware - HP2524	5-46
Single Switch Firmware restore	5-46
Switch to Switch Firmware Restore	5-49
Restoring Switch Firmware - Cisco	5-53
Restoring Wireless M3/M4 Wireless Adapter Firmware	5-59
Restoring Access Point Firmware	5-65
Replaceable Parts	5-71
Testing Product Assurance	6-1
Testing Product Assurance	6-1
Visual Tests	6-1
System Components	6-1
Cables	6-1
Connectors	6-1
Test and Inspection Procedures	6-1
Clinical Network	6-3
Worksheets	A-1

Overview	A-1
Network Installation	A-2
Remote Clients on T1 Lines	B-1
Overview	B-1
System Diagrams	B-2
Changing Network Properties	B-4

Overview

The IntelliVue Clinical Network is the Philips Medical Systems medical network for transmitting and reviewing patient monitoring data from multiple IntelliVue Information Center central monitors within and across units in a clinical care environment. It is based on industry standard components and cabling and provides for interconnecting up to 8 Information Centers at different clinical locations.

Note The **Information Center Installation and Service Manual** provides detailed information on the Information Center, Information Center Client, and the Database Servers.

Note The **Application Server Installation and Service Manual** provides detailed information on the Application Server.

Chapter 1 overviews the Clinical Network in the following sections.

Philips Patient Care System	page 1-2
Components and Options	page 1-12

Philips Patient Care System

The **Philips Patient Care System** provides a comprehensive patient monitoring solution for a variety of clinical environments -- ER, ICU, CCU, Stepdown Unit. It comprises patient monitors for obtaining patient monitoring data, central monitors for displaying and analyzing patient monitoring data, and switches and networks for interconnecting components at multiple hospital locations.

Patient monitors can be Philips hardwired CMS, 24 Monitors, telemetry monitors, IntelliVue Patient Monitors, or M3/M4 monitors (hardwired or wireless). **Central monitors** are the IntelliVue Information Centers. The **switch and network** can be the Philips CareNet with CareNet switch or the IntelliVue Clinical Network that uses industry standard network components. The **database server** is the IntelliVue Database Server or the IntelliVue Small Database Server.

Patient Monitors

Patient monitors from Philips Medical Systems provide a wide variety of patient monitoring solutions with the Clinical Network. Compatible patient monitors that connect directly to the Clinical Network (wired and/or wireless) are the family of M2/M3/M4 Monitors and the family of IntelliVue Patient Monitors. Compatible patient monitors include those that connect to the Philips CareNet are the Philips Component Monitoring System (CMS), 24 Monitors, and Telemetry Monitors. A list of patient monitors compatible with Release E.01 software on the Philips Patient Care System is given in Table 1-1. Currently available models are shown in Figure 1-1. Table 1-1 also gives the software releases for each model that are required for compatibility with Philips Release E.01 software and for EASI capability.

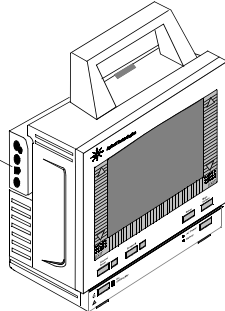
Table 1-1. Patient Monitors Compatible with Software Rel. E.01 and EASI

Product Name	Product Number	Software Release Req'd for Rel. E.01	Software Release Req'd for EASI
IntelliVue Patient Monitor	M8005A/M8007A/ M8010A	A.10 and later	A.10 and later
Component Monitoring System	M1175/76/86A	C and later	C and later
Philips 24 Patient Monitor	M1205A	all	C and later
Compact Configured Monitor	78352A/C, 78353B, 78354A/C 78833B, 78834A/C	all	Not supported
Digital UHF Telemetry	M1403A/J	E.0 and later	E.0 and later
Philips Telemetry System	M2600A	E.00.19 and later	E.0 and later
TeleMon		A.0 and later	
Philips M2/M3/M4 Wired Monitor	M3046A	D.0 and later	E.0
M3/M4 Wireless Patient Monitor	M3046A #J20		
M2/M3/M4 Measurement Server	M3000A	C.04 and later	

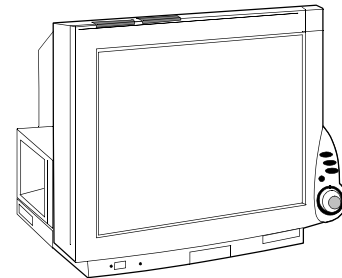
Note M2350/60A CCMs (release B.03.13) that monitor telemetry with release 2.x cannot connect to the same Serial Communications Controller (SCC) as Information Center systems (release C.0 and later).

Patient Monitors connecting directly to the Clinical Network

M2/M3/M4
Measurement
Server

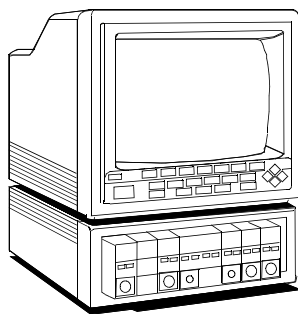


M2/M3/M4 wired Patient Monitor
M3/M4 wireless Patient Monitor

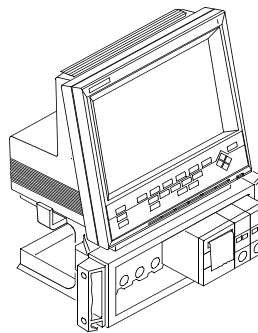


IntelliVue Patient Monitor
IntelliVue Wireless Patient Monitor

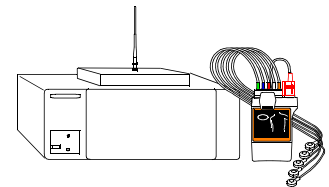
Patient Monitors on the CareNet



Component
Monitoring System



24 Patient Monitor



Philips Telemetry
System

Figure 1-1 Patient Monitors Compatible with the Clinical Network

**Clinical Network
Connected
Operation**

The Information Centers can be connected to the Clinical Network and can provide full Clinical Network/Database Server functionality.

When the Information Center is connected to the Clinical Network with a Database Server, displayed patient monitoring data are transmitted to the Database Server for storage. **Real-time and stored** data are then available for review by any other Information Center on the Network.

For Network connected Information Centers, no patient data are stored in the Information Center workstation, except when the Network or Database Server is experiencing a failure. If the Network or Server becomes unavailable for more than 60 seconds, all Information Centers and Clients on the Network reboot and go into **local database mode**. Patient data are temporarily stored in the Information Center workstation but are lost when the system returns to normal operation.

**Information
Center Client**

With Network/Database Server operation, **Information Center Clients** can also be connected to the network as patient data review stations. The Client can display real-time monitoring

data for any patient monitored by any Information Center on the Network and can review any patient's data stored in the Server. The type of access to patient data by a Client (Full Control, Read Only, or No Access) is controlled by the Information Center that sources the data.

The Client has essentially the same performance features as the Information Center except that it cannot be connected to a CareNet switch and does not receive patient data directly from patient monitors. It can be located at cabling distances up to 1,200 m (3936 ft.) from the Network switch to provide patient data review capability at multiple, distant hospital locations. Release E.01 supports the connection of Clients for remote monitoring over a T1/E1 line.

Networks

Information Centers can operate on two different Philips networks -- the Clinical Network and then Philips CareNet.

Philips CareNet The **Philips CareNet** consists of the Philips Serial Distribution Network (SDN) and System Communications Controller (SCC), and Philips CareNet Controller (PCC) which serves as the CareNet switch for transmitting and managing patient data among patient monitors and central stations. A CareNet switch can support up to 24 patient monitors (hardwired or telemetry) and 6 central monitors. Detailed information on the CareNet is provided in the **SDN/PCC Installation and Service Manual**. A CareNet with connection to the Network and Database Server is shown in Figure 1-2.

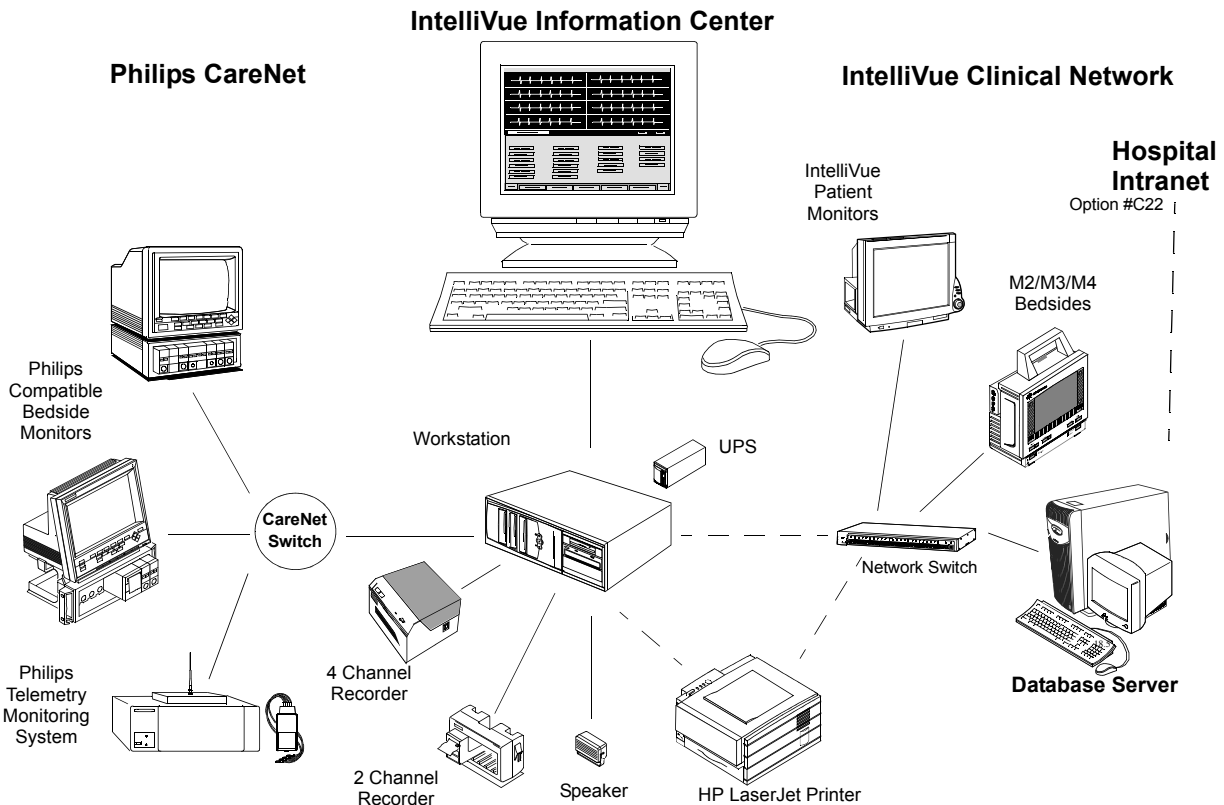


Figure 1-2 CareNet connected to Clinical Network and Database Server

Clinical Network The **Clinical Network** consists of industry standard components and cabling that provide low-cost network installation and maintenance. Up to 8 Information Centers and 8 Information Center Clients can be connected to the Network and at cabling distances up to 1,200 m (3936 ft.) from a Network switch. The Clinical Network can also be used to connect up to 16 IntelliVue Patient Monitors (wired) or M3/M4 patient monitors (wired and wireless) directly to an Information Center.

Standard components for constructing the Clinical Network include the following active components and cabling:

Wireless Access Points connect wireless M3/M4 to the Network. The wireless Access Points can connect to any switch in the Network (Core, Edge, or Extension) using a 10 Mbps Half Duplex connection. They must be spaced at least 3 m (10 ft.) apart. The Access Points used are shown in Figure 1-3.

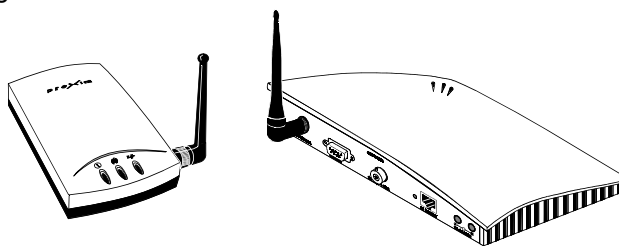


Figure 1-3 Wireless Access Points

Network switches connect Information Centers and Database Servers to the Clinical Network and are industry standard, rack mountable, workgroup switches with RJ-45 ports. The HP2524 switch (Core or Edge) has 24 10/100 Mbit UTP ports and 2 optional 100 Mbit fiber ports. The 10 Mbit ports connect to M2/M3/M4s, IntelliVue Patient Monitors, Access Points, and Printers. The 100 Mbit ports connect to Information Centers, Clients, Application Servers, Database Servers or another Network switch. See Figure 1-4. The Extension switch (available in limited geographies) has 8 10/100 Mbit UTP ports for connecting small clusters of devices to either a Core or Edge switch.

Network cabling for interconnecting devices can be industry standard, UTP Category 5 cable or 62.5/125 micron, multimode, fiber optic cable. UTP cable (orange colored) is available from Philips in bulk and in several patch cable lengths. Fiber optic patch cables are also available from Philips Medical Systems.

Media translators interconnect UTP and fiber optic cable for extending cable distances to 1000 m (3280 ft.) from a Network switch. See Figure 1-4.

Patch panels and wall box kits provide for interfacing devices to the network. 24 port patch panel kits and dual and quad wall box and surface mount kits with UTP, Category 5, RJ-45 terminations are available for US installations. Single UTP wall box kits are available for non-US installations.

Active Network components - switches, repeaters, media translators - are shown in Figure 1-4.

Note Specific switches, media translators and access points shipped with systems may vary with date of purchase as newer models are substituted when they become available. Throughout this Manual, only general descriptions of devices that are subject to change is provided. For more detailed information, refer to the device manuals.

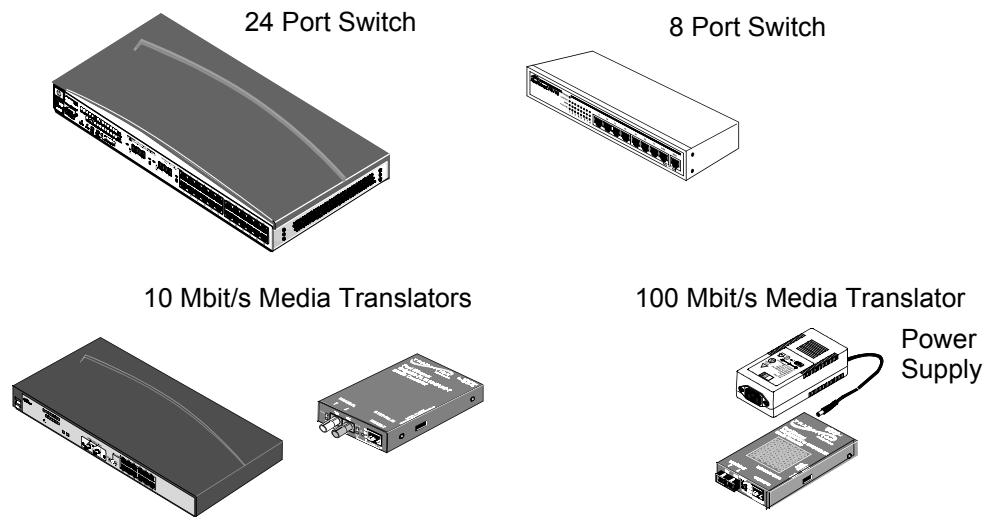


Figure 1-4 M3185 Clinical Network Components

Patient Care Systems

Using the capabilities of the Clinical Network and Database Server, Philips Patient Care Systems can be designed to meet a wide range of clinical monitoring requirements. Examples are given below -- a relatively simple system using wired and wireless M3/M4 and IntelliVue Patient Monitors (Figure 1-5), the Network and a relatively complex system showing full Patient Care System capabilities (Figure 1-6), and a Network using the Small Database Server (Figure 1-7).

Clinical Network Without a Database Server A Patient Care system using the **Clinical Network** to connect M3/M4 (wired and wireless) and IntelliVue Patient Monitors to an **Information Center** is shown in Figure 1-5. In this application, the Clinical Network supports 1 Information Center, 1 Application Server, 2 LaserJet Printers and 16 patients. The Database Server is not required in this application.

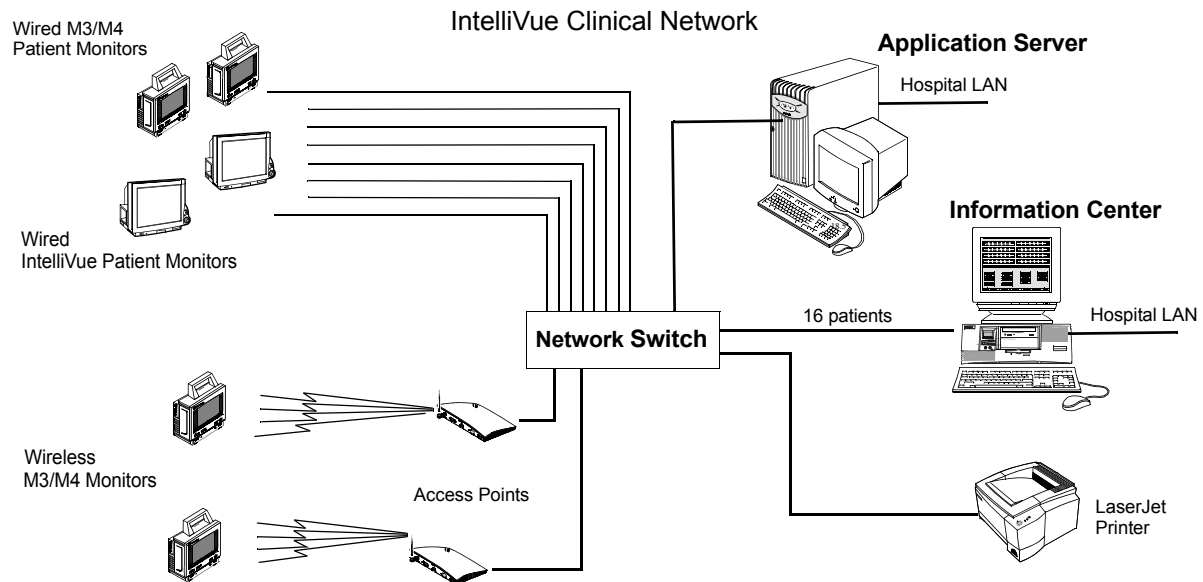


Figure 1-5 Clinical Network with Patient Monitors, Information Center and Application Server

Clinical Network With IntelliVue Database Server A Patient Care System using the **Clinical Network and IntelliVue Database Server** is shown in Figure 1-6. Patient monitoring data from Philips bedside monitors -- CMS, 24 -- and telemetry monitors are transmitted to **Information Centers** via the CareNet switch. Data from Information Centers are transmitted to the Server via Network switches where they are stored. The Server can store up to 96 hours of patient data for up to 128 monitored patients, 16 max per Information Center, and 32 transfer patients. This Network system can support 1 Application Server, up to 8 Information Centers, 8 Information Center Clients, and 8 LaserJet Printers.

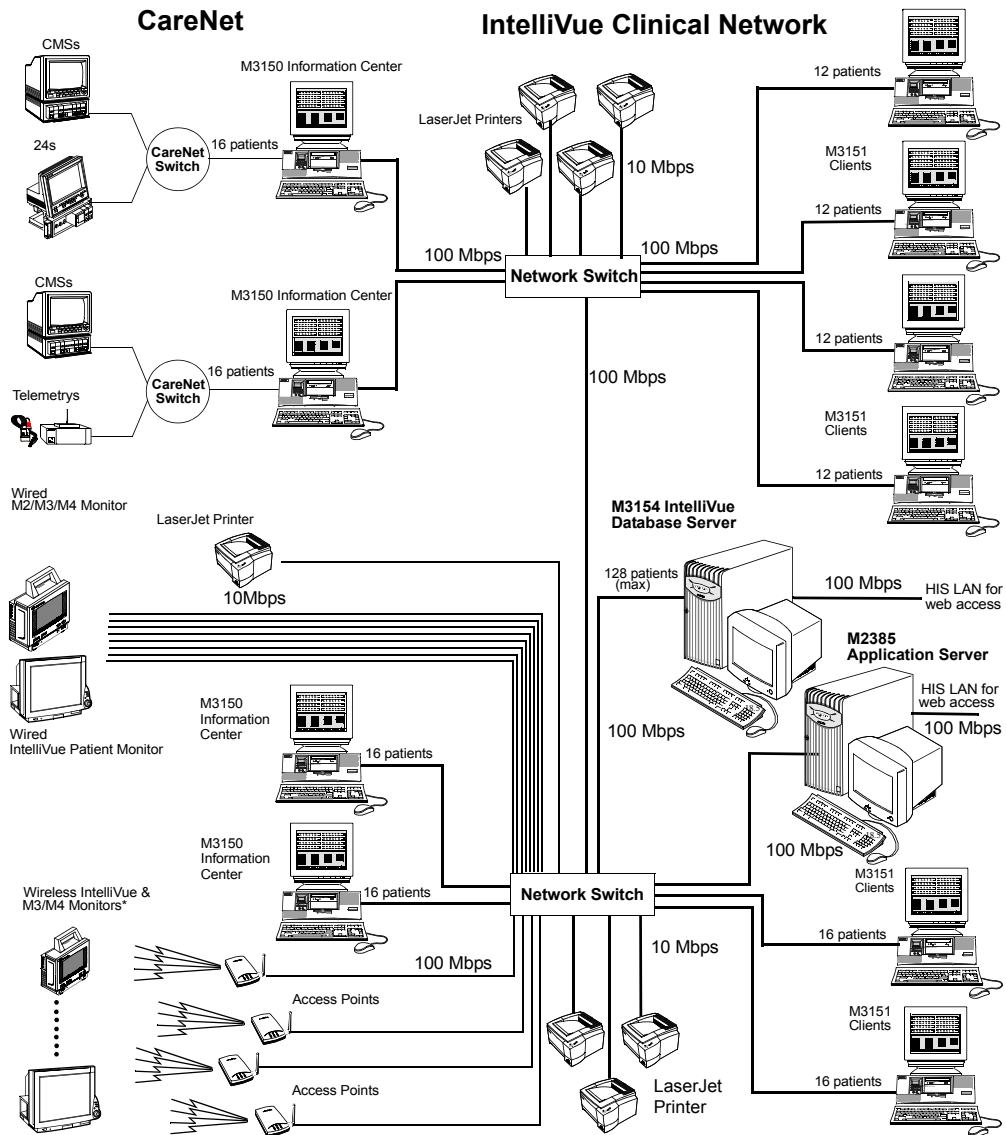


Figure 1-6 Clinical Network with IntelliVue Database Server

Up to ten **M3154 Database Servers** systems can be interconnected on the hospital LAN. This connectivity provides Information Centers with the ability to transfer patient data to a clinical unit outside of its Database Server. Retrospective data, near real-time waves, parameters, and alarms for patients across care units that are on separate database servers can also be reviewed. If a **M2385 Application Server** is present, web-based applications can be displayed on the Information Centers.

Clinical Network With IntelliVue Small Database Server A Patient Care System using the **Clinical Network and the IntelliVue Small Database Server** is shown in Figure 1-7. Patient monitoring data from Philips bedside monitors -- CMS, 24 -- and telemetry monitors are transmitted to **Information Centers** via the CareNet switch. Data from Information Centers are transmitted to the Server via Network switches where they are stored. The Server can store 48 hours of patient data for up to 48 monitored patients, 16 max per Information Center, and up to 12 transfer patients.

This Network system can support 1 Application Server, up to 3 Information Centers, 3 Information Center Clients, and 4 LaserJet Printers.

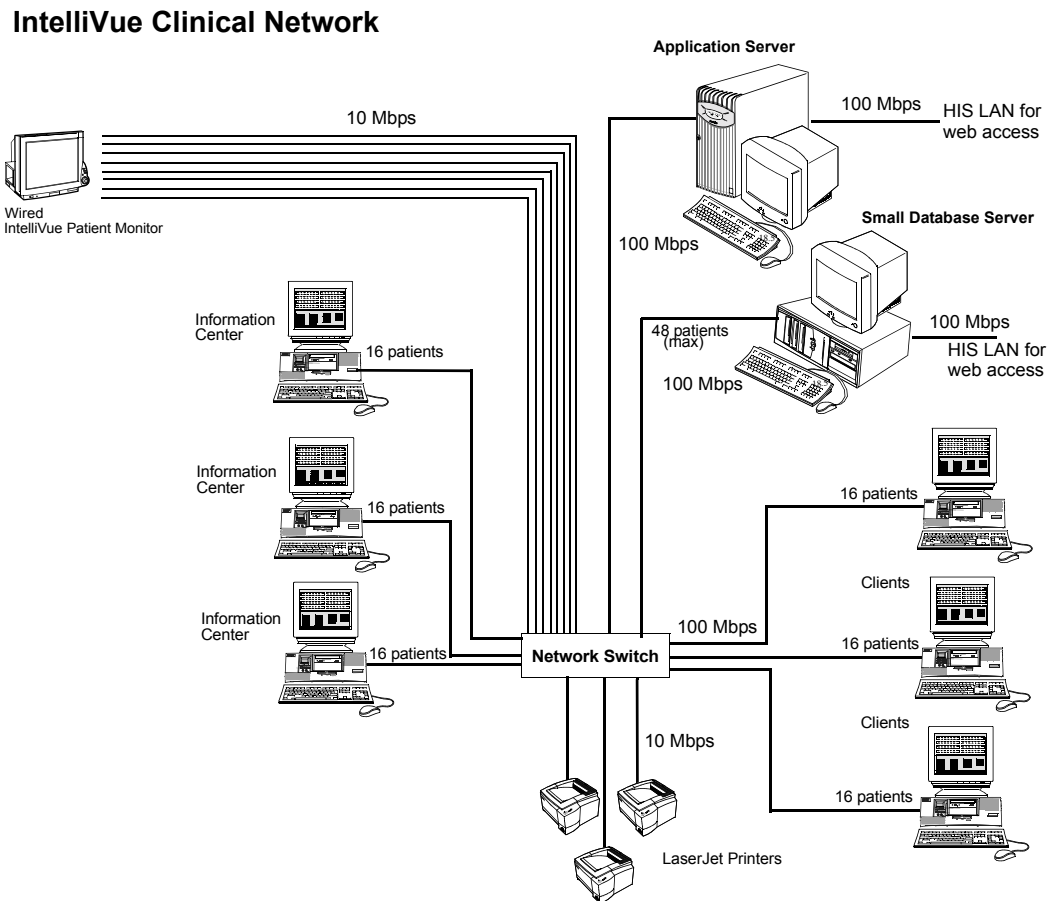


Figure 1-7 Clinical Network with IntelliVue Small Database Server

**M3185
Clinical
Network**

The **Clinical Network** provides networking capability for sharing patient monitoring data -- real-time and stored -- among all Information Centers and Clients connected to the Network.

Switches Communication and data transfer among devices on the Network is managed by network switches.

Network Connections Network connections **between Information Centers, Clients, Application Servers, Database Servers and the switches** are **100 Mbps**. 10/100 Mbit/s interface cards in these devices provide the Network connections.

Extended Distances **Extension Switches, fiber optic cable, and media translators** permit Network devices to be located at widely separated places in the hospital. Hence, patient monitoring data can be made available to many clinicians both within and outside the clinical environment.

The following design rules govern point-to-point cable distance capabilities and limitations between Network devices. See **Figure 1-8**.

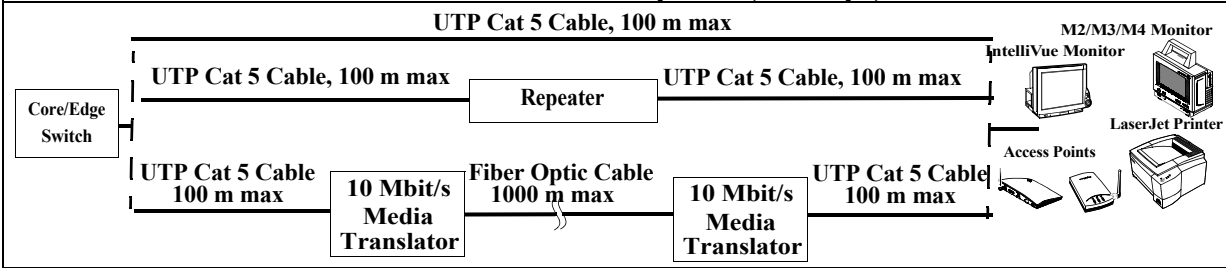
- Switch to wired M3/M4 monitor, wired IntelliVue Patient Monitor, Access Point, and LaserJet Printer (10 Mbps connection)

Note All lengths assume 2 patch cables (< 5 m each) and a single cable length in between is used. So single length = patch cable + other cable + patch cable.

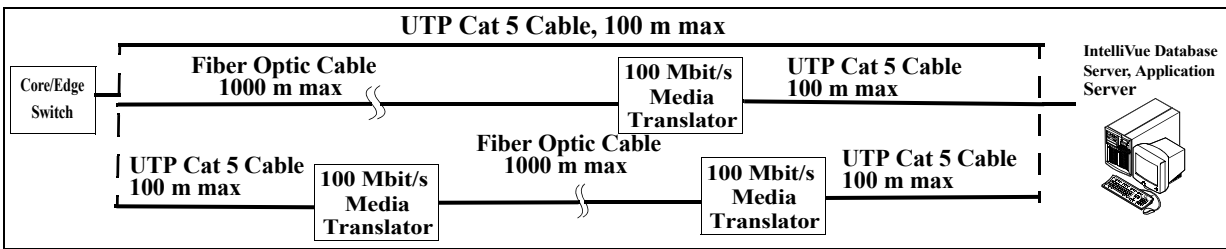
- Switch to Information Center/Client (100 Mbps connection)
- Switch to Database Servers (100 Mbps connection)
- Switch to Application Server (100 Mbps connection)
- Switch to Switch (100 Mbps connection)

These connections are described in detail in **Chapter 3**.

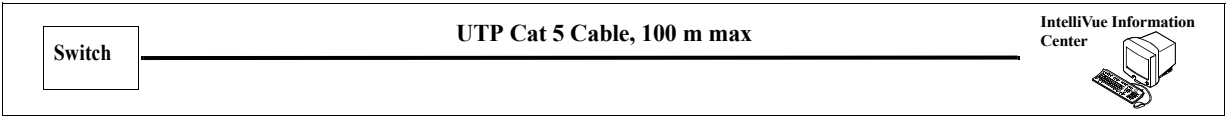
Switch to Network Device Options (10 Mbps)



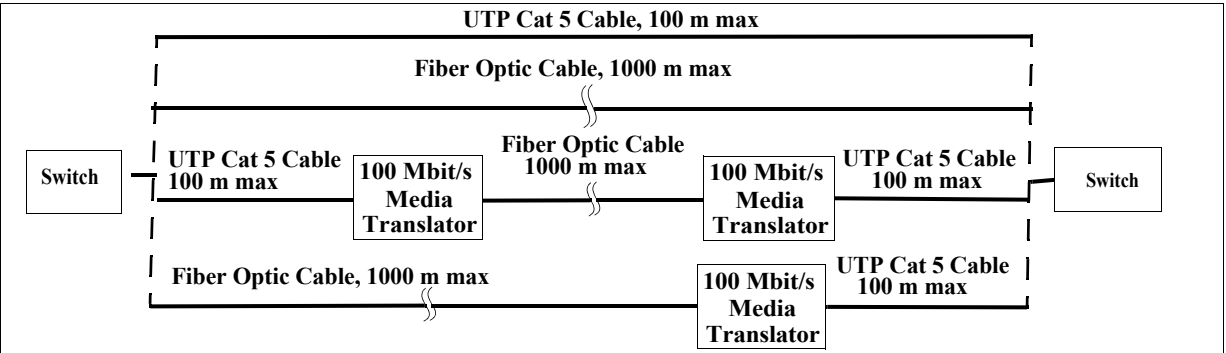
Switch to Network Device Options (100 Mbps, FULL Duplex)



Switch to Network Device Options (100 Mbps, HALF Duplex)



Switch to Switch Options (100 Mbps)



Switch to Access Point Controller Option

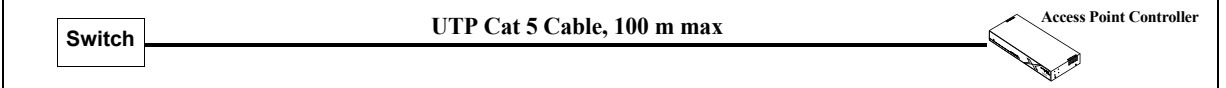


Figure 1-8 M3185 Network Point-to-Point Cable Distance Options

Components and Options

Clinical Network systems can include the Information Center and Information Center Client, the IntelliVue Database Server, IntelliVue Small Database Server, Application Server, and a selection of switches, media translators, and cabling.

The following components are available for the M3185 Clinical Network

Active Components

Table 1-2. Active Components for M3185 Clinical Network

Option	Description
862084	High Density Managed Switch (Core/Edge)
862085	Low Density Unmanaged Switch (Extension Switch)
862086	10 Mbit/s UTP repeater
989803131221	100-FX SC Transceiver (Fiber Port) for the 862084 Switch
862088	10 Mbit/s media translator pair
862089	100 Mbit/s media translator
862105	Harmony Access Point Controller
862092	Harmony Access Point
862093	Remote Power Supply
989803131231	AP Power over LAN Module
862095	Bedside Wireless LAN Adapter

Purchased Options

Table 1-3. Purchased Option for M3185 Clinical Network

Option	Description
862099	650 VA UPS

Cabling Installation Materials

Cabling installation materials are ordered under Product # M3199AI.

Table 1-4. M3199AI Passive Components for M3185 Clinical Network

Option	Description
UTP Cable	
P01	305 m (1000 ft.) Unshielded Twisted Pair (UTP) plenum cable (Cat. 5, Orange)
Patch Cables	
J10	0.9 m (3 ft.) UTP Patch Cable
J11	2 m (7 ft.) UTP Patch Cable
J12	3.7 m (12 ft.) UTP Patch Cable
J20	3.7 m (12 ft.) UTP Crossover Cable
J21	0.9 m (3 ft.) UTP Crossover Cable
J30	3.0 m (9.8 ft.) Fiber Optic Patch Cable - ST/ST

Table 1-4. M3199AI Passive Components for M3185 Clinical Network

Option	Description
J31	3.0 m (9.8 ft.) Fiber Optic Patch Cable - SC/SC
J32	3.0 m (9.8 ft.) Fiber Optic Patch Cable - ST/SC
Patch Panel Kits	
A01	24-Port Patch Panel Kit
A05	Patch Panel Wall Mount Kit
Wall Box Kits	
A10	Dual Port, single gang, RJ-45 UTP Wall Box Kit (US only)
A11	Dual Port, single gang, RJ-45 UTP Surface Mount Kit
A12	Quad Port, dual gang, RJ-45 UTP Wall Box Kit (US only)
A13	Quad Port, dual gang, RJ-45 UTP Surface Mount Kit

Mounting Options

The following **mounting options** are available for Network Components.

The following options are ordered under Product # **M3180A**.

Table 1-5. M3180A Mounting Options for the Clinical Network

Option	Description
A22	Harmony Access Point Steel Enclosure Kit

Hardware Description

Overview

Clinical Network support personnel should be familiar with Local Area Network (LAN) hardware and cabling. Only brief descriptions of these subjects are given in this manual.

Chapter 2 overviews the Clinical Network hardware in the following sections:

System Components	page 2-2
Specifications	page 2-22
Regulatory	page 2-26

System Components

Hardware components of the Clinical Network are primarily industry standard equipment tailored to LAN applications.

These hardware components can change frequently as newer models with improved cost and performance specifications become available. Therefore, this section provides only general descriptions of the Clinical Network hardware and illustrates typical units supplied at the date of the manual's printing.

Documentation on specific units shipped with customer orders is included with the unit.

Warning

Components, topologies, and configurations specified by Philips have been optimized and tested to meet a variety of patient monitoring standards. Hardware and software products not supplied by Philips as part of an Information Center system are not approved or supported by Philips for use with Information Center and Clinical Network/ Database Server systems.

Active hardware components for the Clinical Network include the items listed in “**Active Components**” on page 1-12. These are described in the following sections.

Warning

Refer to Chapter 3 for which active Clinical Network components must be connected to a UPS to assure continuity of operation during brief electrical power interruptions.

Core/Edge Switches

24-port Network Switches are used to route patient monitoring data among the devices on the Clinical Network. It “reads” incoming data from network devices -- Patient Monitors, Information Centers, the Server, another Switch -- and routes them to their destination devices -- other Information Centers, the Server, Printers. The HP ProCurve 2524 (J4813A) switch used is rack mountable. Its front panel has 24, 10/100 MBit/s RJ-45 port connections, two slots for installing supported 100Base-FX transceivers (for fiber optic cable (SC connector)), and a DB9 Console port for configuring the switch. The rear panel contains an ac power supply connection, and a cooling vent outlet. Its internal power supply is auto switching to AC input voltages of 100 - 127V and 200 - 240V. See Figure 2-1.

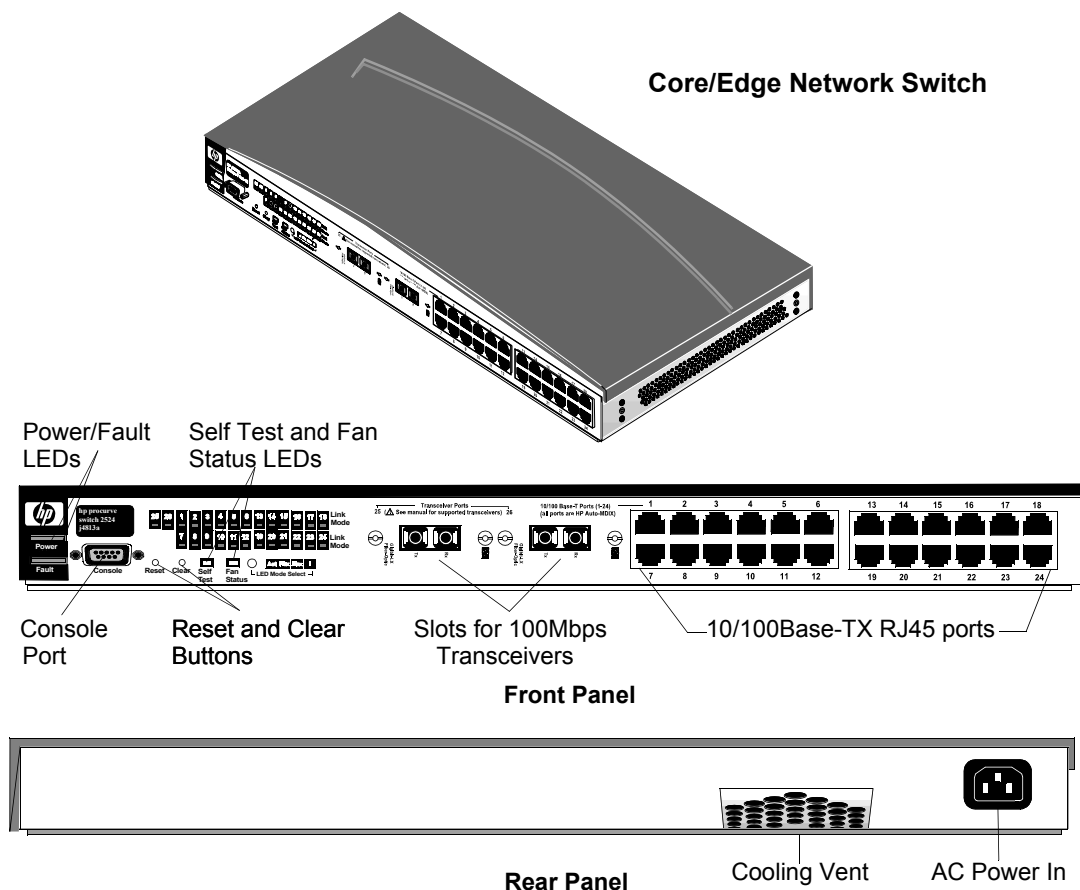


Figure 2-1 24 Port Core/Edge Network Switch

If the system has been upgraded from an earlier release, the Cisco 1900 switch can only be used as an Edge switch to connect 10 Mbps devices. The rules and guidelines for this are given in “Upgraded Systems” on page 3-11.

Extension Switch/ Repeater

An **Extension Switch** is used to allow small clusters of devices to be connected to the system from a remote location. Up to seven devices can be connected to the Extension switch. There is no maximum number of Extension switches specified per system.

A **repeater** is used to extend the distance for UTP cable between a switch and any 10Mbit Network device (Refer to Chapter 3 for details). The maximum standard CAT5 length of a single, continuous, UTP cable is 100 m (328 ft.). A maximum of 1 repeater can connect 2, continuous-length 100 m cables to achieve a total cabling distance of 200 m (656 ft.) between a Switch and any Network device.

The Switch has 8 UTP ports. Networked Devices are connected to the first 7 ports and the Network Switch is connected to Port 8MDI. The Allied Telesyn AT-FS708 switch is used for the Extension switch. See Figure 2-2.

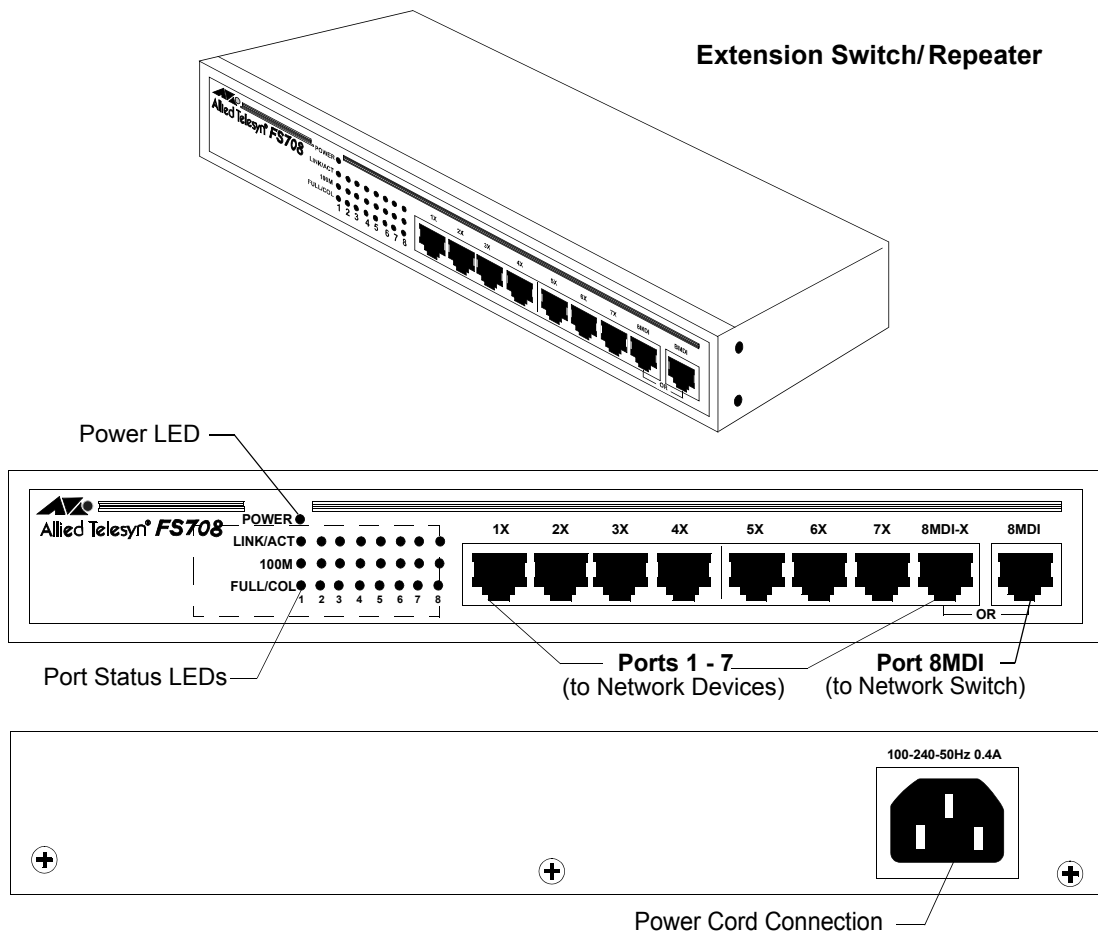


Figure 2-2 Network 8-Port 10/100 Mbit/s Extension Switch & Repeater

Wireless Access Points

Wireless Access Points provide the interface between wireless IntelliVue/M3/M4 Patient Monitors and the Clinical Network. Access Points must be spaced at least 3.0 m (10 ft.) apart.

The Harmony Access Point is shown in Figure 2-3 along with rear panel connections and LED indicators. An external 12 VDC (1.2 A) power supply (included) is required to provide power. The power supply can accept AC input voltages in the range of 100 - 250 VAC. Power to the Harmony Access Point can also be provided via the Remote Power System, in this case, the power supply is not included. Harmony Access Points require an Access Point Controller on the network.

Warning

The Harmony Access Point must be operated at least 15 cm (6 inches) from any person. This is necessary to insure that the product is operated in accordance with the RF Guidelines for Human Exposure.

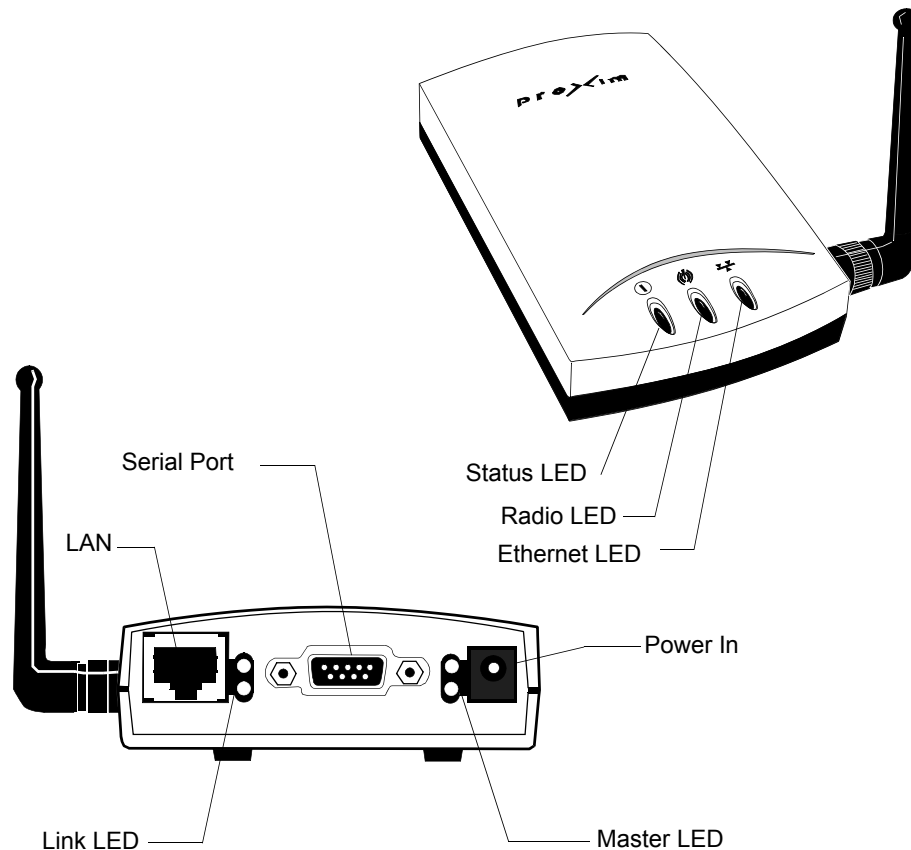


Figure 2-3 Harmony Wireless Access Point

The Harmony Access Point LAN port requires a crossover cable as shown in Figure 2-4. If a crossover cable is not available, a crossover adapter that is shipped with the Harmony Access Point can be used to support this requirement. See Figure 2-5.

Access Point Controller

The **Access Point Controller** provides management, filtering, and security services for the Harmony Access Points and status information for the RangeLAN2 Access Points in the Clinical Network. The Access Point Controller (Figure 2-6) allows for single point system-wide updates to all the Harmony Access Points on the network through the controller's web interface.

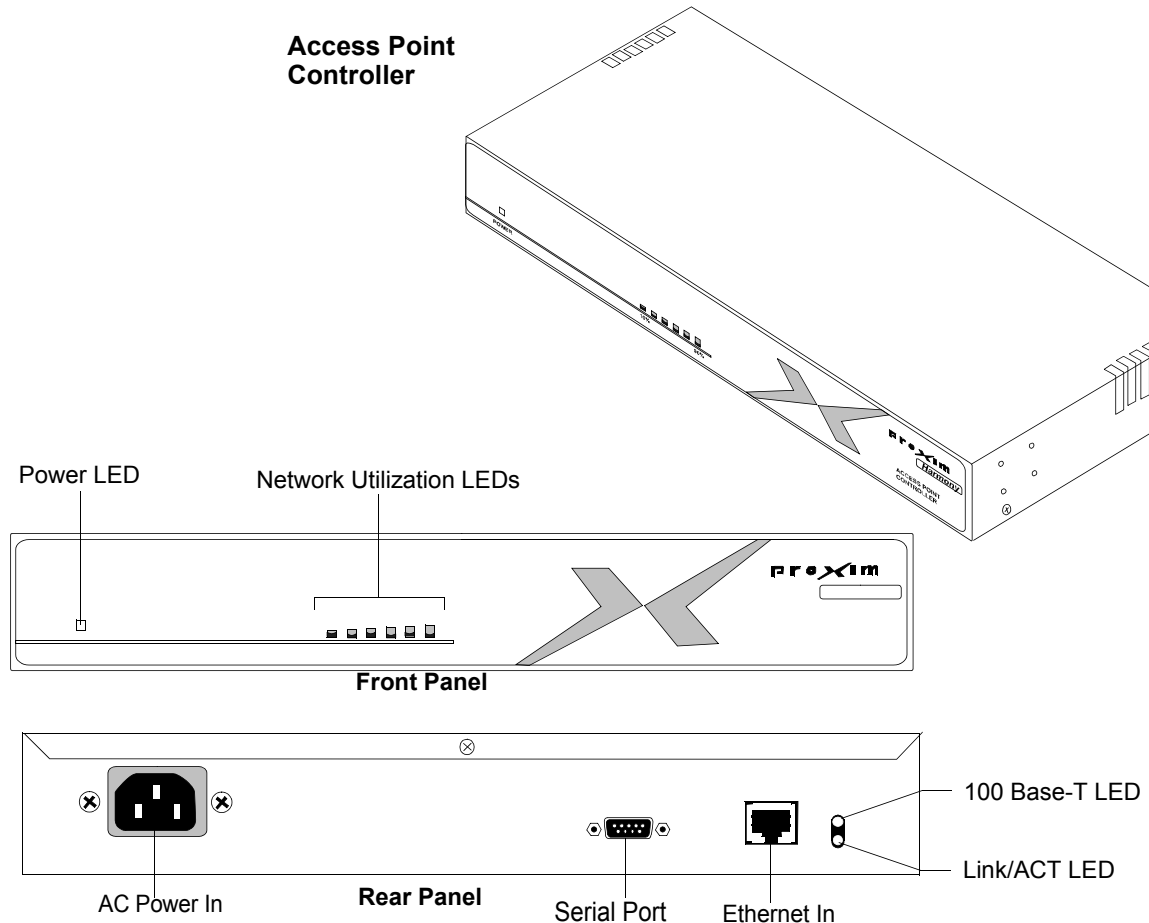


Figure 2-6 Access Point Controller

Remote Power System

The **Remote Power System** provides remote DC power to Harmony Access Points over standard Category 5 twisted pair ethernet cables eliminating the need for AC outlets, UPS and AC/DC Adapters for the Access Points. The Power System (Figure 2-7) connects to a PowerDSine Power Over LAN module (Figure 2-8) which connects to the Harmony Access Point.

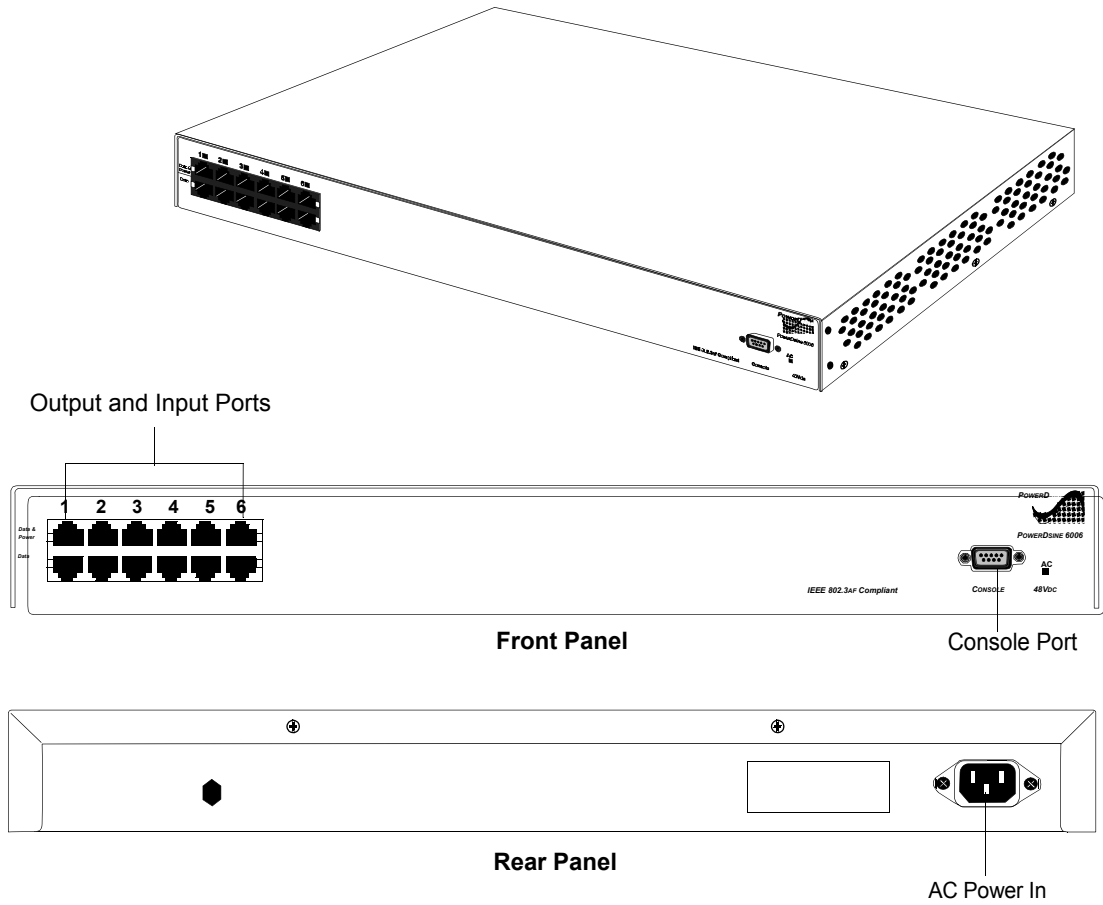


Figure 2-7 Remote Power System

AP Power Over LAN

The **AP Power Over LAN module** (Figure 2-8) connects to the Harmony Access Point to the Remote power System (Figure 2-7). Figure 2-9 shows a Power System component connection diagram.

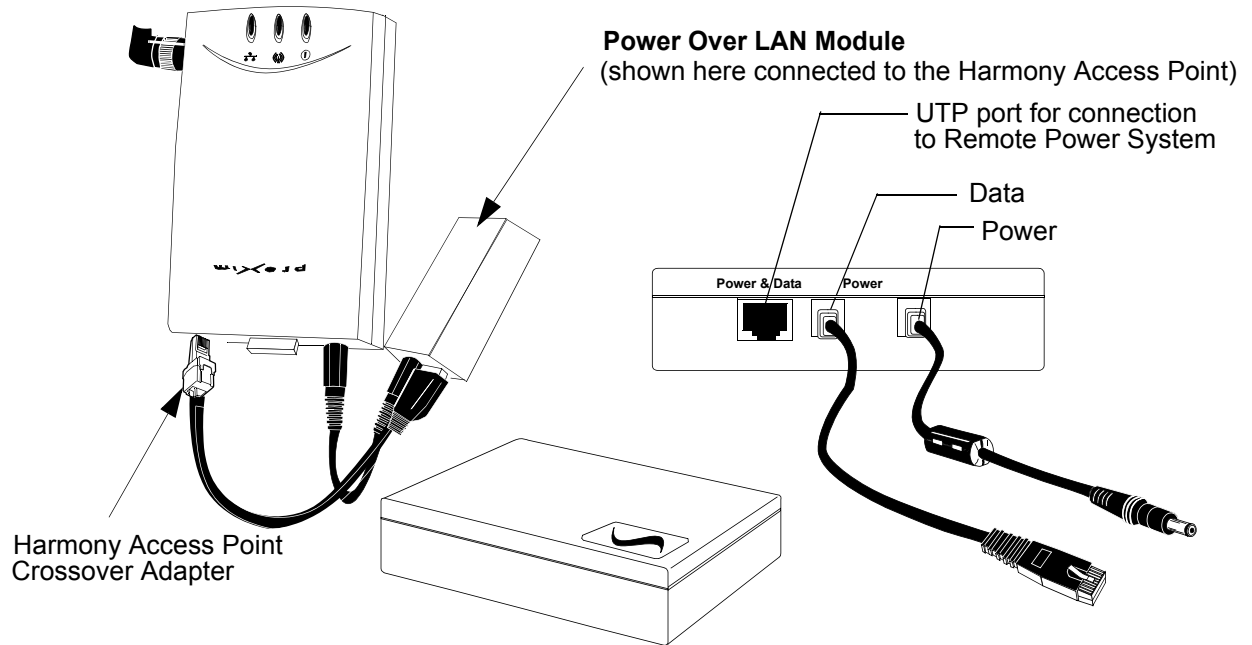


Figure 2-8 AP Power over LAN Module

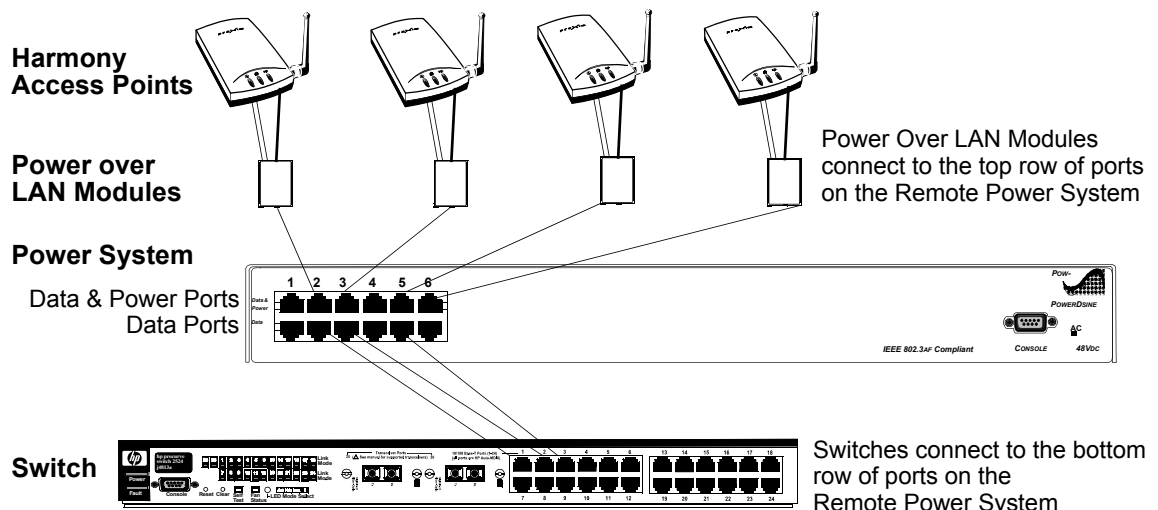


Figure 2-9 Harmony Power System Overview

Wireless Bedside Adapter

The Wireless Bedside Adapter is shown in Figure 2-10 along with rear panel connections and LED indicators. Mounting of this adapter to the IntelliVue Patient Monitor is shown in Figure 2-11

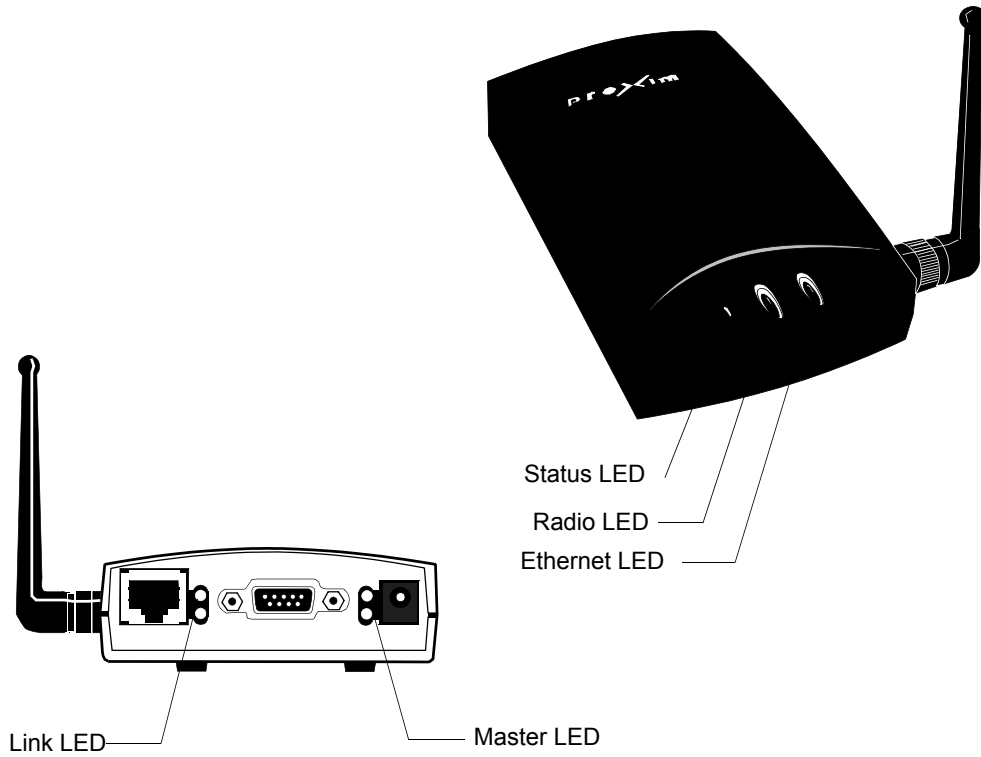


Figure 2-10 Wireless Bedside Adapter

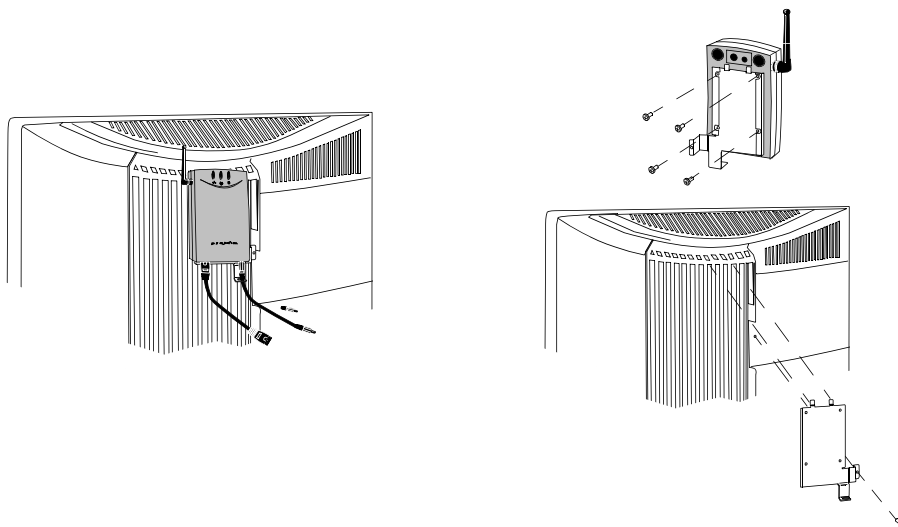


Figure 2-11 Wireless Bedside Adapter Mounting

Media Translators

Media translators are used to interconnect UTP and fiber optic cable. Fiber optic cable permits significantly longer cabling distances than UTP and greater immunity from noise. Continuous fiber optic cable lengths can be 1,000 m (3,280 ft.). Refer to **Figure 1-8** as well as **Chapter 3** for descriptions and an overview of how and where the Media Translators are used.

Note The maximum number of Media Translators in series is 2.

One of the supported 10 MBit/s Media Translator is the E-TBT-FRL-05 model manufactured by TRANSITION Networks and shown in **Figure 2-12**. It is compatible for use in IntelliVue Clinical Networks for all 10 Mbit/s devices. Rear and Front Panels are shown in **Figure 2-13** and **Figure 2-14** respectively. An External Power Supply provides power to the device through a rear panel connection as shown in **Figure 2-13**.



Figure 2-12 10 MBit/s Media Translator

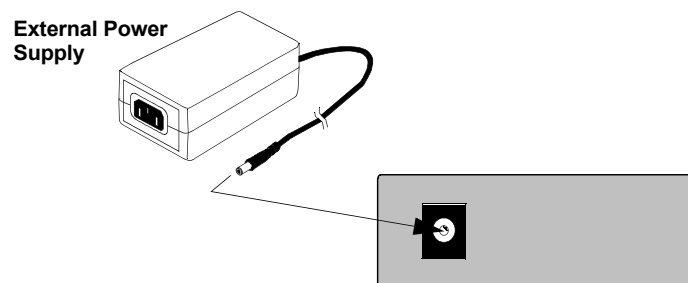


Figure 2-13 Rear Panel of the 10 MBit/s Media Translator

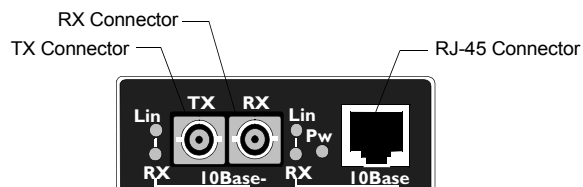


Figure 2-14 Front Panel of 10Mbit/s Media Translator

The front panel contains a female, 10-Base-T RJ-45 connector for connecting the UTP cable and female, 10Base-FL TX (transmit) and RX (receive) connectors for connecting the fiber optic cable. The Media Translator allows either straight through or crossover cables to be used. The

unit determines the characteristics of the cable connection and automatically configures to link to straight through or to crossover cable.

The **LinkALERT** feature is set to **Disable** to allow troubleshooting of device-to-device connectivity using the Link LEDs.

Note The LinkALERT switch on the side of the unit must be set to **Disable**. See Figure 2-12.

The other supported **10 Mbit/s media translator pair** is the HP J3300A with an HP J2606A fiber transceiver installed in its AUI front panel port. The transceiver permits the device to serve as a 10 Mbit/s media translator with one front panel RJ-45 port as the UTP connection and the transceiver as the fiber optic connection. See Figure 2-15.

Caution Only one input port and one output port can be used with this Media Translator.

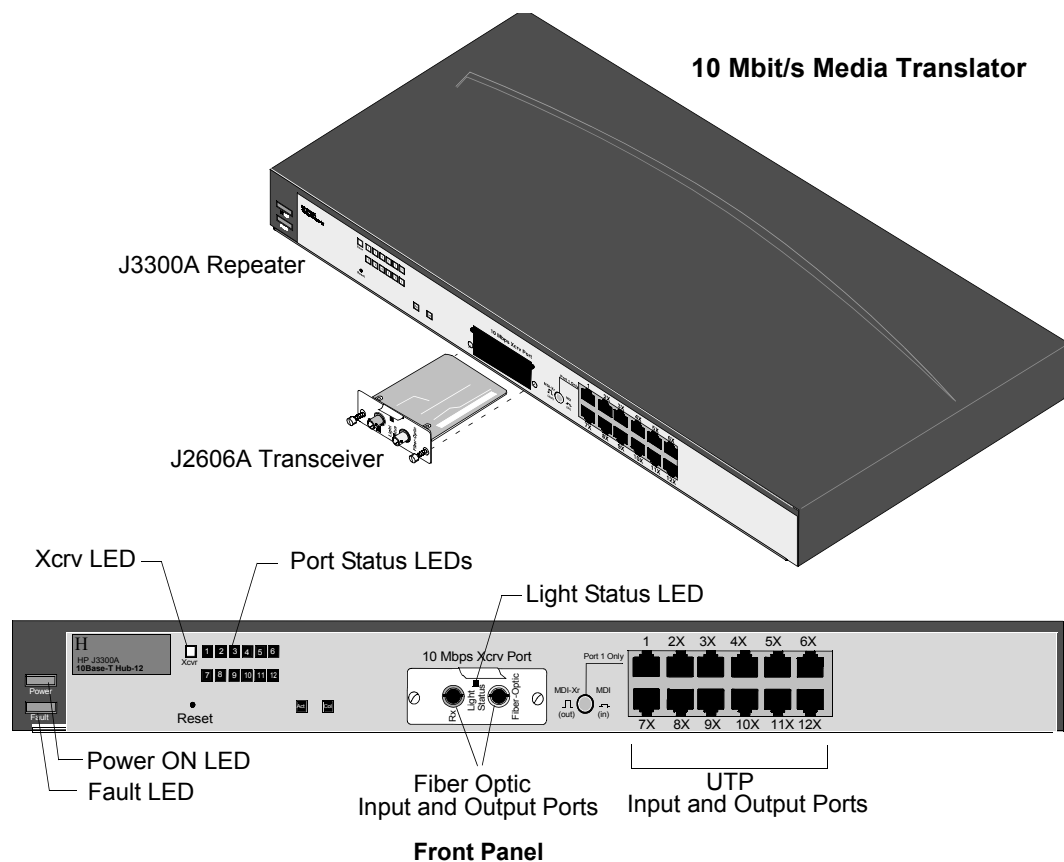


Figure 2-15 J3300 10 Mbit/s Media Translator

The **100 Mbit/s media translator** connects UTP and fiber optic cable between two switches or between the Core Switch and the Database Server. The device used is the Transition Networks 100BASE-TX/100BASE-FX Media Converter, which provides an RJ-45 twisted pair 100Base-TX connector and an RX and TX SC 100Base-FX connector to 1300 nm multimode fiber optic cable. It is shown in Figure 2-16 along with its front and rear panel connections and side panel switches. Configuration switches on the side of the unit are used to set the required duplex settings (see below). An external 9 VDC (.55A) power supply (included) is required to provide power. The power supply can be set to input voltages of either 100-120 VAC or 220-240 VAC with a switch.

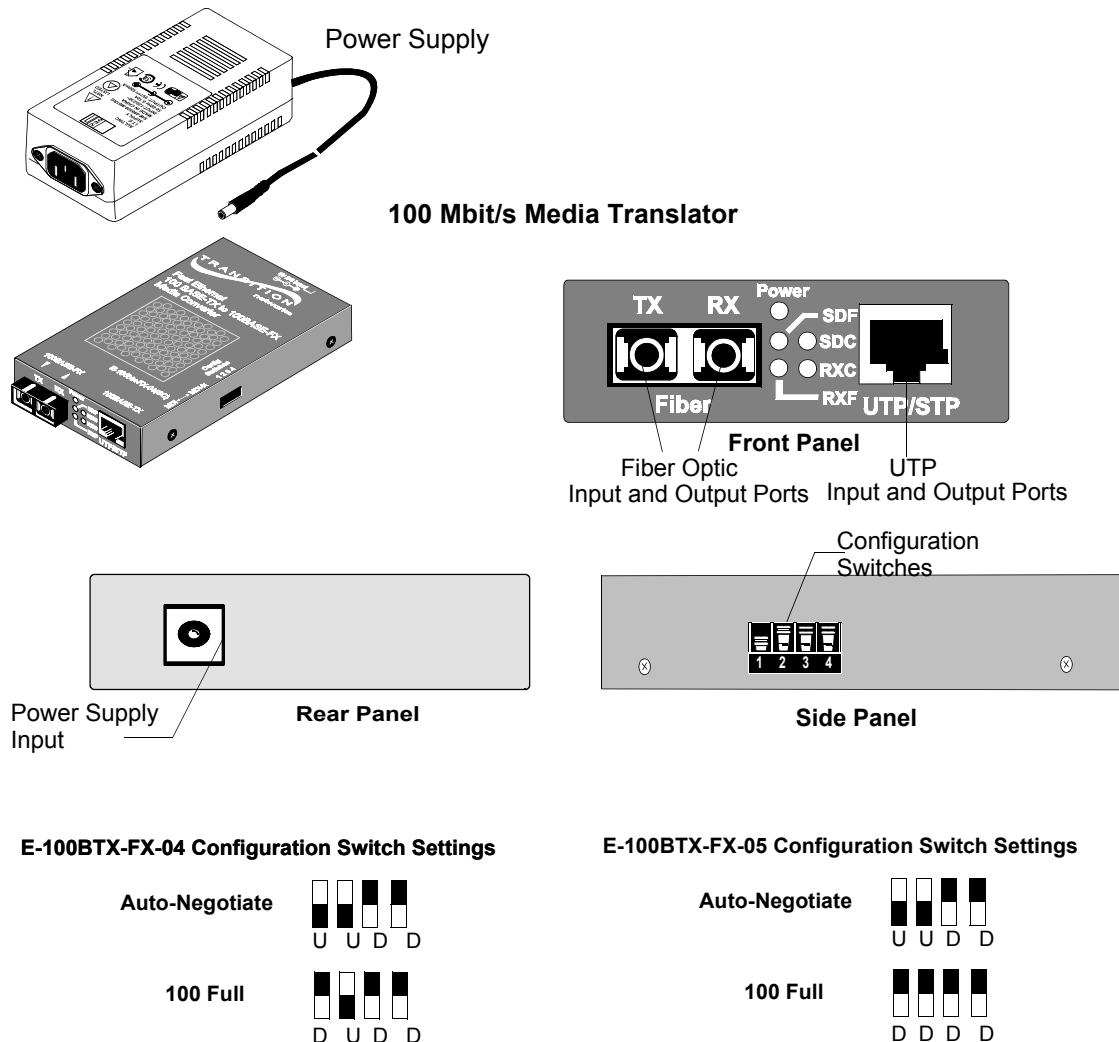


Figure 2-16 100 Mbit/s Media Translator

Printer

An **HP LaserJet Printer** with connectivity to the Clinical Network (Option M3159A #A02) is available for printing patient and configuration data. See Figure 2-17. The Printer is connected to a Switch port via a 10 Mbit/s, UTP cable. It is a 10 Mbit connection. See Figure 1-8.

The Network connection is made via a Jet Direct card, (included with Option M3159A #A02), it is installed in the rear right side of the Printer. See Figure 2-17, where the RJ-45 port and AC power connector are also shown.

Warning

Do not use any other printers or printer drivers.

Note

For additional information on Printer performance, see the Printer's documentation manual and the **HP LaserJet Quick Reference Service Guide**.

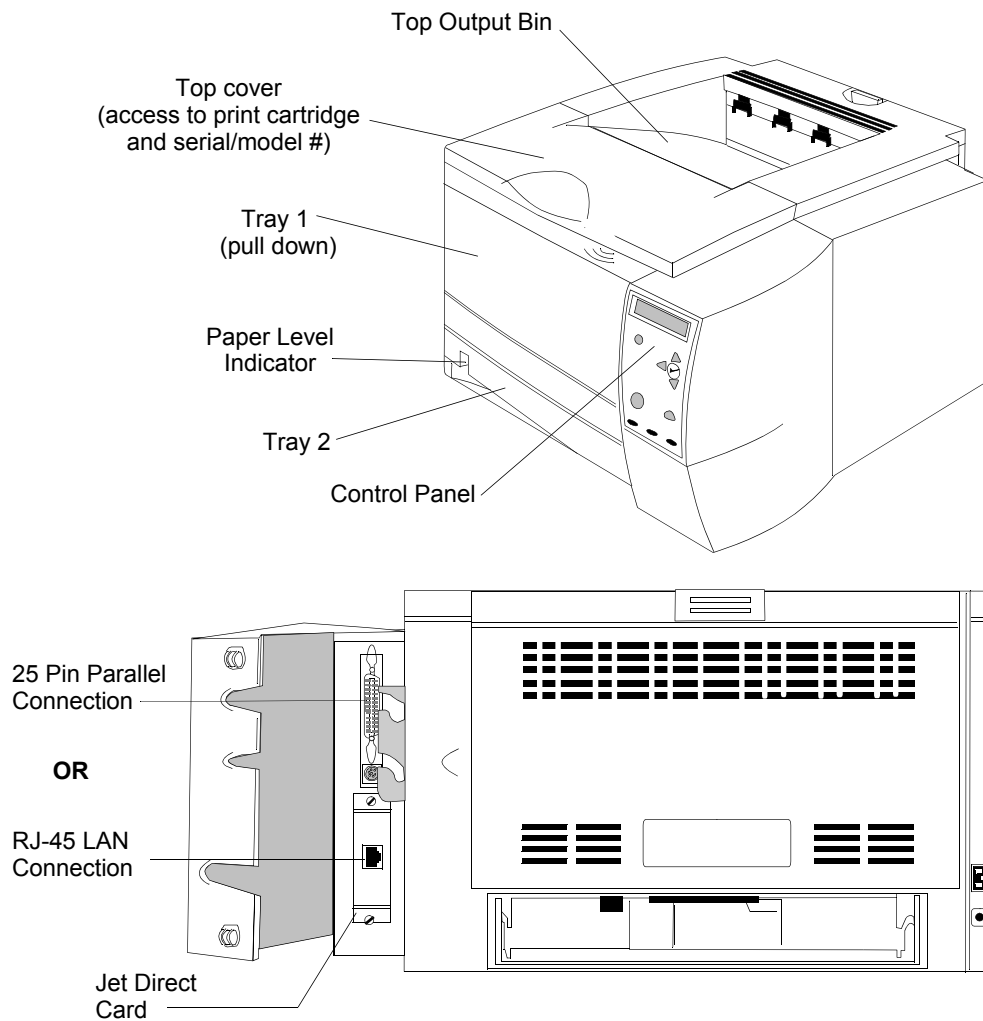


Figure 2-17 HP LaserJet 2300 Printer

Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) is available as an option for Network devices. Its purpose is to provide up to 90 seconds of battery power to maintain system operation and eliminate time consuming software rebooting during short power transitions.

Warning

UPSs are shipped without their internal battery wire connected. Before use, the battery wire must be connected.

Only Voltage Outputs labeled BATTERY BACKUP should be used for UPS protection.

The **UPS for Network devices** is **650 VA** and it comes in 2 versions -- 100-127 VAC (50-60 Hz) and 220-240 VAC (50-60 Hz). The versions look similar and are shown in Figure 2-18 along with typical front and rear panels.

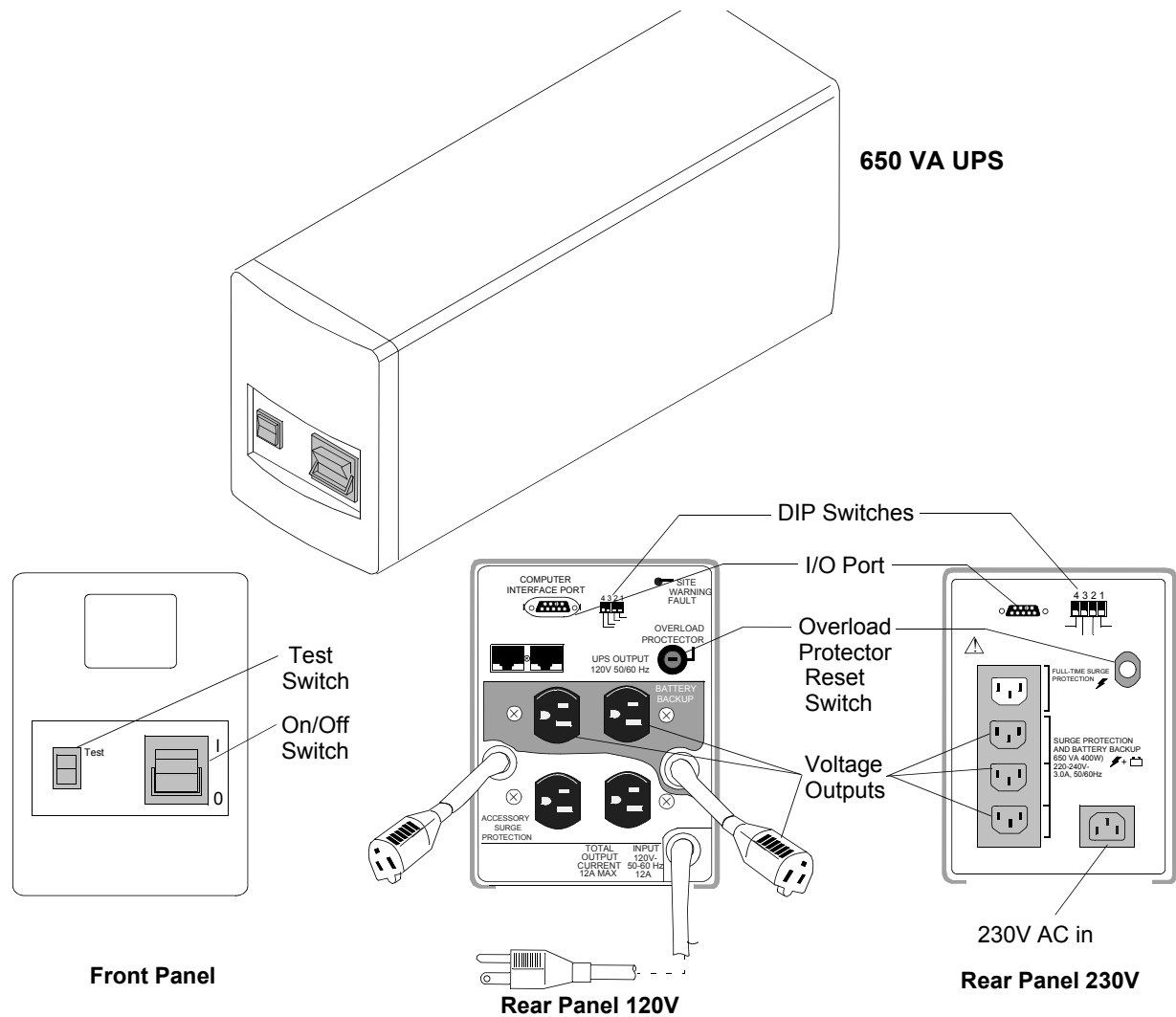


Figure 2-18 650 VA UPS for Network Components

650 VA UPSs have rear panel DIP switches that must be set in specific positions for the UPS to operate properly. The correct dip switch settings for 120V and 230V models are shown in Figure 2-19.

Notes The switch settings of Figure 2-19 **must be made** during installation since they are shipped with all switches on OFF (down).

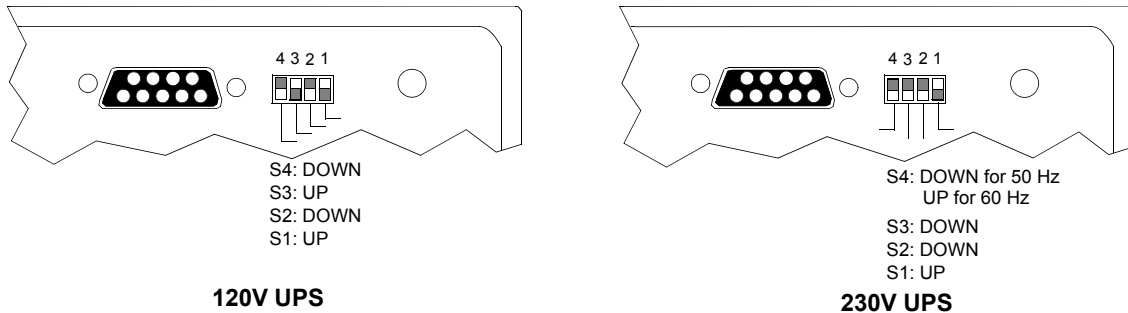


Figure 2-19 Rear Panel DIP Switch Settings for 120V and 230V UPSs

Operation The operation of a UPS after power failure is as follows.

Seconds after power failure	Action
0	Line power fails and UPS goes to battery power. Philips systems continue to run, but displays will be blank (no power). If line power returns during this period, normal operation is restored automatically.
90	The Operating System begins a system shutdown and Philips application software ends.
120-150	The UPS shuts off power to the device. The UPS then typically beeps every 5 seconds until power is restored or the UPS is turned off. When line power is restored, the UPS automatically supplies power to the device. If line power is restored between 90 and 120-150 seconds after power failure, the system shutdown completes and the computer is powered off. The following English language message will appear. It is now safe to turn off your computer. Clicking on RESTART initiates a software boot cycle, after which normal Information Center operation resumes.

Warning After 150 seconds, Information Centers, Clients, and the Server must be manually restarted following proper restart procedure.

Note Power failure and restoration messages will also appear in the **Event Log**.

M3185 Cables and Installation Materials

Passive hardware components for the Clinical Network include UTP and fiber optic patch cables, a variety of RJ-45 wall boxes, and a 24-port patch panel for interconnecting wires. These are described in the following sections.

UTP Cable Network signals are transmitted primarily on **Unshielded Twisted Pair (UTP) Category 5 (CAT5) cable** (orange colored). UTP CAT5 cable is regulated by the Computer Communication Industry Association (CCIA) according to standards developed by the Electronic Industries Association (EIA) and the Tele-communication Industries Association (TIA). These standards, EIA/TIA 568A, were first published in 1991 and their purpose is to specify generic telecommunication cabling systems to support a multiproduct, multivendor environment and provide direction for commercial telecommunication product design.

Category 5 is one of the EIA/TIA 568A standards and is limited to runs less than 90 meters (295 ft.) from the telecommunication closet patch panel to the outlet wall box. It can handle data transmission rates up to 100 Mbit/s and has an impedance of approximately 100 ohms.

Category 5 UTP cable consists of 4 pairs of unshielded, 24 AWG solid copper wires with Polyolefin or Fluorinated Ethylene Propylene (FEP) jackets contained in a plenum rated PVC sheath. The 4 pairs of wires are color coded in pairs as shown in Figure 2-20 with a major color (blue, orange, green, brown) paired with white as **PRIMARY** colors and **stripes**. The pairs are also numbered -- **1, 2, 3, 4** -- as shown in Figure 2-20.

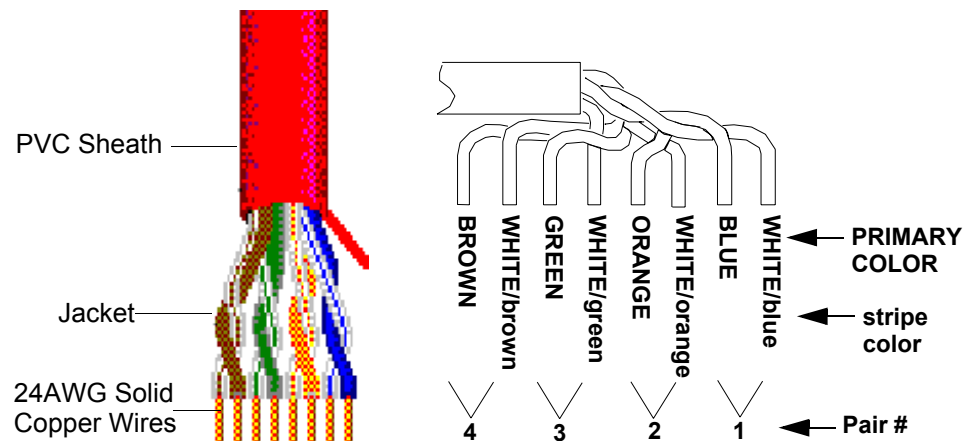


Figure 2-20 UTP Category 5 Cable Showing Wire Pairing

CAT5 cable is compatible with either the 568A or 568B wiring standards for RJ-45 connectors and jacks. Figure 2-21 shows the pairing scheme and signal assignments used by UTP cable on the Clinical Network.

Pair 2 of the UTP cable (**ORANGE** and **WHITE-orange** wires) **receives** the Network data. Pair 2 is connected to pins 3 and 6 of the 568A version and pins 1 and 2 of the 568B versions.

Pair 3 of the UTP cable (**GREEN** and **WHITE-green** wires) **transmits** the Network data. Pair 3 is connected to pins 1 and 2 of the 568A version and pins 3 and 6 of the 568B versions.

Figure 2-21 shows **end views** of both versions of RJ-45 connectors and jacks.

Note

Direct connect patch cables and in-wall wiring use the 568A version on both ends.

Cross over cables use a 568A version on one end and a 568B version on the other. Therefore, they **invert** the transmission and reception wires.

When purchased from Philips, cross over cables have **black boots on cable ends** for identification.

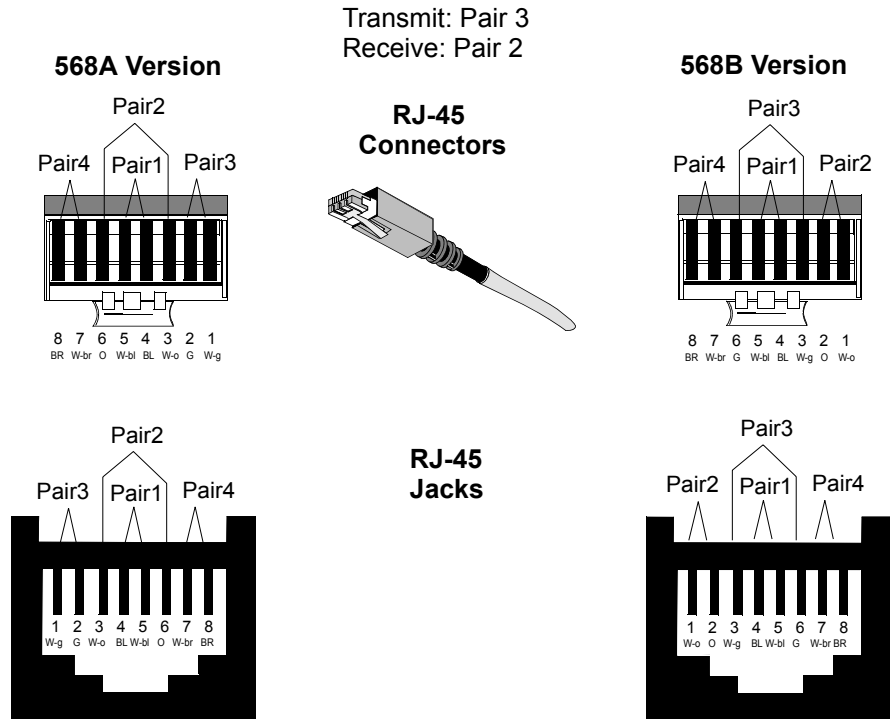


Figure 2-21 UTP Category 5 Connectors and Jacks

Fiber Optic Cable For noise immunity or extended distance cabling, multimode **fiber optic cable** is used. Multimode fiber optic cable consists of a 2-cord pair with each cord having a 62.5 micron fiber optic element core surrounded by 125 micron cladding. Each cord is then surrounded by a thermoplastic buffer layer, a Kevlar jacket, and a PVC sheath. One fiber strand is used for TX (transmit) and the other for RX (receive). See Figure 2-22.

Fiber optic cable is designed for minimal signal attenuation at wavelengths of 850, 1300, and 1550 nanometers. Clinical Network applications uses 1300 nm. A media translator is required when converting between UTP and fiber optic cables.

Note Single, continuous-length **fiber optic cables are limited to 1000 meters (3281 ft.)**.

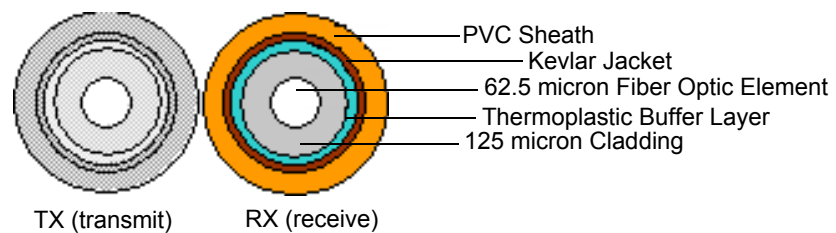
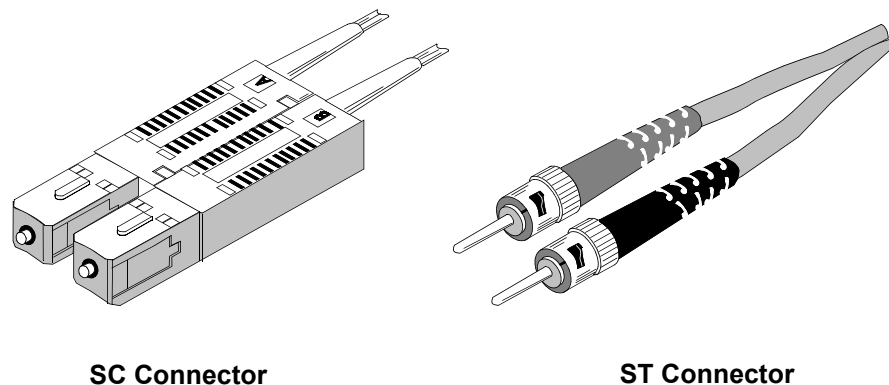


Figure 2-22 Fiber Optic Cable Cross Section

Fiber optic cables can have two different types of connector -- SC and ST -- as shown in Figure 2-23.

SC connectors have a square cross section and are used with a **Switch**.

ST connectors have a round cross section and are used with the **10 Mbps Media Translator**



SC Connector

ST Connector

Figure 2-23 Fiber Optic Cable Connectors

Wall Boxes RJ-45 wall boxes for UTP cable connectors are available from Philips for connecting Patient Monitors, Information Centers, Clients, and the Server to the Clinical Network. Both dual port (Option M3199AI #A10) and quad port (Option M3199AI #A12) wall boxes are available for US installations. Surface mount kits for mounting dual port wall boxes (Option M3199AI #A11) and quad port wall boxes (Option M3199AI #A13) are also available. Single port wall boxes and surface mount kits are also available for certain countries. See your Philips Representative for specific part numbers.

A dual port RJ-45 wall box is shown in Figure 2-24. Each wall box includes places for labeling UTP cables connecting to each port. A typical label would include the patch panel number and port number the cable connects to. For example, a label **2-14** would mean that the connecting UTP cable came from **patch panel 2 - port 14**.

UTP wire connections for each pin of port jacks are the 568A Version of Figure 2-21. Wiring of UTP cables to internal connectors of wall boxes must be performed by a certified CAT5 cable plant installer. They should be wired as shown in Figure 2-21

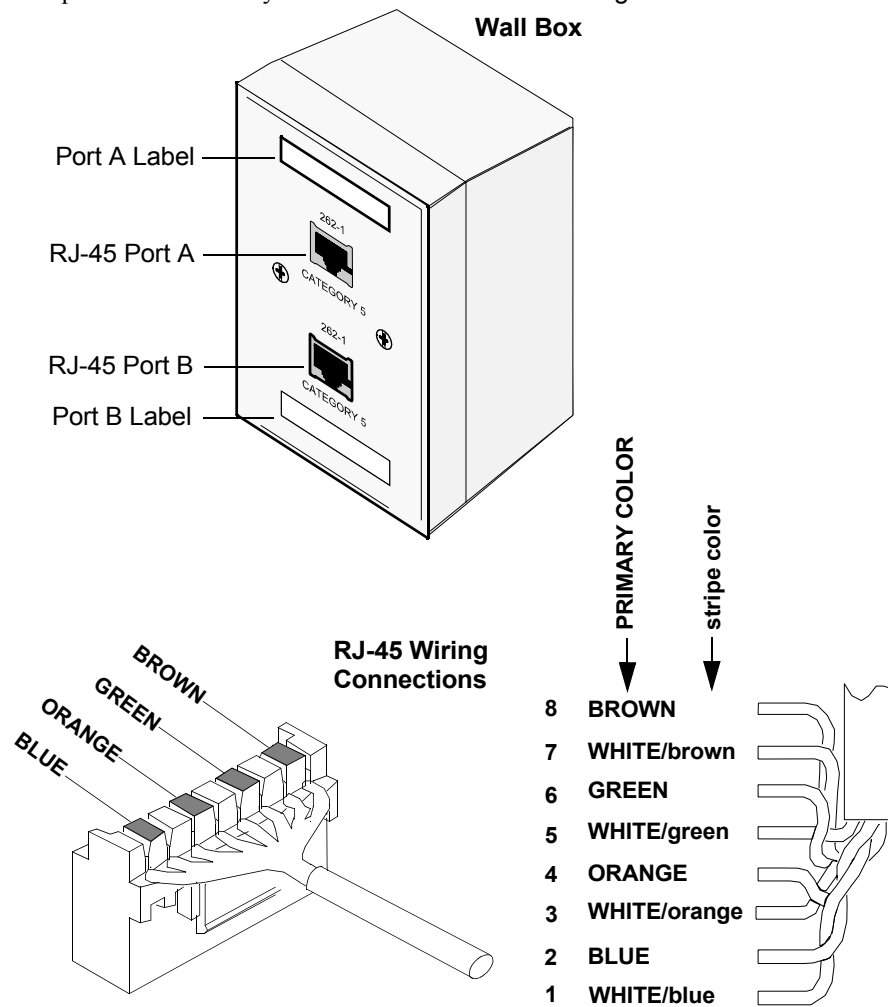


Figure 2-24 RJ-45 Wall Box and Wire Connections for UTP Cable

Patch Panels The Clinical Network contains many interconnecting cables and wires. To assure a robust, reliable, and accessible network, each wire connection must be secure, and identification of wires and cables must be clear. To assist this process, **24-Port Patch Panels** are available from Philips (Option M3199AI #A01). For large systems with many wires, it is recommended that patch panels be mounted in a floor standing rack designed for that purpose. However, Philips also provides a **Patch Panel Wall Mount Kit** (M3199AI #A05) for mounting the patch panel on a vertical wall.

The 24-port patch panel from Philips is shown in Figure 2-25. The **Front Panel** has 24, RJ-45 ports for connecting 24, UTP CAT5 RJ-45 connectors. Each front panel port should be labeled for cable identification. Places for port labeling are provided. Snap-in Philips labels are also included for each port.

The **Rear Panel** has 24 sections for connecting the 8 individual wires from 24 different UTP CAT5 cables. Wiring of UTP cables to the rear of the Patch Panel must be performed by a certified CAT5 cable plant installer. They should be wired as shown in Figure 2-25.

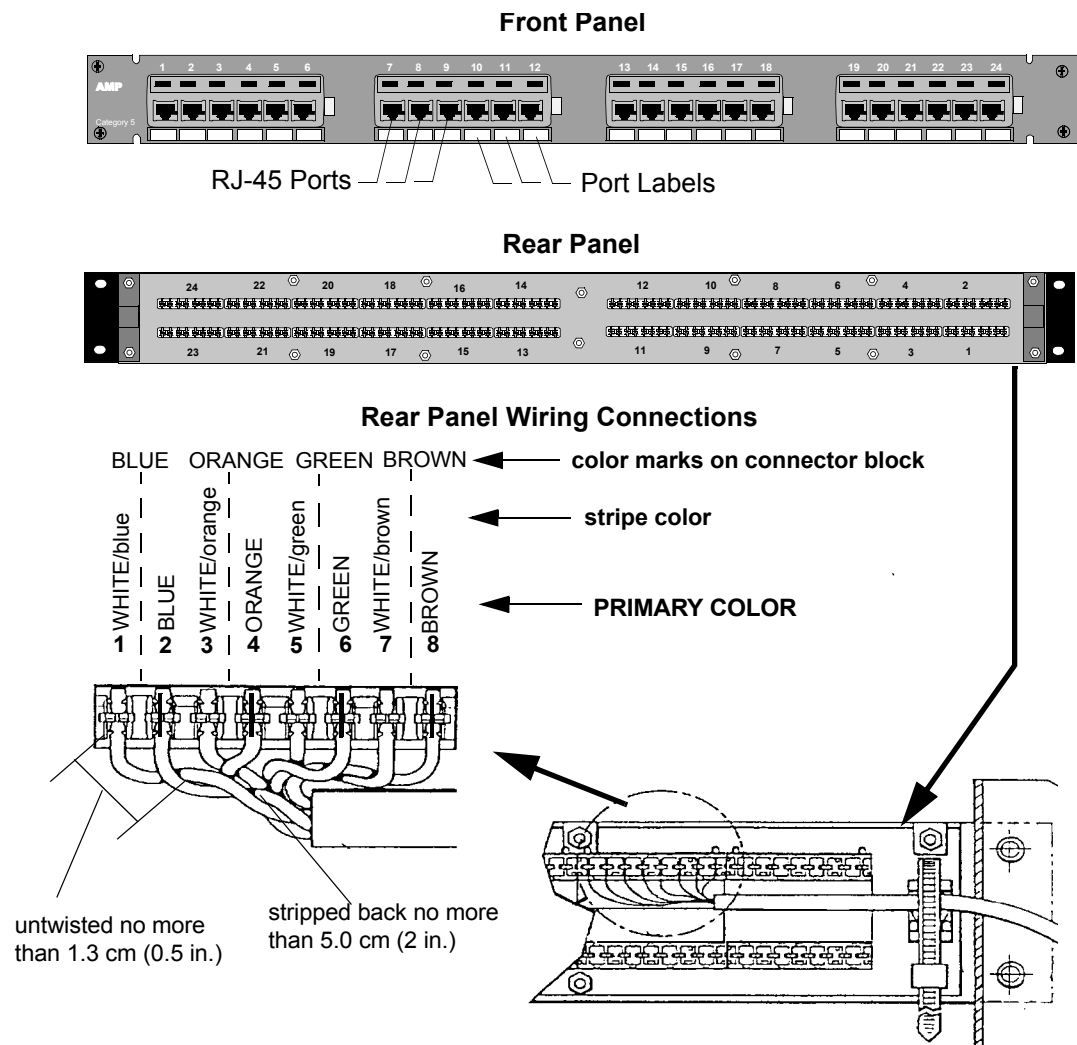


Figure 2-25 24-Port Patch Panel and Wiring Connections

Specifications

This section gives physical, environmental, electrical, and safety specifications for the Clinical Network components.

Caution

The following specifications are for units shipped at the time of this manual's publication. Units shipped with later systems may vary, with newer models substituted as they become available.

Note

Specifications for Information Centers, Clients and the Database Servers and their peripheral devices are given in the **Information Center Installation and Service Manual**.

Note

Specifications for the Application Server and its peripheral devices are given in the **Application Server Installation and Service Manual**.

Physical

The following table gives maximum dimensions and weights of each component of the Clinical Network system.

Table 2-1. Physical Specifications of Clinical Network Components

Philips Component	Product Part #	Height cm (in.)	Width cm (in.)	Depth cm (in.)	Weight kg. (lbs.)
UPS for Network components (650 VA, 120V)	862099	16.8 (6.6)	11.9 (4.7)	36.1 (14.2)	11.4 (25.0)
UPS for Network components (650 VA, 230V)					
24 Port Switch	862084	4.6 (1.8)	44.2 (17.4)	20.3 (8.0)	2.7 (6.0)
RangeLAN2 Wireless Access Point	M3189A	4.2 (1.66)	16.6 (6.54)	21.7 (8.54)	0.7 (1.5)
10/100 Mb/s Extension Switch	862085	3.6 (1.44)	24.9 (9.82)	11.6 (4.58)	0.9 (1.95)
10 Mb/s Media Translator Pair (each)	862088	4.4 (1.7)	42.5 (16.7)	25.8 (10.2)	4.1 (9.1)
100 Mb/s Media Translator	862089	2.5 (1.0)	7.6 (3.0)	11.9 (4.75)	1.4 (3.0)
Harmony Access Point Controller	862105	4.5 (1.8)	2.8 (11)	20.5 (8.1)	.86 (1.9)
Harmony Access Point	862092	3.4 (1.35)	8.4 (3.3)	1.4 (5.4)	.2 (.45)
Remote Power System	862093	4.4 (1.75)	43.3 (17)	30.2 (11.9)	4 (8.8)
AP Power over LAN Module	989803131231	3.2 (1.26)	12.7 (5)	7.62 (3)	.18 (.4)
Wireless Bedside Adapter	862095	3.4 (1.35)	8.4 (3.3)	1.4 (5.4)	.26 (.57)

Specifications

Environmental The following table gives information on the environmental operating requirements for Clinical Network components. Data for both the Philips system as a whole and for individual components are provided.

Table 2-2. Environmental Requirements for Network Components

	Product Part #	Temperature	Relative Humidity (Non-condensing)
Philips Components			
UPS for Network components (650 VA, 120V)	862099	41 - 104 °F 5 - 40 °C	15 - 80%
UPS for Network components (650 VA, 230V)			
24-Port Switch	862084	32 - 131 °F 0 - 55 °C	15 - 95% @ 40 °C
RangeLAN2 Wireless Access Point	M3189A	-4 - 140 °F -20 - 60 °C	10 - 90%
10/100 Mb/s Extension Switch	862085	32 - 104 °F 0 - 40 °C	5 - 95%
10 Mb/s Media Translator Pair (each)	862088	41 - 104 °F 5 - 40 °C	15 - 95% @ 40 °C
100 Mb/s Media Translator	862089	32 - 122 °F 0 - 50 °C	0 - 90%
Harmony Access Point Controller	862105	32 - 122 °F 0 - 50 °C	10 to 85%
Harmony Access Point	862092	32 - 131 °F 0 - 55 °C	10 to 85%
Remote Power System	862093	32 - 104 °F 0 - 40 °C	0- 90%
AP Power over LAN module	989803131231	32 - 104 °F 0 - 40 °C	0 - 90%
Wireless Bedside Adapter	862095	-4 - 140 °F -20 - 60 °C	20 - 90%

Electrical

The following table gives electrical specifications for Clinical Network components. These include the input voltage requirements, whether the unit must be manually switched for that voltage, the acceptable frequency range of the input voltage, and the maximum electrical power required that is dissipated to the environment during operation.

Table 2-3. Electrical Specifications of Clinical Network Components

Philips Component	Product Part #	Input Voltage (VAC)	Manual Switching Required?	Input Frequency (Hz)	Dissipated Power (max) (Watts)
UPS for Network components (650 VA, 120V)	862099	100 - 127	Yes	50 - 60	38
UPS for Network components (650 VA, 230V)		220 - 240	Yes	50 - 60	38
RangeLAN2 Wireless Access Point	M3189A	100 - 250	No	50 - 60	100
24-Port Switch	862084	100 - 127 200 - 240	No	50 - 60	36
10/100 Mb/s Extension Switch	862085	110 - 240		50 - 60	10
10Mb/s Media Translator Pair (each)	862088	100 - 127 200 - 240	No	50 - 60	72
100 Mb/s Media Translator	862089	100 - 120 220 - 240	Yes	50 - 60	
Harmony Access Point Controller	862105	120 - 240	No		
Remote Power System	862093	88- 264		47 - 63	432

Regulatory

Philips Software

The M3290A Information Center Release E.01 software complies with applicable portions of ANSI/AAMI EC-13 and with requirements of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices. It carries CE-marking to the European Medical Device Directive.



Rx ONLY

Philips Hardware

The UPS, switches, repeaters, and media translators comply with IEC 60950, CISPR 22 Level A, and EN 50082-1. They carry CE-marking to the European Low Voltage and EMC Directives. The Access Point carries the CE-marking to the European RTTE Directive.

Warning

Information Center 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.

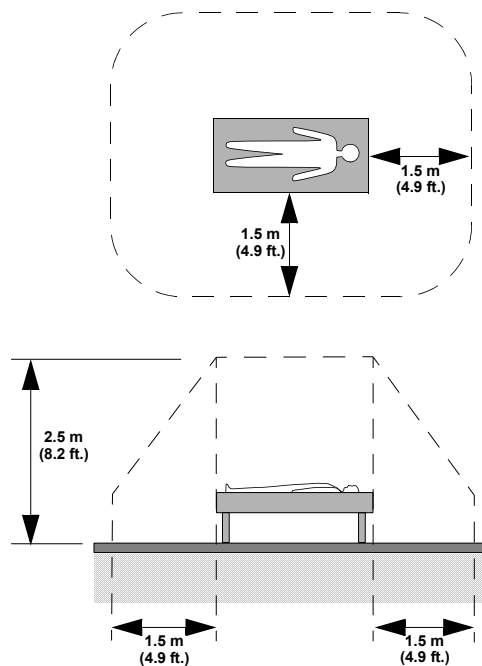


Figure 2-26 Limits of the Patient Environment

Regulatory

Overview

The Clinical Network components are the “hidden” components of the Philips Patient Care Network. Network cabling is installed within the walls and ceilings and Network components -- switches, media translators -- are generally located in out of the way equipment rooms or wiring closets. These components are rarely seen by clinicians or patients but must be accessible to service personnel. Significant planning and careful network design is required to assure low cost and effective network operation.

A key element of Network installations is network cabling. Philips personnel will assist customers in Network and network cabling design, but cable installation is generally a customer responsibility. The Clinical Network and its components must also be dedicated to Information Center applications and independent of other uses.

Chapter 3 describes site planning of the Philips Clinical Network in the following sections.

Site Planning	page 3-2
Network Design	page 3-7
Wireless Network Systems	page 3-19

Site Planning

Considerations

Elements of site planning that should be considered in preparing for a Clinical Network installation include the following:

Design	Selecting Network components that best meet the monitoring needs of the clinical environment.
Location	Selecting locations for the Network components.
Network	Assuring that proper network cabling, conduiting, wall boxes, and faceplates are provided for connecting devices to the Clinical Network.
Cabling	Selecting equipment cabling of the proper type and length to interconnect system components.
Environment	Assuring that the installation meets environmental specifications recommended for each Network component.
Electrical	Assuring that electrical outlets with proper grounding, electrical isolation, voltage, current, and frequency are available to power the system and components.
Mounting	Selecting hardware for mounting system components in their designated locations.
Safety	Assuring that all medical safety requirements are met.

A detailed description of the design of Clinical Network systems, including location of Network components and network considerations, is given in the following section, **Network Design**. Brief descriptions and references to the other considerations are also given in this section.

Responsibilities

Planning and preparing the site for an installation is a joint responsibility between the Customer and Philips. Sales and Support Representatives are available for consultation and assistance in each of the areas above. To assure that the system is properly designed and that all necessary preparations are completed when the system is delivered, the Customer should contact a Sales and Support Representative and develop a schedule for consultation, delivery, and installation.

Customer

The customer is responsible for the following site preparation tasks.

- ensure that the site complies with all structural, environmental, network, electrical, cabling, and safety requirements
- install all wall channels required for wall mounted devices
- install all required Network cables
- removal of old equipment
- frequency management (applies to wireless networks)

Note	<p>If there are any concerns about the structural, environmental, network, electrical, RF, cabling, or safety requirements for the installation, the Customer should contact an independent consulting engineer or the Response Center.</p> <p>The Customer is also expected to assist the Service Provider during the installation process by providing personnel with knowledge of the hospital environment and its facilities, resources, policies, and procedures.</p>
-------------	--

Philips Factory The Philips Factory is responsible for assuring shipment of a fully configured Philips product including:

- all ordered system hardware, network components, and peripheral equipment fully tested and ready for installation
- all ordered mounting hardware and equipment cabling
- all Philips support and service documentation
- shipment inventory Packing List

Philips Service Provider The Service Provider is responsible for installation of the Network system at the Customer site including:

- unboxing the products from their shipment containers
- installing the products in their designated locations, including any required mounting hardware
- connecting the Information Centers, Clients, Printers, and Servers to the Network and to all peripheral equipment
- connecting electrical power to Information Centers, Clients, Printers, Server, and all Network components
- installing purchased and upgrade options
- starting up the Philips system and configuring it to Customer specifications
- verifying system operation and testing system performance using recommended Product Assurance Testing procedures
- assuring Customer satisfaction and acceptance of the installation
- removal of packaging materials (if necessary)

Location The location of active Network components is a critical first step in site planning and network design. These components include the Database Servers, Application Server, switches, access points, and media translators. In general, they should be located in places inaccessible to patients and clinicians but convenient to service and support personnel. Typically this is a wiring closet or room specifically designed for Network equipment. The following issues should be considered when selecting and planning locations for active Clinical Network components.

Note	<p>Locating Information Centers, Clients, Database Servers, Application Servers and their peripheral equipment -- recorders, speakers, printers, remote displays -- is described in the Information Center or Application Server Installation and Service Manual.</p>
-------------	--

Wiring Closets Locked wiring closets or equipment rooms are recommended locations for all active Network components (except access points) because they can be made secure from unauthorized access and required electrical and environmental conditions can be maintained.

Caution In planning wiring closets, careful consideration must be given to the availability of properly grounded electrical outlets of the correct voltage and frequency for each device and to the environmental control of temperature and humidity. The high density of devices in a small room can lead to large heat loads in a small space that must be controlled.

Rack Mounting Most of the Network devices -- switches, media translators, patch panels -- are 48.3 cm (19 in.) wide and designed for rack mounting. Although they can be mounted on vertical surfaces or simply placed on horizontal surfaces, it is recommended that they be securely attached to wiring racks specifically designed for holding them. This will provide convenience in device wiring and managing the large number of cables that are typically required for Network systems.

Warning Clinical Network components and racks used for mounting Clinical Network components must be connected to an earth ground.

Switches Network switches are the central communication hubs of the Clinical Network. Therefore, they should be located at a point central to the Information Centers, Application Server, Clients, and Server. In selecting switch locations, consideration should be given to the cabling distances between devices because cabling is a key cost and limitation of Network design. In general, switches should be in wiring closets centrally located on the Network.

Wireless Access Points Wireless Access Points receive the patient data transmitted from wireless patient monitors and transmit them via the Clinical Network to the Server. The minimum spacing between access points is 3 m (10 ft.). Locating access points to assure full coverage of all possible locations of wireless monitors requires careful design consideration. A methodology for determining the number and locations of access points is provided later in this chapter along with design examples.

Extension Switches & Media Translators These devices must be located at points on the network determined by cabling distances between devices. They also should be located in wiring closets where required electrical and environmental conditions can be maintained.

Note Extension switches and media translators must **not be located above ceilings** where safety, security and environmental conditions cannot be assured.

UPSs Active Network components **must be on a UPS** (Uninterruptible Power Supply) to assure network operation during short power interruptions.

Warning

The Database Server and Application Server **must** be connected to a BATTERY BACKUP outlet of the 1000 VA UPS.

The following components **must** be connected to the BATTERY BACKUP outlets of a UPS: (See Figure 2-18)

- all switches
- media translators
- Harmony Access Point Controller
- workstations for all Information Centers and Clients
- Philips 2 Channel and 4 Channel Recorders

Up to 3 Clinical Network components -- switches, repeaters, media translators -- may be connected to a single, 650VA UPS.

It is **recommended** that Access Points and Harmony Remote Power Supplies also be connected to a 650 VA UPS.

The following components **may** be connected to the ACCESSORY outlets of a 650 VA UPS or to a separate non-UPS electrical outlet with the **same ground**.

- displays
- video splitters
- printer spooler

The LaserJet Printer **must not** be connected to the UPS.

Other Other issues to consider when selecting device locations include the following:

- Assure adequate distance of all devices from electrical equipment that may produce strong electromagnetic fields that can effect data transmission.
- Do not expose devices to water or excessive moisture, lint, dust, or dirt.
- Provide easy access to all devices by service personnel
- Provide at least 5 cm (2 in.) of clearance on all sides of each device for adequate air circulation.
- Do not obstruct ventilation holes at the top, bottom, sides, and rear of devices.

Network

Network cabling, conduit, wall boxes, and faceplates are generally the responsibility of a certified cabling installer. However, the network design should give careful consideration to the locations of RJ-45 wall boxes, both for the clinical equipment -- Information Centers, Clients, Application Servers, printers -- and for the active Network components that require them, e.g. repeaters.

Cabling

Interconnecting cable options for Information Center hardware -- workstations, displays, recorders, printers, UPSs -- is given in the Information Center and Database Server Installation and Service Manual.

Environmental Requirements	Environmental requirements for Network hardware are given in Chapter 2, Specifications . Refer to these requirements when selecting Clinical Network hardware locations.
Electrical Requirements	Electrical requirements for Clinical Network hardware are also given in Chapter 2, Specifications . Refer to these requirements when designing electrical power outlets for Network components.
Equipment Mounting	Mounting options for Information Center equipment are listed in the Information Center Installation and Service Manual . Network component mounting information is provided in their respective documentation
Safety	
Medical Device Standards	<p>Any medical device that connects directly to a patient, such as bedside monitors, must comply with IEC 60601-1, IEC 60601-1-1, and IEC 60601-1-2, the international safety requirements for medical electrical equipment. Any equipment that connects directly to a bedside monitor creates a medical electrical system that must also comply with IEC 60601-1-1. In practice, this means that the combined chassis leakage current of a medical device connected directly to a patient and any directly interconnected device must be less than 500 mA (300 mA in the U.S.)</p> <p>IEC 60601-1-1 does allow, however, for the use of other equipment in a medical environment provided that it complies with the relevant IEC standard and is not directly connected to a patient. Relevant IEC standards are IEC 60950 for computer equipment and IEC 61010 for laboratory equipment.</p>
Philips Device Requirements	Philips workstations, server, displays, LaserJet printers, and active Clinical Network components may be connected to bedside monitors through the Clinical Network and CareNet provided that they are located outside the patient environment and provided that the CareNet or telemetry mainframe contains a redundant Protective Earth connection. CareNet redundant Protective Earth connections are described in the Information Center Installation and Service Manual . When the CareNet and telemetry mainframe are properly installed, the resulting system complies with IEC 60601-1-1.
Patient Environment	None of the Network equipment is approved for use within the patient environment. Figure 2-26 shows acceptable distances from the patient environment beyond which all network equipment must be located.

Warning

The Information Center workstation, server, displays, recorder, LaserJet Printer, and Network components are not approved for placement within the 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.

Network Design

This section describes a methodology for designing a Philips Patient Care Network for a specific clinical environment. It includes the capabilities of the Clinical Network components, and rules that govern Patient Care Network design.

Clinical Requirements

Designing a **Patient Care Network** requires a full understanding of the monitoring requirements of the clinical unit(s) it will serve. There are several key elements that optimize system design:

- **number of clinical units and beds** to be simultaneously monitored
- **level of patient monitoring** required by each unit
- **types of patient monitors** to be used -- Clinical Network connected (IntelliVue Patient Monitors, M3/M4), SDN/PCC connected (hardwired and/or telemetry) or both types.
- **locations** of clinical units, central monitoring stations, and review stations
- **type of patient data access** required at each location (real-time or stored -- read, write, or both)
- possible **future capability** or expansion

Number of Units and Beds

The first issue to consider is the number of clinical units and beds to be served by the Patient Care Network and their location. The number of beds determines the number of patient monitors and Information Centers required to monitor patients. The number of clinical units and their locations determines how the Information Centers should be networked to provide efficient and convenient access to patient monitoring data.

Patient Monitor Type

Another consideration is the type of patient monitor that will be used -- SDN/PCC (hardwired and/or telemetry), Clinical Network connected monitors (M3/M4 (wired and/or wireless), IntelliVue Patient Monitors), or both types. For installations of acute patient care, where patients remain in their beds, hardwired bedside monitors, either SDN/PCC or Network connected, are generally required. For less acute care installations, in which patients are ambulatory, SDN/PCC telemetry monitors are generally required. For installation in which patients may change from bed restricted to ambulatory, both hardwired and telemetry monitors should be available. And for installations where patient monitors may be frequently moved from bed to bed, wireless monitors, may be preferred. The software can accommodate all of these types of installations, providing continuous collection of monitoring data as patients change beds or from bed restricted to ambulatory.

Central Monitoring Locations

Locations where central patient monitoring will take place. These will generally be in clinical units where patient beds are located.

Patient Data Review Locations

Locations where review of patient data is required. While the Patient Care Network provides extensive access to patient monitoring data, both within and across clinical units and at multiple distant locations, there are limitations on the length of cable runs for each network interconnection. Cable length limitations must be carefully reviewed in selecting patient data review locations.

Type of Patient Data Access The type of access to patient data and monitoring controls at each monitoring location. For example, does the clinician need to view both real-time and stored patient data from a clinical unit and/or other clinical units? Will it be necessary to silence alarms or change monitoring control settings? The answers to these types of questions are critical to the selection of monitoring hardware and network design. And they have great impact on the effectiveness of the Information Center system in meeting the needs of clinicians, as well as system cost.

Future Capability When designing a Patient Care Network, both present and future requirements should be considered. There are limitations on cable lengths for each type of component interconnection. Hence, consideration should be given to possible future growth or requirements in system design. Review this thoroughly with a Service Provider.

Note Design of the CareNet portion of the Patient Care Network and clinical requirements for patient data collection, storage, and review are described in the **Information Center Installation and Service Manual**. Only the Clinical Network portion of the Patient Care Network is described here.

Philips Hardware Capability

The design also requires a full understanding of the capabilities and limitations of network components so they can be properly matched to the clinical requirements.

Figure 1-6 shows an extensive Patient Care Network as an overview of the components available for network design. This network can collect and display patient monitoring data from SDN/PCC connected monitors (hardwired and telemetry), M3/M4 monitors (wired and wireless), and IntelliVue Patient Monitors and store patient monitoring data for up to 128 patients monitored by 8 Information Centers at 8 separate locations. It can also accommodate 8 Clients for viewing data (real-time and stored) at 8 separate locations and viewing of stored patient data from any browser equipped PC on the hospital’s intranet. From this overview of maximum system capability, smaller, more limited systems can be designed.

A Patient Care Network is designed from the following general components:

- **patient monitors** for collecting patient monitoring data
- **CareNet** (Serial Distribution Network and Philips Communications Controller) for transmitting and managing patient data among monitors and central stations
- **wireless access points** for receiving monitoring data from wireless patient monitors
- **central monitoring stations** for displaying patient monitoring data
- **review stations** for viewing real-time and stored patient data
- **Database Servers** for receiving, storing, and retransmitting monitoring data from multiple patients
- **Application Server** for delivering clinically significant applications across the IntelliVue Clinical Network and the hospital information LAN to ‘information portals’ on the IntelliVue Patient Monitor, the Information Center, and Information Center Clients
- **Clinical Network** for transmitting and managing patient data among monitors and for interconnecting multiple central monitoring and review stations and the database server
- **Printers** for printing patient data and configuration settings

Following is a brief description of the key capabilities of these components that must be considered when designing a Patient Care Network to meet specific clinical monitoring requirements.

Patient Monitors Patient monitors can be connected to the Clinical Network in one of two ways -- via the CareNet (SDN/PCC, either hardwired or telemetry), and directly, either wired or wireless. Each type of monitor can monitor only **1 patient**.

Clinical Network monitors can be:

- **Hardwired IntelliVue/M3/M4 Patient Monitors** that connect directly to a Network switch.
- **Wireless IntelliVue/M3/M4 Patient Monitors** that transmit patient monitoring data to a Wireless Access Point that is connected to the Clinical Network

CareNet monitors can be:

- **Hardwired Monitors** can be the Philips Component Monitoring System (CMS) with extensive monitoring capability, the Philips 24 patient monitor with more limited monitoring capability, or the older Compact Configured Monitor.
- **Telemetry Monitors** can be Philips Telemetry system or the older model Digital UHF Telemetry system. **Each telemetry mainframe** can accommodate up to **8 telemetry monitors**, 1 per patient.

CareNet To display data from multiple patient monitors on a central monitoring station, the monitors can be connected to the **CareNet** switch, which receives, transmits, and manages the flow of data among patient monitors and central stations connected to the SDN.

Note Each CareNet switch can accommodate a total of **24 patient monitors per PCC** (hardwired and telemetry) and **6 central monitors** .

Clinical Network The **Clinical Network** provides networking capability that permits over-viewing real-time and stored patient data within, across, and outside clinical units. The Clinical Network utilizes industry standard components (switches, repeaters, media translators), cabling (UTP, fiber optic), and connection hardware (patch panels, cables, wall boxes). A summary of the design characteristics of these components is given below. For more detailed information, see **Chapter 2, Hardware Description**.

Switches (Core/Edge) - rack mountable workgroup switches with **24, 10/100 Mbit/s ports** (UTP, RJ 45) and **0, 1 or 2, 100 Mbit/s fiber optic ports** provide for the connection of Patient Monitors, Printers, Media Translators, Access Points, wireless network devices, Information Centers, Clients, Application Server and a Database Server to the Network. These switches are managed (have an IP Address), and have network statistics available at the Information Center or Database Server for remote troubleshooting. These switches must be used when the monitors are switch-port mapped.

Cabling - Ethernet, **Category 5 UTP cable** and **62.5/125 micron multimode fiber optic cable** are used to interconnect devices. Cable distance limitations for various interconnections are given in **Chapter 1, M3185 Clinical Network**. Philips offers CAT5

UTP orange cable so the patient monitoring network can be distinguished from other hospital network cabling.

8 Port Switches - 8, 10/100 Mbit/s UTP ports allow small clusters of devices to be connected to the system from a remote location. These switches are not managed, do not have network statistics available, and cannot be used when the patient monitors are switch-port mapped.

Media Translators - 10Base-T and 100Base-T media translators permit interconnecting UTP and fiber optic cable for transmitting data extended distances.

Printers **HP LaserJet printers** can be connected to the network for shared printing capability.

Switch Function The switch function vs switch type differs in the Release E.01 system than in previous releases. In Release E.01, the following applies:

- The Core switch must be a HP2524 switch
- Edge switches can be any of the following switches
 - Cisco 1900 (managed switch)
 - HP2524 (managed switch)
 - HP 408 (unmanaged switch)
 - AT-FS708 (unmanaged switch)

Switch Firmware The supported switch firmware is listed below:

- HP2524 Switch: F.02.02 and F.02.13
- Cisco 1900 Switch: 9.00.04 & 8.01.02

Switch Rules Switches (except for unmanaged switches) and access points must be configured using the ConfigTool. See **Device Configuration on page 4-7**. There are special rules that apply to the use of switches in the Release E.01 system. See **Figure 3-1** for how some of these rules are implemented:

- Only one Core switch is allowed on a network
- The Core switch is configured as the center, or “core” of the clinical network
- Tier 1 switches connect to the Core switch
- Tier 2 switches connect to Tier 1 switches
- Tier 3 switches connect to Tier 2 switches
- A maximum of 3 tiers of switches are allowed
- There are no restrictions on the total number of switches
- In a central database network, the Database Server must connect to the Core switch.
- In an Information Center local database network, the Information Center must connect to the Core switch
- Information Centers and Clients must connect to the HP2524 managed switch (connection to the Cisco switch is **not** supported)
- In a standalone Application Server network, the Application Server must connect to the Core switch.
- Access points and network printers can connect to any switch

- IntelliVue/M2/M3/M4 Patient Monitors can connect to the Core or Edge switch. Besides that are switch-port mapped must be connected to a **managed** switch.

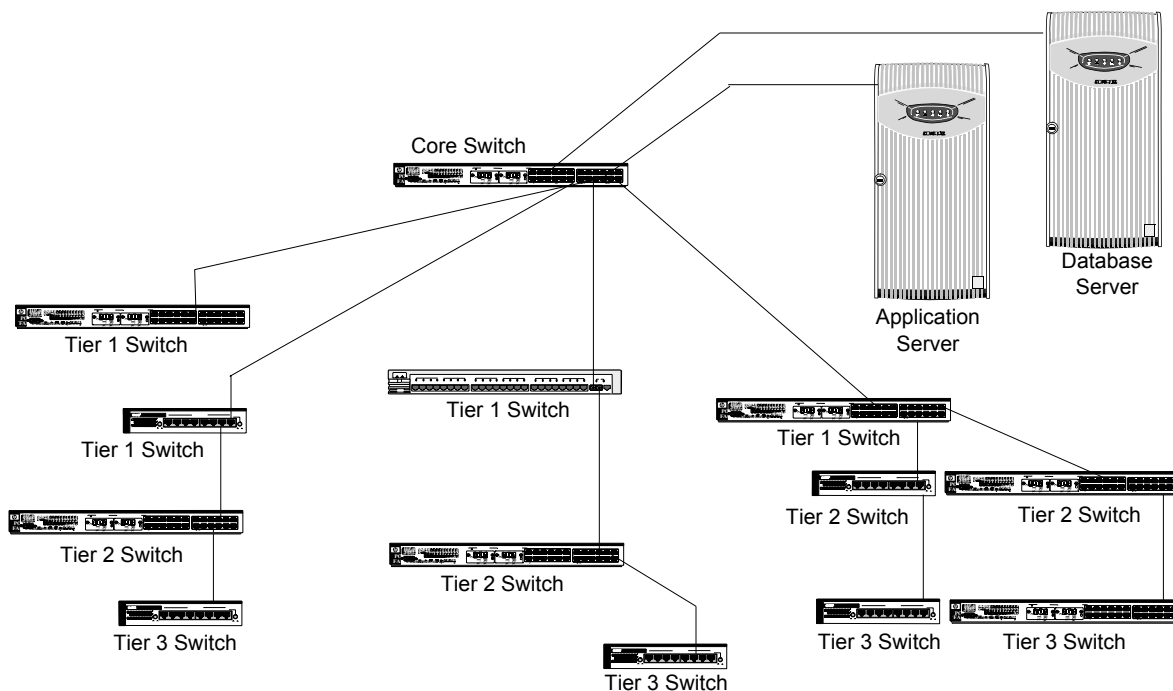


Figure 3-1 Example of supported Switch Hierarchy

Upgraded Systems All switches (except for the Extension switch), and the RangeLAN2 access points must be reconfigured using the Release E.01 ConfigTool. For instructions on upgrading these devices, see Device Configuration on page 4-7. Switches must be configured to the appropriate port settings (Auto-negotiate, 10 or 100 Mbps, Half or Full Duplex, Table 3-1.)

Warning

The Cisco switch used in earlier releases cannot be used in a Release E/E.01 system to connect Information Centers and Clients to the clinical network. Doing so will cause undesired performance problems.

Designing Clinical Network Systems

The design of a Clinical Network system depends on the type of patient monitors connected to it - SDN/PCC monitors, M3/M4 monitors, IntelliVue Patient Monitors, or mixed SDN and IntelliVue/M3/M4 Patient Monitors.

The design of **Clinical Network systems** involves two major steps. The first is to determine the **switch requirements**, that is, the number of switches required, and the devices (central monitors and review stations, M3/M4 monitors, IntelliVue Patient Monitors, access points) that will be connected to each switch port. The second is to determine the **Cable Plant requirements** -- cabling types and lengths and components (wall boxes, repeaters, media translators) necessary to interconnect network devices.

Note This manual does not describe the design and implementation of Clinical Network systems in detail because each clinical environment requires careful analysis by an experienced network designer. Philips Service Providers are specially trained to assist customers in reviewing their clinical requirements and designing a Clinical Network system that meets those requirements and will be supported by Philips Medical Systems.

The general concepts and capabilities of Network components and systems given here should only be used as a reference for understanding the final design. Two examples are provided to illustrate the design process.

Consult a Philips Service Provider for Clinical Network system design advice.

Connecting Devices Review the locations of the network devices and select the repeaters, media translators, cable types and lengths required to interconnect them. (See Network Connections on page 4-45).

Table 3-1 summarizes the Clinical Network devices and the settings required for connection. Start with device and switch selection, and follow across to determine what speed and duplex settings are needed to make the connection. Then, determine which connection type is appropriate. Table 3-2 shows the current hardware and the port settings they are capable of supporting.

Note The network connections for these devices are described in detail in Network Connections on page 4-45.

Device Requirements with Applicable Port Settings

The following table represents the devices supported in the clinical network, the device settings, operational speed and duplex requirements, and the acceptable switch port settings.

Table 3-1. Network Device Requirements with Applicable Port Settings

	Network Device	Device NIC Setting	Operational Speed and Duplex Setting	Acceptable Switch Port Setting*
10 Mbps	<ul style="list-style-type: none"> • Wired Patient Monitors • Network Printers • RangeLAN2 Access Points • Harmony Access Points & Remote Power Supply 	10 Mbps Half Duplex	10 Mbps Half Duplex	Auto-Negotiate or 10 Mbps Half Duplex
100 Mbps	<ul style="list-style-type: none"> • Information Centers • Clients 	100 Mbps HALF Duplex	100 Mbps HALF Duplex	100 Mbps HALF Duplex
100 Mbps	<ul style="list-style-type: none"> • Database Server • Small Database Server • Application Server 	100 Mbps FULL Duplex	100 Mbps FULL Duplex	100 Mbps FULL Duplex

Table 3-1. Network Device Requirements with Applicable Port Settings

	Network Device	Device NIC Setting	Operational Speed and Duplex Setting	Acceptable Switch Port Setting*
100 Mbps	• Switch	Auto-Negotiate or 100 Mbps Full Duplex	Auto-Negotiate or 100 Mbps Full Duplex	Auto-Negotiate or 100 Mbps Full Duplex
Auto-Negotiate	Harmony Access Point Controller	Auto-Negotiate	100 Mbps Full Duplex	Auto-Negotiate

* The Switch port setting must be configured using the Config Tool. See Device Configuration on page 4-7.

Note All Switch to Switch connections need to operate at 100 Mbps FULL duplex. Acceptable port settings are 100 Full to 100 Full or Auto-Negotiate to Auto-Negotiate.

Specific Network Device Settings Table 3-2 lists the current Clinical Network infrastructure devices and the speed and duplex settings they support in the Information Center network.

Table 3-2. Network Device Speed & Duplex Settings

Device	Port(s)	Auto-Negotiate	10Mbps Half	100 Mbps Half	100 Mbps Full
HP2524 Switch	1-24 (UTP)	yes	yes	yes	yes
	25-26 (fiber)				yes
Cisco 1900 Switch	1-24 (UTP)		yes		
	A (fiber)				yes
	B (UTP)	yes*			yes
8 Port Switch	All	yes			
J3300 10 Mbps Repeater			yes		
J3300 + J2606 10 Mbps Translator Pair			yes		
100 Mbps Media Translator (E-100BTX-FX-04)		yes*			yes
100 Mbps Media Translator (E-100BTX-FX-05)		yes*			yes

* this device only supports 100Mbps operation

Drawing the Design The final step is to draw the Patient Care Network using the devices, components, and cabling. Figure 1-6 illustrates a typical schematic design. Your final design, however, should show all relevant information (Device Names, Locations, Cable Types and Lengths, etc.).

Design Guidelines

This section describes the guidelines to be followed when designing a Clinical Network system. Two examples are given: one is a single switch network and the other is a multiple switch network. These examples describe hardware design only.

The basic principles in designing the network design are:

- design a network that will minimize the number of devices data needs to flow through, this
 - optimizes performance by minimizing traffic on the network
 - minimizes the impact of a single device failure
- design systems with troubleshooting in mind
 - combine in as few locations as practical
 - use host names to easily identify device information (i.e. unit and location)
 - recognize the trade-offs in using managed and unmanaged switches

There are three types of messages that are used in the network. **Directed**, **Broadcast**, and **Multicast** messaging.

Directed Messages

A directed message is a message that is sent from one device to another device using the receiving device’s IP address. Most network communication is handled via directed messaging. Some examples of this are Wave, Event and Trend Review exchanges between the Information Center and DBS, print requests between the Information Center and printer, and physiological data and control messages between a bedside and the Information Center.

Broadcast and Multicast Messages

Broadcast and Multicast messages are messages that are sent to the entire network, regardless of the network design. Some examples of **broadcast** messages are time synchronization and bootp requests. Bed to Bed Overview is handled via a **multicast** message.

Note

Access points block multicast messages to the wireless bedsides to conserve bandwidth on the wireless network. This is why the Overview feature is not available on the wireless bedsides.

Example 1: Single Switch Network

The first network must meet the following clinical requirements:

- 12 bed ICU with primary monitoring using 12 hardwired CMS monitors
- 8 bed CCU with primary monitoring using 8 hardwired CMS monitors
- 1 printer shared by the CCU and ICU
- Patient data overview capability in a hallway location
- Patient data overview capability in a doctors lounge

Approximate cable run distances from a centrally located wiring closet to each of these locations is measured in Table 3-3.

Table 3-3. Single Switch Network Requirements

Device	Distance	Speed	Duplex
ICU Information Center	87 m (285 ft)	100 Mbps	Half
CCU Information Center	65 m (213 ft)	100 Mbps	Half
Printer	70 m (230 ft)	10 Mbps	Half
Hallway Client	41 m (135 ft)	100 Mbps	Half
Doctor’s Lounge Client	137 m (450 ft)	100 Mbps	Half
Database Server	5m (16 ft)	100 Mbps	Full

These requirements are shown schematically in Figure 3-2.

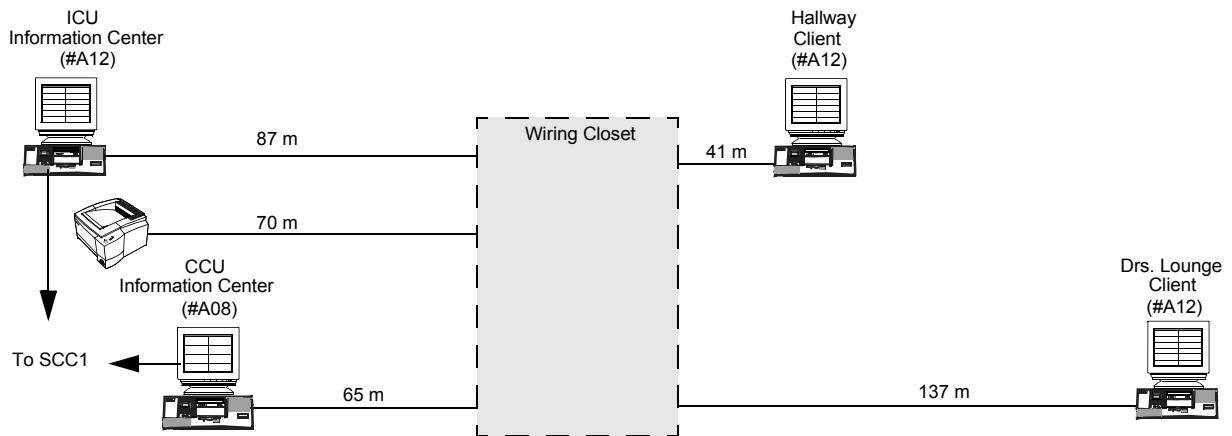


Figure 3-2 Single Switch Network Requirements

The **Network Design** for the Patient Care Network for this example is shown in Figure 3-3. Note that the power supplied to all devices except the Printer are from UPSs and that wall boxes are provided for the Information Centers, Clients and Printer. The cable between the Core Switch and the Server is a UTP patch cable. All others are in-wall, continuous, UTP cables.

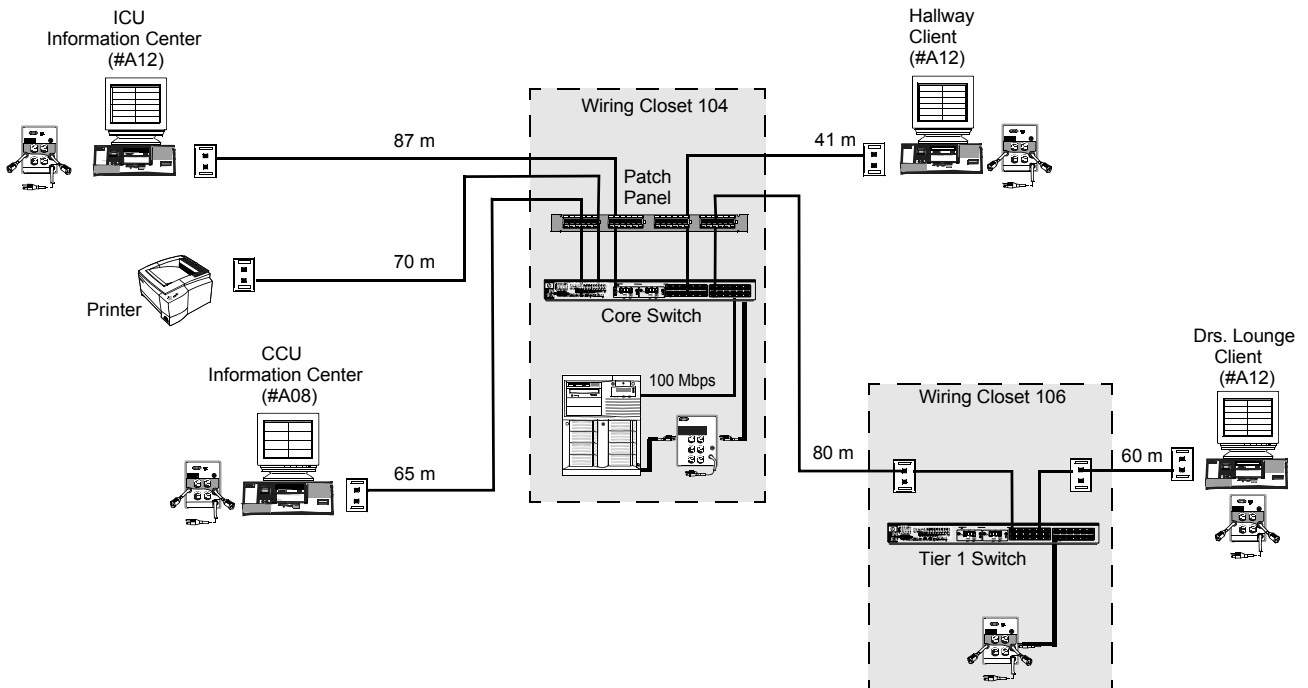


Figure 3-3 Single Switch Network Design Example

Table 3-4 lists the Connection types to be used for this example. These were determined using the guidelines listed in Network Connections on page 4-45.

Table 3-4. Single Switch Network Requirements w/Connection Types

Device	Distance	Speed	Duplex	Connection Type
ICU Information Center	87 m (285 ft)	100 Mbps	Half	D
CCU Information Center	65 m (213 ft)	100 Mbps	Half	D
Printer	70 m (230 ft)	10 Mbps	Half	A
Hallway Client	41 m (135 ft)	100 Mbps	Half	D
Doctor’s Lounge Client	80 m (262 ft)	100 Mbps	Half	D
	60 m (197 ft)	100 Mbps		
Database Server	5m (16 ft)	100 Mbps	Full	D

**Example 2:
Multiple
Switch
Network**

The second network design example must meet the following clinical requirements:

- 12 bed ICU with primary monitoring using 12 hardwired CMS monitors on 3rd floor
- 12 bed CCU with primary monitoring using 12 hardwired CMS monitors on 3rd floor
- 48 bed Step Down Unit (SDU) on 3rd floor using 24 telemetry, 12 wired M3 and 12 wired IntelliVue Patient Monitors
- 6 bed SICU on 2nd floor using wired IntelliVue Patient Monitors
- 8 bed ER on 1st floor using wireless M3 monitors and 2 access points
- Patient data overview capability in ICU and CCU
- 1 printer shared by the ICU and CCU
- 1 printer in SDU

Approximate cable run distances from a centrally located 3rd floor wiring closet to each of these locations are listed in Table 3-5.

Table 3-5. Multiple Switch Network Requirements w/Connection Types

Unit	Device	Distance to Wiring Closet (Room 304)	Speed	Duplex	Connection Type
ICU	Information Center	70 m (230 ft)	100 Mbps	Half	D
	Client	70 m (230 ft)	100 Mbps	Half	D
	Printer	70 m (230 ft)	10 Mbps	Half	A
CCU	Information Center	70 m (230 ft)	100 Mbps	Half	D
	Client	70 m (230 ft)	100 Mbps	Half	D
SDU	Information Center (x4)	216 m (708 ft) 60 m to Room 316	100 Mbps	Half	D
	Printer	216 m (708 ft) 60 m to Room 316	10 Mbps	Half	A
	M3 (x12)	216 m (708 ft) 60 m to Room 316	10 Mbps	Half	A
	IntelliVue Patient Monitors (x12)	216 m (708 ft) 60 m to Room 316	10 Mbps	Half	A
	(Tier 1 Edge Switch)	156 m (512 ft) from Room 316	100 Mbps	Full	E
SICU	Information Center	82 m (269 ft) 28 m (92 ft) to Room 204	100 Mbps	Half	D

Table 3-5. Multiple Switch Network Requirements w/Connection Types

Unit	Device	Distance to Wiring Closet (Room 304)	Speed	Duplex	Connection Type
	IntelliVue Patient Monitors (x6)	82 m (269 ft) 28 m (92 ft) to Room 204	10 Mbps	Half	A
ER	Information Center	114 m (374 ft) 60 m to Room 204	100 Mbps	Half	D
	Access Points (x2)	114 m (374 ft) 60 m to Room 204	10 Mbps	Half	A
	(Tier 1 Edge Switch)	54 m (177 ft) from Room 204	100 Mbps	Full	D

Note The ICU, CCU will be served by SCC1, and the SDU by SCC2.

Note that the **Core Switch** and the **Server** will be located in a wiring closet (304) near the ICU and CCU and the Edge Switches, Tier 1 and Tier 2 will be located in a wiring closet (316) near the SDU.

Note that the connection between the **Core Switch** and **Edge Switch Tier 1** is an in-wall, continuous, fiber optic cable. An Edge switch is used and is placed in a wiring closet (204).

The **Network Design** for the Patient Care Network for this example is shown in Figure 3-5.

Note UPSs for Information Centers and Clients are not shown for simplicity.

Network Design

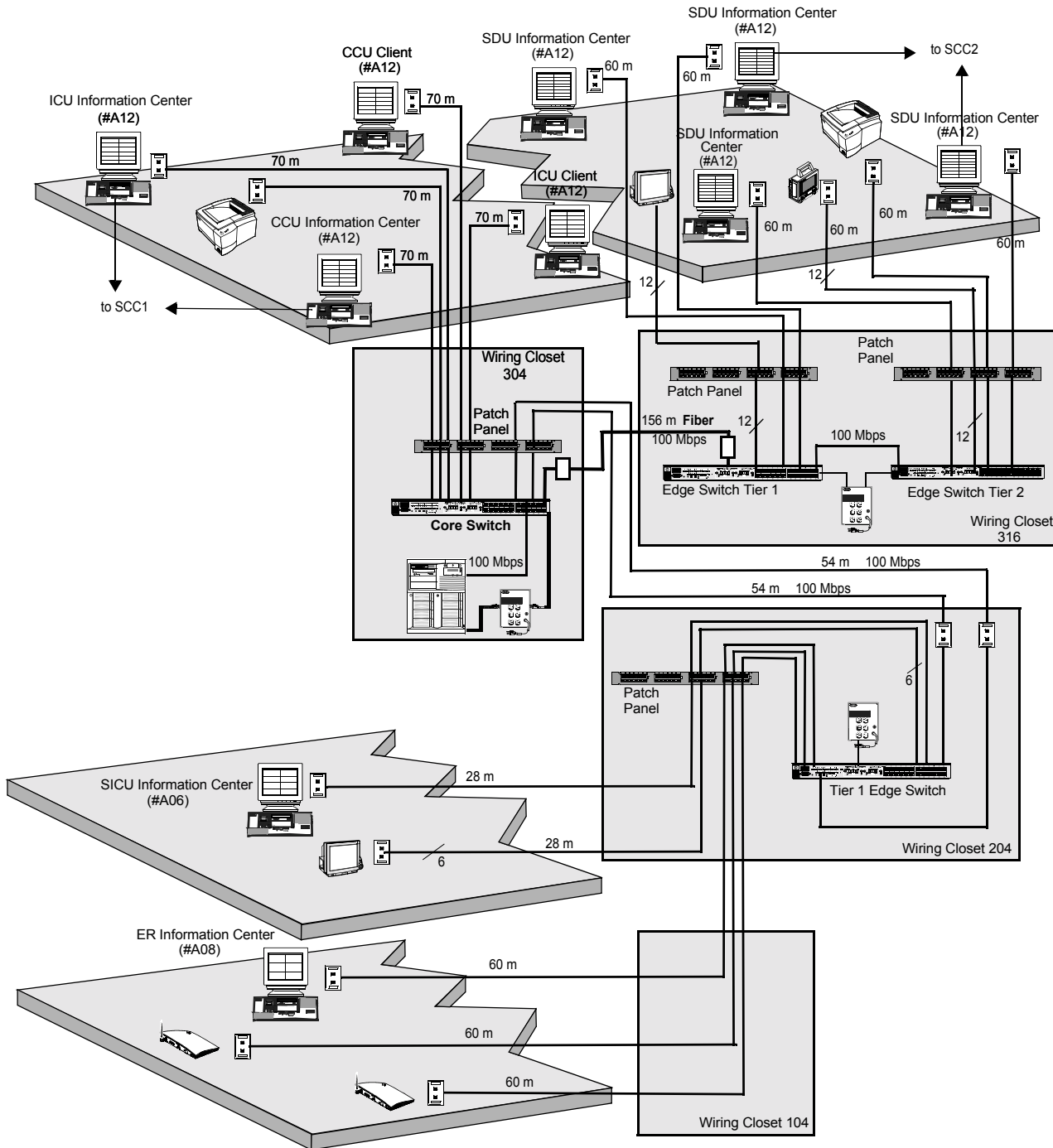


Figure 3-5 Multiple Switch Network Design Example

Wireless Network Systems

Bedside 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 from a bedside cannot be 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 bedside at the central station can range from a momentary period to a lengthy period of data loss. Although data loss due to the wireless link may be occurring at the central station, monitoring and alarms continue at the bedside.

Frequency Management

Frequency management is the selection of the frequencies for wireless devices within a facility to prevent interference between devices. Frequency management is the responsibility of the hospital. Philips Medical Systems has no control over the RF environment in the hospital. If interference exists at the operating frequencies, the wireless system will be affected.

The Philips wireless network operates in the 2.4-2.485 GHz range. Other devices that might be found in the hospital that can radiate in the 2.4-2.485 GHz range and create interference are:

- other wireless networks
- microwave ovens
- some wireless telephone headsets
- devices utilizing BlueTooth technology
- some programming devices for pacemakers
- other

A quick check for interference while doing a site survey can be done using a “Snoop” tool (see RF Survey on page 3-27). However, there is no guarantee that all the devices are operating at that time. With the recent explosion in the use of wireless devices, there is no substitute for a central authority in the hospital that tracks and licenses (if required by local regulations) all wireless devices used within the facility.

Wireless Network Design Guidelines

Wireless monitoring has many advantages, but it also has some 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 from a bedside cannot be as dependable as a wired network connection.

Caution

Failure to adhere to the rules and guidelines provided in this section will result in an increase in the number of dropouts the users see at the Information Center. You can avoid dropouts by avoiding things that cause the corruption of wireless data.

Standard vs Non-Standard Systems

A standard wireless Clinical Network system:

- has no more than 15 Access Points, and
- has no more than 24 wireless M3/M4 Patient Monitors, or
- has no more than 12 wireless IntelliVue Patient Monitors, and
- has no restrictions on where the Patient Monitors can be used

A non-standard wireless Clinical Network system:

- needs more than 15 Access Points, or
- has more than 24 wireless M3/M4 Patient Monitors, or has more than 12 wireless IntelliVue Patient Monitors, and
- has restrictions on where the Patient Monitors can be used

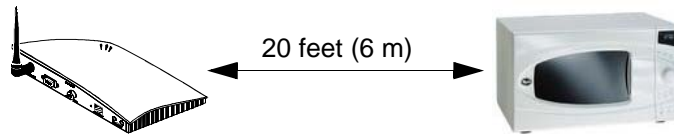
Table 3-6. Wireless Design Rule Summary

	Standard	Non-Standard
	Unrestricted Cell-to-Cell Roaming	Limited Cell-to-Cell Roaming
Restrictions	None, beds will work anywhere in the coverage area	Site and design dependent. Signal brown-outs can occur if design limits are exceeded
Maximum Number of Access Points	No Channel Reuse	15
	With Channel Reuse	Unspecified, determined by the RF Characteristics of the site
Maximum Number of Wireless Patient Monitors	24 M3/M4 Patient Monitors 12 IntelliVue Patient Monitors	Unspecified
Maximum Number of Wireless Patient Monitors per domain	6	-
Maximum Number of Wireless Patient Monitors per Access Point	-	6
Maximum Number of Access Points per Cell	4 M3/M4 Patient Monitors 2 IntelliVue Patient Monitors	2
Maximum Number of Wireless Patient Monitors per Cell	24 M3/M4 Patient Monitors 12 IntelliVue Patient Monitors	12
Maximum Number of Access Point Controllers	15	15
Maximum Number of Wireless Access Points per Access Point Controller	15	15

Note In mixed wireless systems (e.g. M3/M4 and IntelliVue Patient Monitors) the wireless design rules and limitations for the IntelliVue Patient monitors takes precedence.

In both standard and non-standard systems, if there are large metal objects in the coverage area, position the Access Points to avoid blocking the RF signal. To avoid interference,

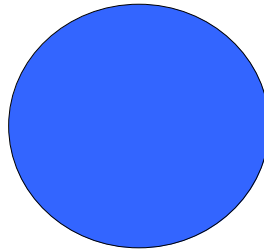
position Access Points a minimum of 20 feet (6 m) from microwave ovens and do not have a microwave between the access point and the wireless bedside:



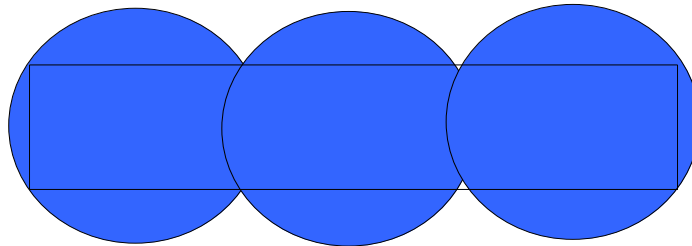
Standard System Design

To implement a standard wireless design, the following rules must be considered:

A **cell** is the physical area that can be covered by a single access point. A circle with a radius of 50 ft (15 m) is used to estimate the bounds of a cell.



A set of contiguous cells that covers all of the desired coverage area defines a wireless domain. For standard systems, a wireless bedside can be used, or can roam into any cell in this wireless domain.

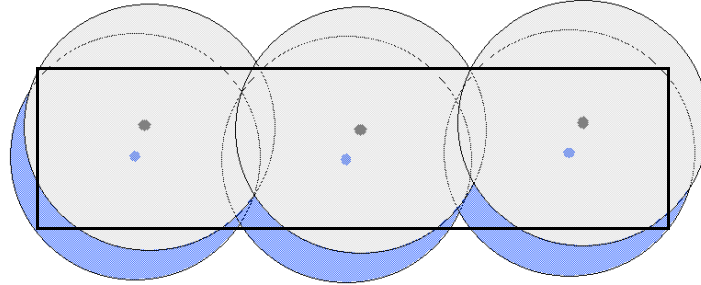


Caution

If the wireless bedside are not distributed evenly, or if more monitors are added to the system, it is possible to overload the access point.

A limit of 6 wireless bedside can be served by a single wireless domain in a standard network. If there are more than 6 bedside, just add another layer of Access Points creating a

second domain. This allows another 6 beds. When you add this additional domain, you must separate the Access Points by 10 feet (3 m) to prevent interference:

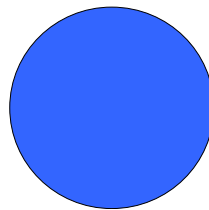


If there are more than 12 M3/M4 bedsides, add another layer of Access Points creating a third domain, for another 6 bed capacity. Only 4 layers of domains, with a 24 M3/M4 wireless bedside maximum is supported in a single RF system. Only 2 layers of domains are supported with wireless IntelliVue Patient Monitors.

Note Systems with more than 24 wireless M3/M4 Patient Monitors or 12 wireless IntelliVue Patient Monitors fall into the non-standard category.

Standard System Example At a customer site, there is an area where wireless Network coverage is desired. This area covers patient bed locations. A single Access Point covers an area that is roughly determined by a circle with the Access Point in the center. This area is called a cell.

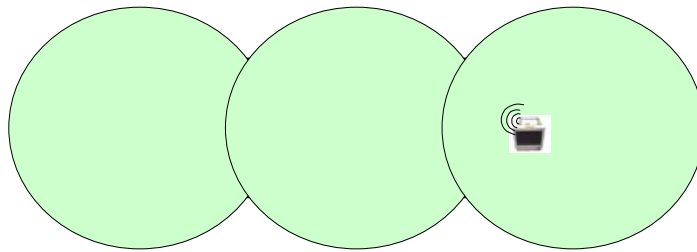
Step 1. To estimate coverage, use circles with a radius of 50 feet (15 m) with the Access Point in the middle.



Caution Position Access Points to avoid both RF Signal Attenuating and RF Interference hazards. To minimize interference from microwave ovens, position Access Points a minimum of 20 feet (6 m) from them.

Step 2. If the customer wants to use the wireless bedside in an area that is larger than the single cell, just add another access point.

Step 3. Keep adding access point cells until the whole area is covered, minimizing overlap:

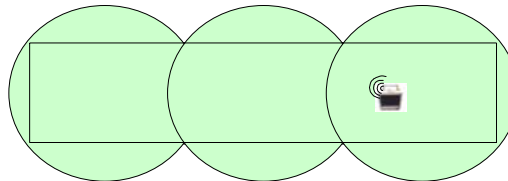


This system has 1 domain and can support 6 Wireless Patient Monitors. To cover 6 more monitors to this system, an additional 3 access points would be required.

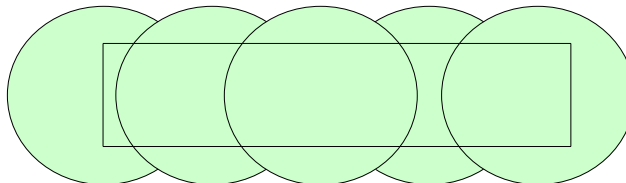
Caution

Coverage Overlap should be avoided. When a wireless patient monitor is used in the coverage overlap area, “passive roaming” occurs. The patient monitor flip flops back and forth between the Access Points which consumes bandwidth and erodes system performance.

Do this:

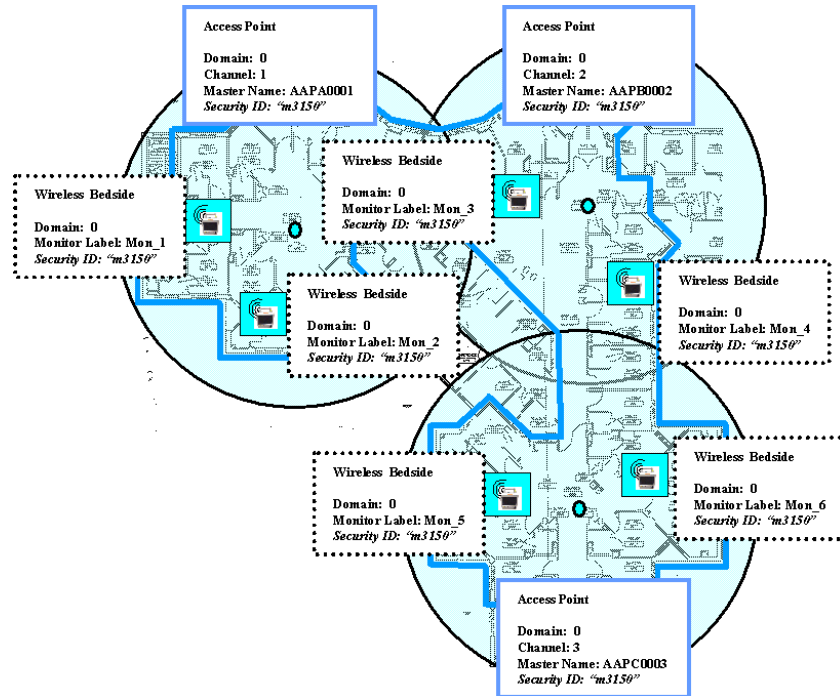


not this



The following figure (Figure 3-6) provides an overview of a standard 2 domain system with 12 M3 monitors. The Access Points and wireless bedside configuration parameters specified.

Domain 0



Domain 1

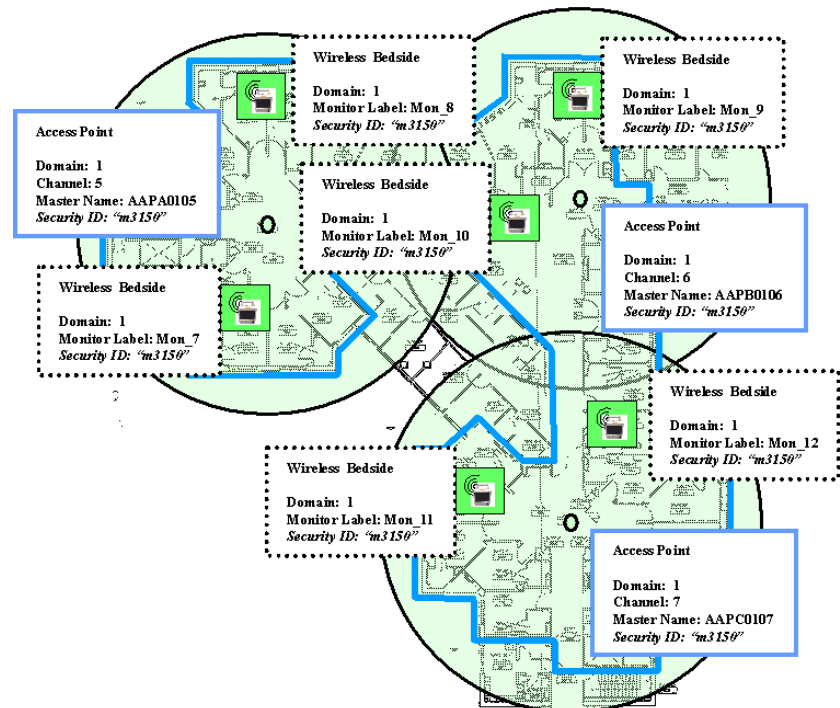


Figure 3-6 Access Point and Wireless Bedside Config Example

Non-Standard System Design

If a system requires more than 15 Access Points, or requires more than 24 wireless M3/M4 Patient Monitors or 12 wireless IntelliVue Patient Monitors, it falls into the Non-Standard category. If the RF characteristics of the site and location of the Access Points permit channel reuse without interference, you can go beyond the 15 Access Point limit.

In order to reuse channels, an RF Data Throughput Survey must show that no significant signal from the first Access Point is picked up in the coverage area of the second access point. This is described in **Checking for Channel Reuse** on page 3-30. If this criteria is not met, it means that interference exists, and it will cause problems.

Caution

To achieve an acceptable performance level, (i.e. dropout rate) access points and cells cannot become overloaded with RF activity. In some sites, the use model and floor plan ensure that overloading will not occur. In other sites, active device management may be necessary (i.e. restricting number of wireless monitors in area of floor).

There are two ways that overloading can occur in a non-standard system:

- Access Point Overloading - too many wireless monitors talking to an access point
 - Monitors have to compete for transmission slots. When there are too many devices, and if there are transmission problems, delays increase.
- Cell Overloading - too many wireless monitors and access points in a single cell
 - Too much RF energy in too small of an area creates an interference problem between devices.

Non-Standard System Example

This non-standard system has a large coverage area, moderate to low bedside density (wireless bedsides per cell), and a low roaming requirement.

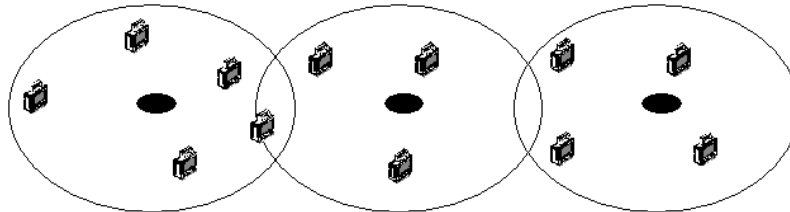
The rules that apply are:

- No more than 6 wireless bedsides per access point
- No more than 2 access points per cell (i.e. no more than 2 stacked domains)
- No more than 12 wireless bedsides in a single cell.

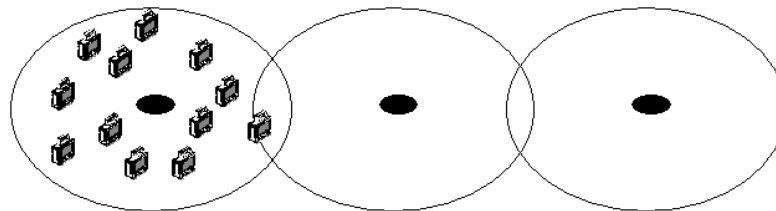
Based on the customer use model, they accept the following restrictions:

- They can allow no more than 6 wireless bedsides in a single cell talking to a single access point
- If more than 6 wireless bedsides do end up talking to a single access point, performance will be degraded (i.e. more dropouts)

A non-standard approach is possible. This non-standard system distributes the 12 wireless bedsides throughout the coverage area so no Access Point will be talking to more than 6 wireless bedsides. This system has only 1 domain, so cell-to-cell roaming is possible:



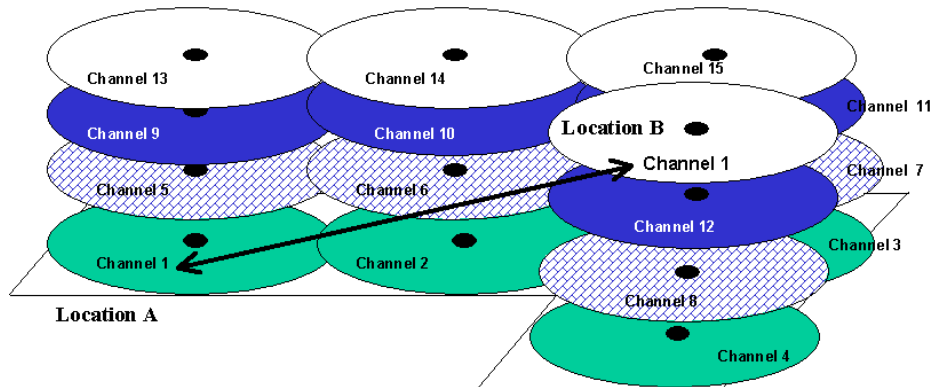
However, unlike the standard system design, if all 12 wireless bedsides were moved into a single cell, **performance would degrade to an unacceptable level:**



Channel Reuse-Example

In this example, 4 Access Points are needed to cover each domain. The customer would like to use 24 wireless bedsides in this unit, for a total of 16 Access Points.

If we look at our channel assignments, one channel would have to be reused:



The data throughput survey would have to confirm that if an Access Point set for Channel 1 is installed at location A, no significant signal is received in the coverage area of the Channel 1 Access Point in location B. See the section Checking for Channel Reuse on page 3-30.

Notes

Channel Reuse interference also applies to systems covering multiple floors.

Channel Reuse criteria also must be checked if there are more than 15 Access Points in use in a hospital even if they are used in different RF systems and operate on different networks.

A building to building survey may be necessary if the facility has a lot of windows and if the buildings are within sight of each other.

RF Survey

After the layout design of the wireless network is completed, a RF Data Throughput Survey must be performed to confirm that the design will work. The data throughput rate of the connection from the wireless bedside to the access point is what is measured in the RF Data Throughput Survey.

Performing the RF Data Throughput Survey

To perform the RF Data Throughput Survey, the following equipment is required:

- Access Point configured using the ConfigTool
- A portable PC
- A Proxim RangeLAN2 PCMCIA card with snap-on antenna
- Floor plan of the coverage area
- Several different color pencils

Step 1. Establish communication between the survey tool and an Access Point (only one is needed for the survey)

- Install the PCMCIA card, the antenna, and the required software driver and tools per the RangeLAN2 User's Guide instructions
- Configure the Access Point. See Device Configuration on page 4-7.
- Power up the Access Point and wait until the Status LED turns green.
- Shut down all programs on the PC. Select Programs\RI2\Pnetcon from the PC Start Menu. If the tool cannot find the Access Point, a dialog box with the message "**Could not find a Master to synchronize with. Verify that your Domain and Security ID match those of a Master**"
 - If this is the first time you are using this equipment, you will need to set the Security ID and Domain of the survey tool to match the Access Point.
 - To set the Security ID:
 - Press **Configuration**
 - Press **Set Security ID**
 - Press **Continue**
 - Enter **m3150** and press **OK**
 - Back in the **Configuration** window, select the correct Domain from the pull-down list to match the Access Point and press **OK**.
- If the tool sees the Access Point, it synchronizes with it and identifies it by its MAC address and its configured Master Name.
- Select **Masters**
- If the tool shows no Access Points in the **Master List** window, select **Search All** in the **Network Domain** area and the tool will cycle through all 16 domains and the Access Point if it finds it. When the Access Point is found, highlight it by clicking on it and then press **Test Link**.

Notes

Make sure the **Packet Size** setting is **1500** and the **Ping Type** is set for **Radio Level**. Close all other programs on the PC when using this tool. If other programs are running on the PC, the numbers may be inaccurate.

- Stand about 10 feet (3 m) from the Access Point:
 - Click on **Reset**
 - Wait 30-40 seconds (see the Total Seconds field in window)
 - The Average Packets/sec (pps) value should be 60-65 at 10 feet (3 m)

Step 2. Temporarily mount the Access Point in the desired location

- Mount the Access Point temporarily at or as close as possible to the desired location for the most accurate results. A network connection is not required. Power must be connected.

Step 3. Using the survey tool, walk the expected coverage area and record the data throughput rate to the Access Point

- Use the floor plan for this step, with all the desired Access Point locations marked.
- Only have one Access Point powered on at a time
- Turn off any wireless bedsides that are on
- At each measurement location:
 - Click on the **Reset** button and wait 30-40 seconds.
 - Write down the **Average** pps
- Go in all patient rooms where patients are expected to be monitored - walk to all corners and check throughput with the room door closed.
- Go in all open areas of hospital, unit, hallways where coverage is desired
- In each area, stand in one spot for 30-40 seconds, and use the Average pps value (coverage area limit is at 50pps)
- Be aware of Radio Hazards
 - Signal Attenuators
 - **Large Metal Objects:** Elevator shafts, large mirrors, metal lockers, large metal medication dispensing systems (i.e. PYXIS), hallway fire doors, fire walls, foil-backed white boards
 - Interference Sources
 - Microwave Ovens, other wireless LANs in use in the hospital

- Mark the Floor plan with the actual Access Point location and the data throughput numbers. Use a different color for each Access Point placement. Try to establish where the 50 pps threshold is. See Figure 3-7.

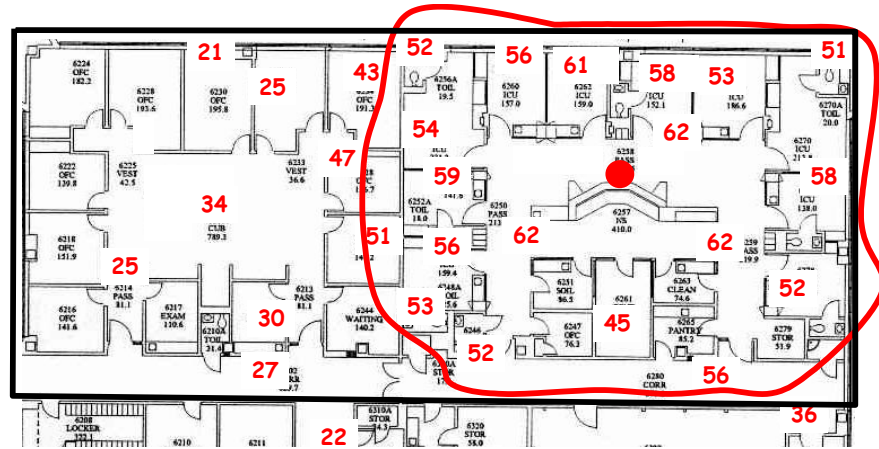


Figure 3-7 Floor Plan with Access Point and Throughput Results

Step 4. Repeat these steps for all of the Access Point locations in one domain - if the system is to have stacked domains, only one domain needs to be checked.

Step 5. Check for inadequate coverage and excessive overlap. See Figure 3-8.

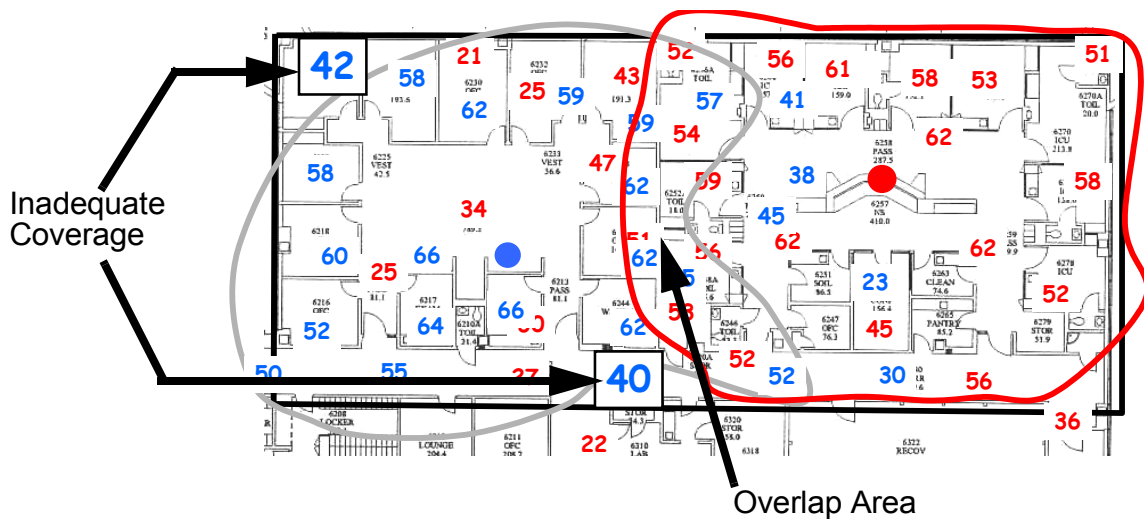


Figure 3-8 Floor Plan with Overlap and Inadequate Coverage Area

Step 6. Adjust the placement of the access points if necessary to ensure adequate coverage and to minimize overlap of the cells. See Figure 3-9.

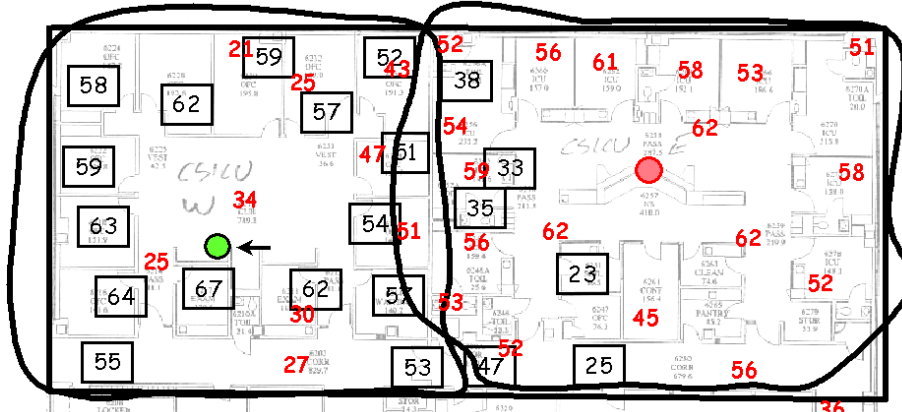


Figure 3-9 Adjusted Design based on Access Point and Throughput Results

Checking for Channel Reuse

If there will be more than 15 access points in the facility, channel reuse is required. RF characteristics of the site must be checked to allow channel reuse without interference between the access points. The RF Data Throughput Survey can also be used to check for channel reuse. You will need two Access Points to perform this test.

- Step 1.** Configure both access points (using the ConfigTool) for the same domain, channel number, and security ID. See Device Configuration on page 4-7.
- Step 2.** Temporarily mount both access points in the desired locations, as close to the actual position as possible. Connect power to both access points.
- Step 3.** Using the survey tool, walk the expected coverage area for each access point (you must be able to get a minimum data throughput reading of 50 pps. **If the readings are less than 50 pps, then the access points are interfering with each other, and channel reuse is not possible.**
- Step 4.** Turn off the access point that is closest to you. Check the data throughput numbers again while you walk the coverage area. The readings should be as close to 0 pps as possible (best performance) but may be no greater than 10 pps.
- Step 5.** Turn the Access Point back on, and turn the other access point off and repeat step 4 in the coverage area of the other access point. **If the readings are greater than 10 pps, the signal strength from the other access point is high enough to interfere and channel reuse is not possible.**

Installing the Clinical Network

Overview

The Clinical Network are the “hidden” components of the Philips Patient Care Network. Network cabling is installed within the walls and ceilings and network components -- switches, media translators -- are generally located in out of the way equipment rooms or wiring closets. These components are rarely seen by clinicians or patients but must be accessible to service personnel. Significant planning and careful network design is required to assure low cost and effective network operation.

A key element of Network installations is network cabling. Philips personnel will assist customers in Network and network cabling design, but cable installation is generally a customer responsibility. The Clinical Network and its components must also be dedicated to Information Center applications and independent of other uses.

Chapter 4 describes the installation of the Clinical Network in the following sections.

Preparing for Installation.	page 4-2
Network Component Installation	page 4-7
Clinical Network Devices: Names and IP Addresses . .	page 4-50

Preparing for Installation

The process for installing a Clinical Network comprises the following general steps. They are described in detail in the following sections.

Cable Plant Installation - of the UTP and fiber optic cable, including patch panels and wall boxes, that will interconnect Clinical Network components.

Unpacking and Inspection - of Clinical Network hardware and software.

Network Component Installation - of active Network components -- switches, repeaters, wireless access points, media translators -- that will support the Clinical Network system.

Information Center, Client, and Server Installation - of Information Centers, Clients, Application Server, and Database Servers in their intended locations, including any required mounting and peripheral equipment -- recorders, UPSs, remote displays.

Printer Installation - of LaserJet printers that will be connected to Network switches.

Network Connections - interconnecting all of the components that will be connected to the Clinical Network.

Cable Plant Installation

Philips requires that the customer contract with a certified CAT5 cable installer for cable plant installation and that the installer provide test documentation that demonstrates that the cable plant meets required specifications.

Note

The hospital cable plant should be completely installed and tested before Philips Representatives and Information Center and Clinical Network/Server equipment arrive.

Installation Materials

Philips supplies a variety of UTP Category 5 (orange colored) cable and installation materials, including bulk UTP cable [in 305 m (1000 ft.) rolls], UTP patch panels, UTP and fiber optic patch cables, and UTP wall boxes. Available options are given in **Table 1-4, M3199AI Passive Components for M3185 Clinical Network**.

Note

Philips does not supply bulk fiber optic cable.

Noise Immunity

UTP CAT5 cable has excellent immunity from noise when installed correctly. To achieve this characteristic, all UTP cables and active network components should be kept as far away as possible from all sources of electrical noise, which includes all RF sources and AC powered devices and their power cables. Data signals on UTP cables that receive excessive electrical noise, e.g. line power surges or spikes, can become corrupted and produce unpredictable results on the networks they support.

When installing the cable plant, UTP cables, patch panels, wall boxes, and active network components should:

- **not** be in wiring closets where RF transmission sources are used
- **not** be placed within 1 m (3 ft.) of any AC device (UPS, CRT, etc.) or AC power cord except where necessary to connect them to workstations or the server

The noise immunity of fiber optic cable is superior to UTP cable so that fiber optic cable should be used for any 10 Mbps cable runs over 100 m for which RF or electrical noise is a potential problem.

UTP Cable Plant Installation

A typical cable plant installation for UTP Category 5 cables for Information Centers, Clients, Application Servers, Clinical Network, and Database Server components is shown in Figure 4-1.

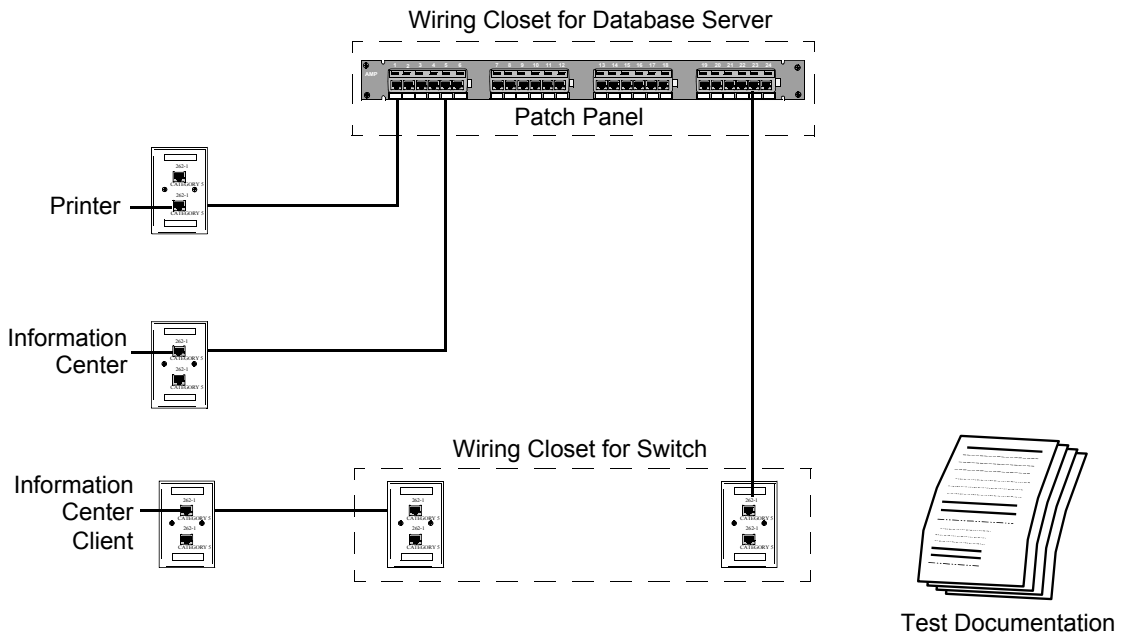


Figure 4-1 Typical UTP CAT5 Cable Plant Installation

The UTP CAT5 cable plant should meet the following:

- **Patch panels for all switches** should be in the wiring closets where switches will be installed
- **RJ-45 wall boxes or patch panels for extension switches** should be in closets where they will be installed. Extension Switches should **not** be located above a ceiling.
- **RJ-45 Wall boxes for Information Centers, Clients, Printers, and Servers** should be within patch cable lengths of their devices.
- **Cabling, patch panels, switches, repeaters, and media translators** should be more than 1 m (3 ft.) from all powered devices (Server, UPS, etc.).

- **Labels on all UTP CAT5 cables and terminations** should identify the cable, patch panel, port number, and wall box termination.
- **Test Documentation** should demonstrate that the UTP CAT5 cable plant meets CAT5 standards for NEXT, attenuation, wiremap, and length.

Caution

In-wall cabling -- UTP and fiber optic -- must be terminated at a patch panel or wall box and not directly at an active Network device.

RJ-45 Connections

RJ-45 connectors should also be securely seated in their sockets. The rubber boot over the end of the connector can be slid back slightly to assure that the connector can be inserted far enough for the connector lock to engage. The boot should then be repositioned over the connector after the connection has been made. The RJ-45 connection should also be tugged lightly after insertion to verify that the connector lock has engaged.

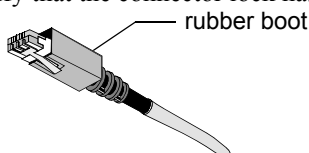


Figure 4-2 RJ-45 Connector

Fiber Optic Cable Plant Installation

Fiber optic cable installation should follow similar installation, testing procedures, and requirements.

Unpacking and Inspection

Once the cable plant has been installed, Information Center, Application Server, Clinical Network, and Database Server hardware and software are ready for installation. The first step is unpacking system components from their shipment containers and thoroughly inspecting them. An inventory Packing List is provided with the shipment for verifying that all ordered components have been received.

Philips Shipments

Some Philips hardware components are manufactured by HP/Compaq and others by other electronic equipment manufacturers. All components for a customer order are consolidated at the Philips Medical Systems facility and shipped to the customer as a complete order. Most components remain unopened and are shipped as they are received.

An **Accessories Box** is also included in the shipment containing a variety of accessories to the Information Center system including:

- Keyboards
- Mouse (or optional Trackball)
- Cables
- Service Kits
- Operating System and Application software CD ROMs and Field Install Support Tool floppy disk

Caution

The Information Center Application and Operating System CD ROMs contain the Application software and the Operating System software. They are a CRITICAL PART of the shipment. Be sure they are carefully unpacked and placed in a secure place for software installation!

Unpacking Components

When the shipment is received by the customer, it should be moved to the installation area but remain unopened. The Philips Service Provider assigned to the installation will remove the components from their packaging and assure the integrity of the shipment. The Philips Service Provider will also remove shipment packaging materials from the customer site if requested.

Checking Inventory

An inventory **Packing List** is included with the shipment. Each shipped item should be carefully checked against the Packing List to assure that it has been received. As items are identified they should be set aside and missing items should be looked for thoroughly. If an item on the Packing List is not found, call the **Response Center** and report the missing item. It will be shipped immediately to the customer site.

Note

An **Archive floppy disk** is attached to the side of the server and workstations. Make certain that it is in place and does not get lost.

Inspection

The Philips system has been carefully packaged at the Philips factory so that no damage should occur in shipment. However, Philips has no control over shipping and handling after it leaves its facility, and a thorough inspection of Philips components after removal from their packaging is an essential step to assuring that no damage has occurred.

Note

Documenting possible damage in shipment may be necessary to support claims for hidden damage that becomes apparent only during testing and operation.

Packaging Inspection

Before removing the components from their packaging, the shipment container should be inspected for damage. External damage to shipping containers may indicate damage to its contents.

Open the shipping containers and check the cushioning material. Note any signs of stress for indications of rough handling in transit. Document any damage conditions.

Mechanical Inspection

Unpack each component from its shipping material. Examine all parts of each component for visible damage -- broken connectors or controls, dents or scratches on instrument surfaces, or any other unusual appearance. Document any damage conditions.

Preparing for Installation

Electrical Inspection No detailed internal or electrical inspection is required. The equipment has undergone extensive electrical testing and configuration prior to shipment and all PC boards and operating software have been pre-installed.

Claims for Damage If physical damage is evident during unpacking or if, during initial testing and operation, the Philips system fails to meet performance specifications in any way, immediately notify the shipment carrier and the nearest Philips Sales/Support Office. Philips will arrange for immediate repair or replacement of the instrument without waiting for any claims to be settled.

Re-packaging for Shipment To ship the system to a Philips Sales/Support Office, the original Philips packaging materials should be used (if at all possible) to provide proper protection during shipping. If the original packaging is not available or reusable, contact the Philips Sales/Support Office, which will provide information on alternative packaging materials and methods.

When addressing the shipment, securely attach a label and include the name and address of the owner, the instrument model and serial number, and a detailed description of any damage, repair required, or symptoms of faults.

Network Component Installation

Once the passive LAN cable plant has been installed and certified, the active Network components can be installed. These components include switches, repeaters, and media translators and will be located in wiring closets designed for that purpose.

Warning

The Database Server and Application Server **must** be connected to a **BATTERY BACKUP** outlet of the 1000 VA UPS.

The following components **must** be connected to the **BATTERY BACKUP** outlets of a UPS: (See Figure 2-18)

- all switches
- media translators
- Harmony Access Point Controller
- workstations for all Information Centers and Clients
- Philips 2 Channel and 4 Channel Recorders

Up to 3 Clinical Network components -- switches, repeaters, media translators -- may be connected to a single, 650VA UPS.

It is **recommended** that Access Points and Harmony Remote Power Supplies also be connected to a 650 VA UPS.

The following components **may** be connected to the **ACCESSORY** outlets of a 650 VA UPS or to a separate non-UPS electrical outlet with the **same ground**.

- displays
- video splitters
- printer spooler

The LaserJet Printer **must not** be connected to the UPS.

Switch Firmware

The switches must be verified to ensure it is running a supported firmware revision. The supported revisions are:

- The HP2524 switch: F.02.02 and F.02.13
- Cisco 1900 Switch: 9.00.04 & 8.01.02

To downgrade to a supported firmware revision, see the procedures beginning on page 5-46.

Device Configuration

The next step is to configure the devices - network switches, RangeLAN2 Access Points, Wireless Patient Monitors, and Access Point Controllers. This includes setting their IP Address. There are two methods of configuring these settings using the **Database Server** or another **PC or laptop** via the ConfigTool (for all devices including switches) or a HyperTerminal connection (for switches only).

Note

Configuration of all network devices is to be done before they are connected to the network.

To connect the Laptop or Database Server to these devices, the following are needed:

- **Network Switches and RangeLAN2 access points:** 9-pin D female - 9-pin D female null modem cable (PN RS232-61601P, 5182-4794P, or HP PN 5184-1894)
- **M3/M4 Wireless Monitors:** 9-pin D female - 1/8 in. male stereo phono cable (PN M1360-61675)
- **Wireless Bedside Adapters:** 9-pin D female - 9-pin D female null modem cable with 9-pin D male - 9-pin D male adapter; or 9-pin D female - 9-pin D male null modem cable

The **configuration tool** for this procedure is contained on the Information Center Application Software CD and must be copied to the PC used for the configuration procedure. The HyperTerminal instructions are given beginning on page 4-29.

The **configuring PC** must meet the following requirements.

- Microsoft Operating System software (Windows 2000 or Windows NT)
- 200 MHz or faster
- RS 232 serial interface port (9-Pin D type connector)

Using ConfigTool

Copying the Configuration Tools to the Configuring PC

Note Some steps (or paths) may differ slightly based on the Operating System and PC Setup.

The first step in the procedure is to copy the configuration tool software from the Application Software CD to the configuring PC.

Step 1. Turn on the configuring PC to display the **Windows Main Menu**. Make sure no applications are running on this PC.

Step 2. Copy the **ConfigTool** software (from the Viridia\Tools directory) to a folder on the configuring PC to be used for storing this program.

Note The **ConfigTool** software files are less than 1.4 Mb so it can be stored on a 1.4 Mb floppy disk for later use or for transfer to a PC.

Making the Config Files Writable

The **ConfigFiles** are read-only and must be made writable for the tool to be used for configuration. The following steps describe the procedure after the files have been copied to the configuring computer:

Step 3. Open the **ConfigFiles** directory by clicking on the **ConfigFiles** folder in the menu on the configuring PC.

Step 4. Select all ***.CFG** files as follows:

- Click on one of the files
- Hold down the keyboard **Ctrl** key and simultaneously click on the other files

- Release the **Ctrl** key

Note

The selected files must be made writable because settings used in the configuration process are saved to this file so they can be reused when the configuration tool is used again.

Step 5. Place the cursor over any of the highlighted fields and **right-click** the mouse to display a menu listing **Properties**, as shown in Figure 4-3.

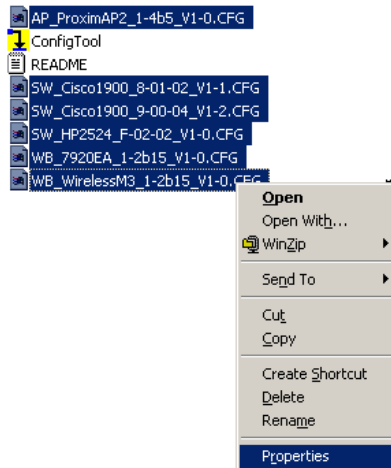


Figure 4-3 File Menu Showing Properties

Step 6. Click on **Properties** to display the selected file's **Properties** window.

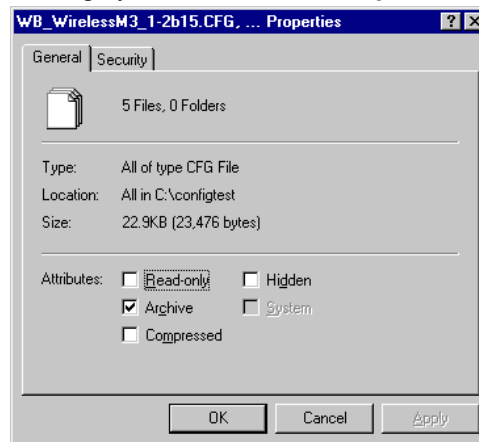


Figure 4-4 File Properties Window

Step 7. Click in the **Attributes:** box preceding **Read-only** to **remove the check**. This removes **Read-only** from the selected files (shown in Figure 4-4).

Note

If the configuration tool is run with this file set as **Read-only**, the following error message will be displayed. Clicking **OK** will exit the tool and the **Read-only** attribute must be removed to clear this condition.



Running the Configuration Tool

Once the tool has been copied and made writable, it can be run. The first step is to select which device -- Access Point, Switch, or Wireless Monitor -- to configure.

Step 8. Run the configuration tools as follows:

- select **Start** -> **Run** in the Windows Main menu
- click **Browse** to access the **Browse** application
- select **ConfigTool** in the menu of the stored configuration tools files
- locate the file **ConfigTool.exe** in the ConfigTool directory
- double click on **ConfigTool.exe** to enter it into the **Open:** field of the **Run** window.
- click **OK** to open the **Configuration Tool** window of Figure 4-5.

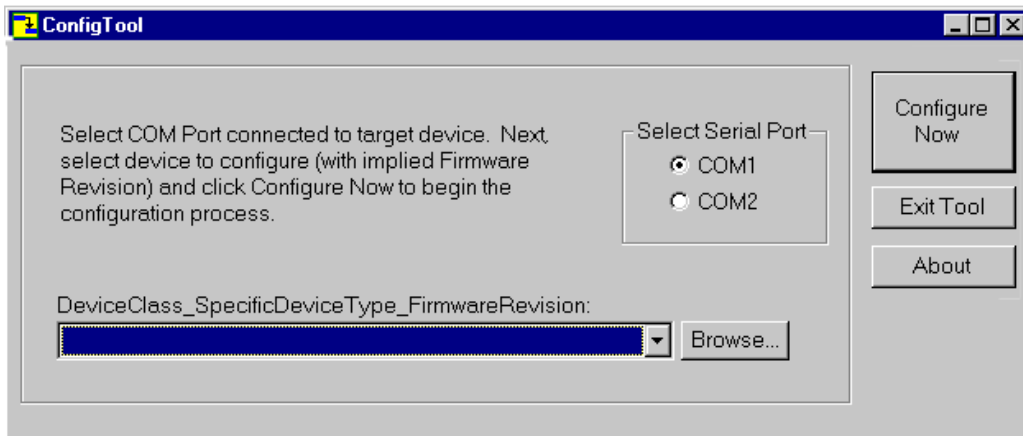


Figure 4-5 Configuration Tool Window

The Configuration Tool Window is used to select the Serial Port (**COM1** or **COM2**) on the configuring PC that will be used to perform the configuration and the configuration file for the device being configured -- **Access Point, Network Switch, or Wireless Bedside.**

Step 9. Select the Serial Port to be used (**COM1** or **COM2**) in the Select Serial Port field by clicking in the circle preceding the appropriate port.

Step 10. Select the appropriate Device to Configure in the drop down list in the **Configuration Tool** window of the configuring PC. See Figure 4-5.

Step 11. In the Configuration File field, select:

- **SW_HP2524*.cfg** for HP2524 Network switch or **SW_Cisco1900_*.CFG** for the Cisco switches (make appropriate selection based on firmware revision).
- **AP_ProximAP2*.CFG** for RangeLAN2 Access Points
- **WB_WirelessM3*.CFG** for M3/M4 Monitors
- **WB_7290*.CFG** for IntelliVue Patient Monitors

Note If this file does not automatically appear in the Configuration File field, click **Browse** and find this file on the computer drive directory where it was stored.

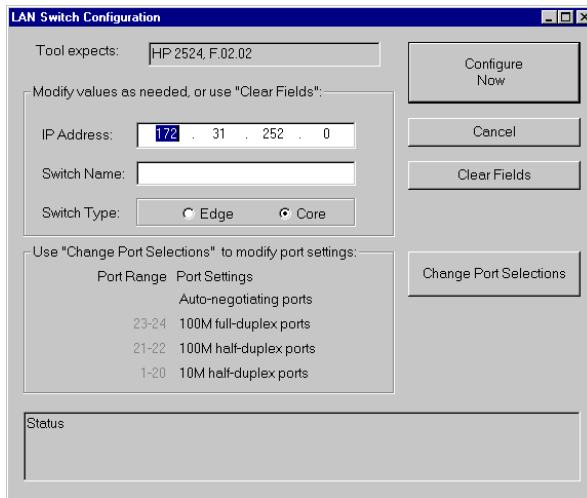
Network Switches

Step 1. Plug one end of the 9-pin D female - 9-pin D female cable into the configuring PC.

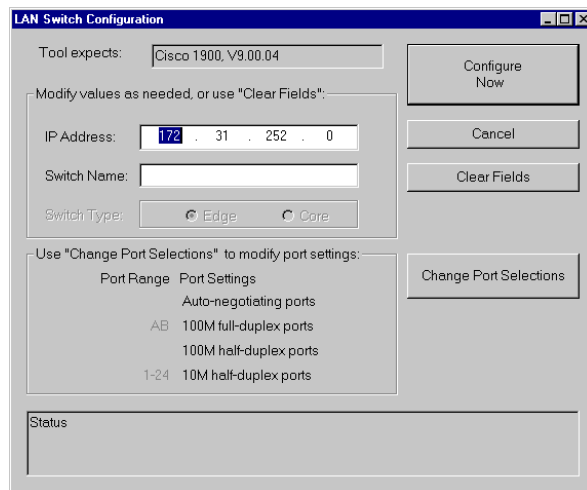
Step 2. Plug the other end of the cable into the **CONSOLE** port on the front of the HP ProCurve 2524 switch, as shown in Figure 2-1 (for CISCO switches, the **CONSOLE** port is on the rear panel).

Note If a firmware mismatch error opens, the switch must be restored to a supported firmware revision. The HP2524 switch supports F.02.02 and F.02.13. See **Restoring Switch Firmware - HP2524** on page 5-46 or **Switch to Switch Firmware Restore** on page 5-49

Step 3. Click **Configure Now** in the Configuration Tool window of Figure 4-5 on the configuring PC to open the **LAN Switch Configuration** window of Figure 4-6.



HP2524 Network Switch



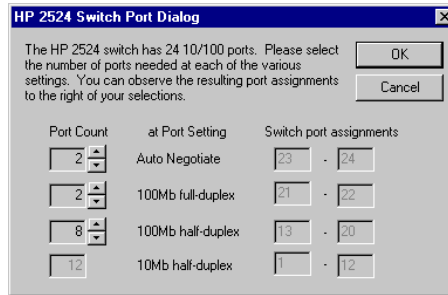
Cisco 1900 Network Switch

Figure 4-6 Network Switch Configuration Window

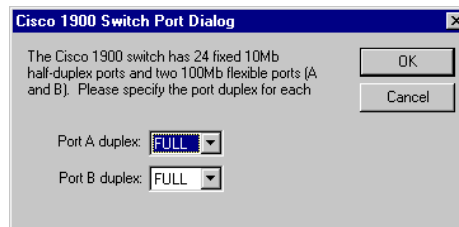
Step 4. Enter the requested information in the Switch Name, Switch Type (only 1 Core switch permitted per Database Server system). This information should have been recorded in the worksheets in Appendix A.

Step 5. Select **Change Port Selections** to configure the appropriate number of Full/Half Duplex Settings for the Network Switch being configured. Table 3-1, Network

Device Requirements with Applicable Port Settings lists all the Network devices and their required speed and duplex settings. Click **OK** when finished.



HP2524 Network Switch



Cisco 1900 Network Switch

Figure 4-7 Network Switch Port Configuration Window

For the HP2524 switch, both speed and duplex settings must be set for the switch, starting at port 24 and working down. In the example above, 2 Auto Negotiate ports are assigned to ports 24 and 23, two 100 Mbps full duplex ports are assigned to ports 22 and 21. The remaining ports are configured as eight 100 Mbps half duplex and 12 10 Mbps half duplex.

For the Cisco switch, port A (top) is the Fiber Port, and port B (bottom) is the UTP port.

Caution

On Cisco switches, do not select Auto-Negotiate for Port A, or Half Duplex on Port A or Port B, as this is not supported. If these settings are selected, system performance will be degraded.

Step 6. Click **Configure Now** to initiate the Network Switch configuration.

Note

If an error message appears, see **Troubleshooting** at the end of this section.

The configuration process takes about 3 minutes. During configuration, status messages will be displayed in the field at the bottom of the **Network Switch Configuration** window as the tool resets the configuration to factory default values, sets the configuration parameters, and then resets the Network Switch.

Step 7. Repeat **Steps 1** through **6** for other Network Switches on the system.

**RangeLAN2
Access Points**

Step 1. Connect one end of the 9-Pin D Female - 9-Pin D Female cable to the 9-pin D Male Serial Port connector on the configuring PC and the other end to the **Serial** port on the rear panel of the RangeLAN2 Access Point to be configured. See Figure 4-8.

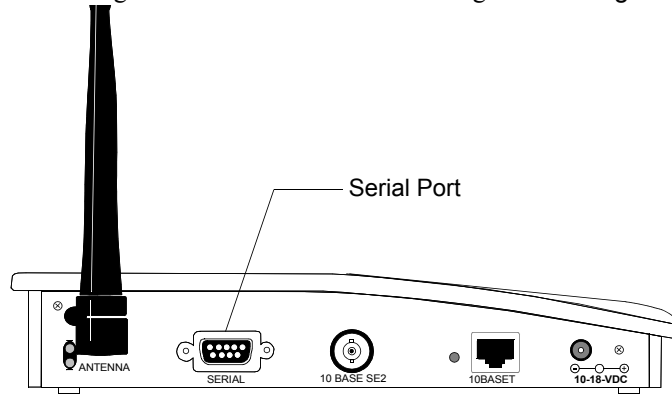


Figure 4-8 Rear Panel of RangeLAN2 Access Point

Step 2. Turn on the Access Point and insure that it passes its self-test by waiting for the Status LED **1** on the top of the of the Access Point to turn green. This will take about 20 - 30 seconds

Step 3. Click **Configure Now** in the Configuration Tool window of Figure 4-5 on the configuring PC to open the **Access Point Configuration** window of Figure 4-9.

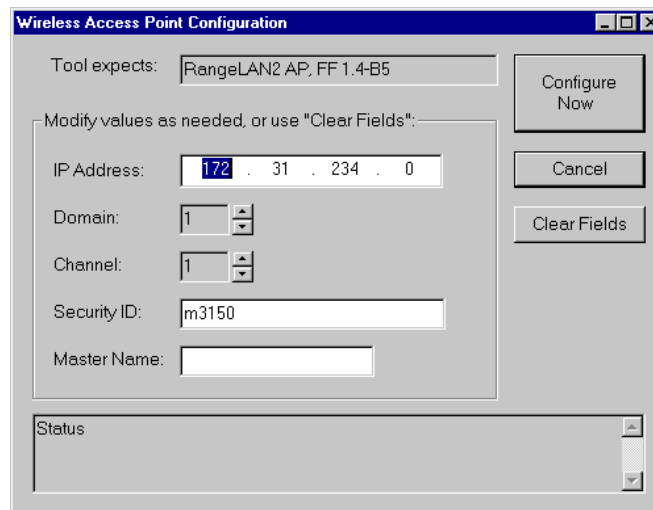


Figure 4-9 Access Point Configuration Window

Step 4. Enter the requested information in the Modify Values as needed, or use “Clear Fields” for the Access Point being configured. This information should have been recorded on the Access Point Configuration Attributes Worksheet provided in Appendix A. Figure 3-6 shows an example of a configuration of a 2 domain system with Access Points and Bedsides. The parameters are:

- **Domain:** A set of contiguous cells that covers all of the desired coverage area. All Access Points and associated wireless monitors must be configured with the same

domain number. The valid range is 0-15. If there is more than one domain in an RF system, each domain must have a different domain number.

- **Channel:** a number between 1 and 15. The bedside changes channels while roaming between Access Points. In order to roam properly, adjacent cells (i.e. Access Points) cannot have the same channel number. Also consider interference with Access Points in other domains, other systems, and in other areas of the hospital. To minimize interference, do not reuse channels.
- **Security ID:** is a alpha-numeric string that is added to every packet of data sent over the wireless link. This security ID insures that no foreign wireless LAN devices exchange data with our devices. **Keep the default entry m3150**
- **Master Name:** a unique name used to identify this device in network manager applications. It should be the same as its **Device Name** in **Network Configuration** on the Database Server. It has a limit of 11 characters.

Step 5. Click **Configure Now** to initiate the Access Point configuration.

Note

If an error message appears, see **Troubleshooting** at the end of this section.

The configuration process takes about 3 minutes. During configuration, status messages will be displayed in the field at the bottom of the **Access Point Configuration** window as the tool resets the configuration to factory default values, sets the configuration parameters, and then resets the Access Point.

When the tool has successfully completed the configuration, the **Access Point Configuration is completed successfully** window of Figure 4-10 appears.

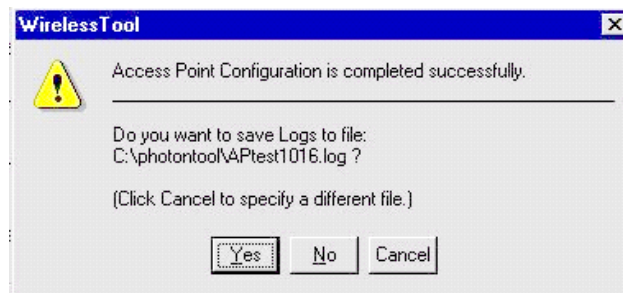


Figure 4-10 Configuration Completion Window

The configuration tool will write the configuration dialog and summary information to a file if you wish. It will create a **Log file** name by combining **AP**, **Master Name**, and the **last octet** of the IP Address entered in the Access Point Configuration window.

Step 6. Create a **log file** of the Access Point configuration as follows:

If you want to create a log file with the **Log file** name given:

- click **Yes** and a **log file** containing the text of the menu dialog between the configuring computer and the Access Point will be created and stored in the **ConfigTool** directory of the configuring computer's hard drive.

Note The **log file** is a **.txt** file that contains the menu dialog of the most recent configuration. Near the end of this file is a summary of the device's configuration settings. This file may be viewed in **Notepad** or printed for later reference.

There are several configuration settings for the Access Point that are made by the configuration tool that are not site specific but are different from factory default settings. These settings can be seen in the log file, but are not displayed to the user when the tool is used.

If you do not want to create a log file:

- click **No** to close this window.

If you want to specify a **different filename**:

- click **Cancel** and a window will open allowing the specification of a different filename.
 - enter the **new filename** in the field provided.
 - click **Yes** to create the new filename
-

Note If a **filename** is entered for which a configuration file already exists, that file will be overwritten by the new file.

Configuration of this Access Point is now complete.

Step 7. Remove the 9-Pin D connector from the rear of the Access Point.

If there are additional Access Points to be configured:

Step 8. Repeat **Step 1** through **Step 7** for each Access Point to be configured.

Note The **Configuration Tool** retains the parameter values entered when it was previously run. For each subsequent Access Point configured, enter the parameters for that Access Point in the Access Point Configuration window of Figure 4-9.

M3/M4 Monitors **Step 1.** Turn **OFF** the power of the Wireless M3/M4 Monitor and disconnect any cable connected to the RJ-45 port on its rear panel.

Step 2. Unsnap the gray cover on the upper right side of the M3/M4 Monitor housing to expose the female stereo phono plug on the Wireless Adapter, as shown in Figure 4-11.



Figure 4-11 Stereo Phono Plug on Wireless Adapter of M3/M4 Monitor

Step 3. Connect the phono plug end of the 9-Pin D female - 1/8 in. male Stereo Phono cable into the phono plug connector on the Wireless Adapter as shown in Figure 4-11 and the 9-pin D end of the cable into the 9-Pin D Serial Port connector on the configuring PC.

Step 4. Turn **ON** the M3/M4 Monitor and insure that it passes its self-test.

Step 5. Select the **WB_WirelessM3_1-2b15.cfg** item in the drop down list in the **Configuration Tool** window of Figure 4-5.

Step 6. Click **Configure Now** to open the **Wireless Bedside Parameters** window of Figure 4-12.

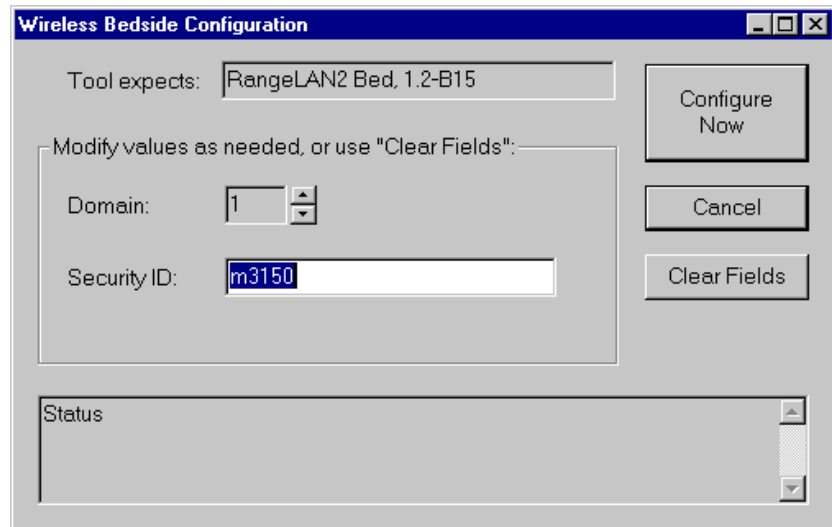


Figure 4-12 Wireless Bedside Parameters Window

Step 7. Enter the requested information in the Modify values as needed, or use “Clear Fields” for the M3/M4 being configured. This information should have been recorded on the Wireless M3/M4 Monitor Configuration Attributes Worksheet provided in Appendix A. Figure 3-6 shows an example of a configuration of a 2 domain system with Access Points and Bedside.

- **Domain:** A set of contiguous cells that covers all of the desired coverage area. All Access Points and associated M3/M4 monitors must be configured with the same domain number. The valid range is 0-15. If there is more than one domain in an RF system, each domain must have a different domain number.
- **Security ID:** is a alpha-numeric string that is added to every packet of data sent over the wireless link. This security ID insures that no foreign wireless Network devices exchange data with our devices. **Keep the default entry m3150.**

This configuration process takes about 1 minute. During configuration, status messages will be displayed in the field at the bottom of the **Wireless Bedside Parameters** window as the tool resets the configuration to factory default values, sets the configuration parameters, and then resets the Wireless Adapter.

When the tool has successfully completed the configuration, the **Wireless Bedside Configuration is completed successfully** window of Figure 4-13 appears.

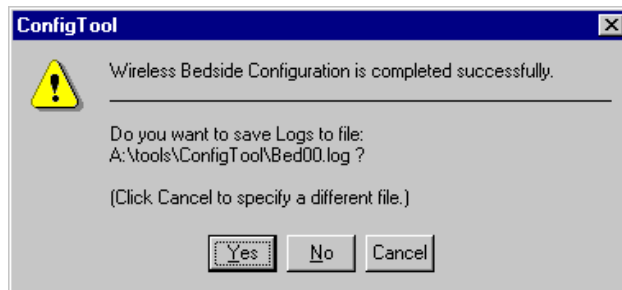


Figure 4-13 Configuration Completion Window

The configuration tool will write the configuration dialog and summary information to a file if you wish. It will create a **Log file** name by combining **Bed** and the **2 digits** of the **Domain** entered in the **Wireless Bedside Parameters** window.

Step 8. Create a **log file** of the Wireless Bedside configuration as follows:

If you want to create a log file with the **Log file** name given:

- click **Yes** and a **log file** containing the text of the menu dialog between the configuring PC and the Wireless Adapter will be created and stored in the **ConfigTool** directory of the configuring computer's hard drive.

Note

The **log file** is a **.txt** file that contains the menu dialog of the most recent configuration. Near the end of this file is a summary of the device's configuration settings. This file may be viewed in **Notepad** or printed for later reference.

There are several configuration settings for the M3/M4 monitor that are made by the configuration tool that are not site specific but are different from factory default settings. These settings can be seen in the log file, but are not displayed to the user when the tool is used.

If you do not want to create a log file:

- click **No** to close this window.

If you want to specify a **different filename**:

- click **Cancel** and a window will open allowing the specification of a different filename.
- enter the **new filename** in the field provided.
- click **Yes** to create the new filename

Note If a **filename** is entered for which a configuration file already exists, that file is overwritten by the new file.

Configuration of this Wireless Adapter is now complete

Step 9. Remove the phono plug from the rear of the Wireless Adapter and replace the cover.

If there are additional Wireless M3/M4 Monitors to be configured:

Step 10. Repeat **Step 1** through **Step 9** for each to be configured.

Note The **Configuration Tool** retains the parameter values entered when it was previously run. For each Wireless Adapter configured, enter the parameters for that Wireless Adapter in the **Wireless Bedside Parameters** window of **Figure 4-12**. It is possible that all of the Wireless M3/M4 Monitors in a system will have the same configuration parameters.

When all Wireless M3/M4 Monitors have been configured:

Step 11. Click **Close** in the upper right corner of the Configuration Tool of **Figure 4-5**.

Wireless Bedside Adapters

Step 1. Connect one end of the 9-Pin D Female - 9-Pin D Male cable to the 9-pin D Male Serial Port connector on the configuring PC and the other end to the **Serial** port on the rear panel of the wireless adapter to be configured.

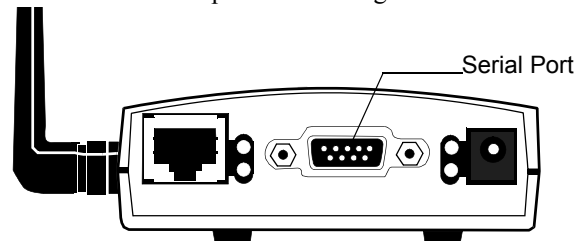


Figure 4-14 Wireless Adapter Serial Port

Step 2. Power on the adapter (if pre-configuring without connection to the IntelliVue Patient Monitor, use the power supply included with the adapter; otherwise connect the adapter to the bedside and power on). Ensure that it passes its self-test by waiting for the Status LED **1** on the top to turn green.

Step 3. Click **Configure Now** in the Configuration Tool window of Figure 4-5 on the configuring PC to open the **Wireless Adapter Configuration** window of Figure 4-15.

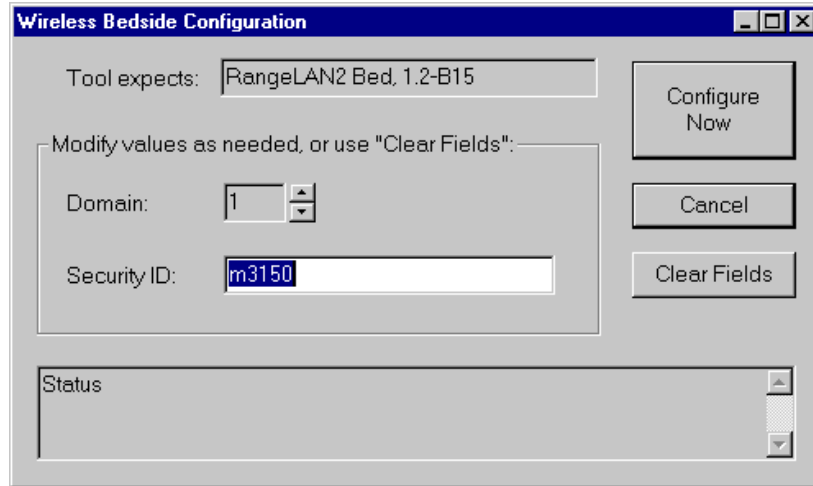


Figure 4-15 Wireless Adapter Window

Step 4. Enter the requested information in the Domain or Security ID fields for the Wireless Adapter being configured. The parameters are:

- **Domain:** A set of contiguous cells that covers all of the desired coverage area. All Access Points and associated wireless monitors must be configured with the same domain number. The valid range is 0-15. If there is more than one domain in an RF system, each domain must have a different domain number.
- **Security ID:** is a alpha-numeric string that is added to every packet of data sent over the wireless link. This security ID insures that no foreign wireless LAN devices exchange data with our devices. **Keep the default entry m3150.**

This configuration process takes about 1 minute. During configuration, status messages will be displayed in the field at the bottom of the window as the tool resets the configuration to factory default values, sets the configuration parameters, and then resets the Wireless Adapter.

When the tool has successfully completed the configuration, the **Wireless Bedside Configuration is completed successfully** window of Figure 4-16 appears.

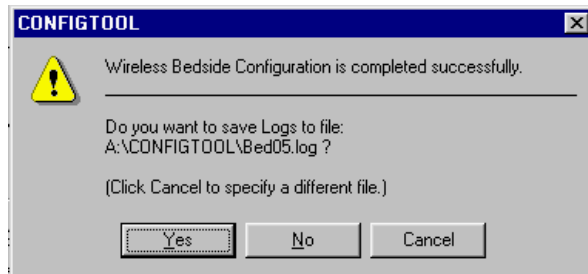


Figure 4-16 Configuration Completion Window

The configuration tool will write the configuration dialog and summary information to a file if you wish. It will create a **Log file** name by combining **Bed** and the **2 digits** of the **Domain** entered in the **Wireless Bedside Parameters** window.

Step 5. Create a **log file** of the Wireless Bedside configuration as follows:

If you want to create a log file with the **Log file** name given:

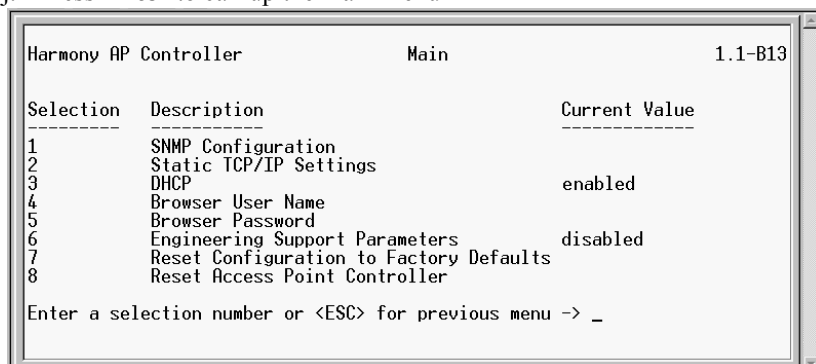
- click **Yes** and a **log file** containing the text of the menu dialog between the configuring PC and the Wireless Adapter will be created and stored in the **tools\ConfigTool** directory of the configuring computer's hard drive.

Access Point Controllers & Harmony Access Points

Before the Harmony Access Point Controller (APC) can be installed and configured, the Database Server must be configured to include the APC. Mounting hardware for rack or wall mounting is provided with the devices, although they can be placed on a horizontal shelf or table.

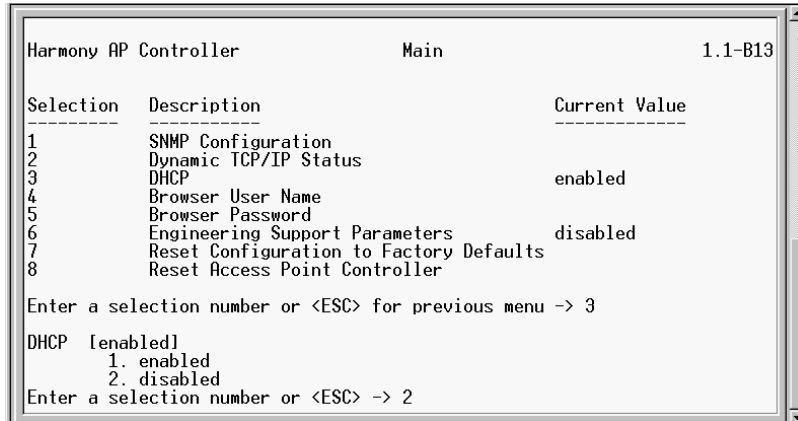
Step 1. Using HyperTerminal, set the IP Address of the APC:

- a. Connect power and turn on the APC
- b. Connect one end of a null modem cable to the serial port of the APC and the other end to the serial port of the configuring PC.
- c. Open the HyperTerminal application.
- d. Click on **File -> Properties** to open the **New Connection Properties** window.
- e. Click **Connect to**.
- f. Click on the **Connect Using** pull down arrow to display its menu.
- g. Click on **COM1** (or **Direct to COM1**).
- h. Click **Configure**.
- i. Configure the **COM1** port to the following RS 232 settings:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
- j. Press **Enter** to call up the main menu

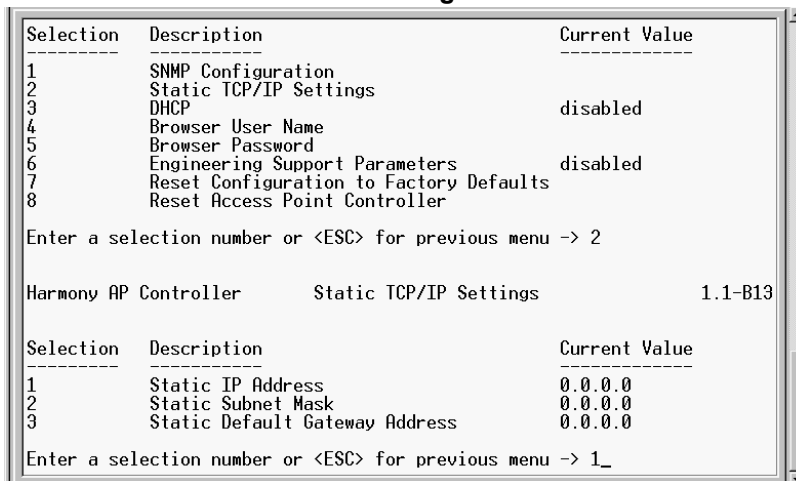


- k. Select **7** to **Reset the APC to Factory Defaults**

- l. Enter **3** to select the **DHCP** menu.
- m. Enter **2** to disable DHCP



- n. Enter **2** for the **Static TCP/IP Settings** menu.



- o. Enter **1** and enter the **Static IP Address**
- p. Enter **2** and enter the **Static Subnet Mask**
- q. Enter **3** and enter the **Static Default Gateway Address**
- r. Enter **ESC** to return to the Main Menu

- s. Enter **8** to **Reset the Access Point Controller**

Selection	Description	Current Value
1	Static IP Address	172.31.238.0
2	Static Subnet Mask	255.255.0.0
3	Static Default Gateway Address	172.31.241.0
Enter a selection number or <ESC> for previous menu ->		
Harmony AP Controller		Main 1.1-B13
Selection	Description	Current Value
1	SNMP Configuration	
2	Static TCP/IP Settings	
3	DHCP	disabled
4	Browser User Name	
5	Browser Password	
6	Engineering Support Parameters	disabled
7	Reset Configuration to Factory Defaults	
8	Reset Access Point Controller	
Enter a selection number or <ESC> for previous menu -> 8_		

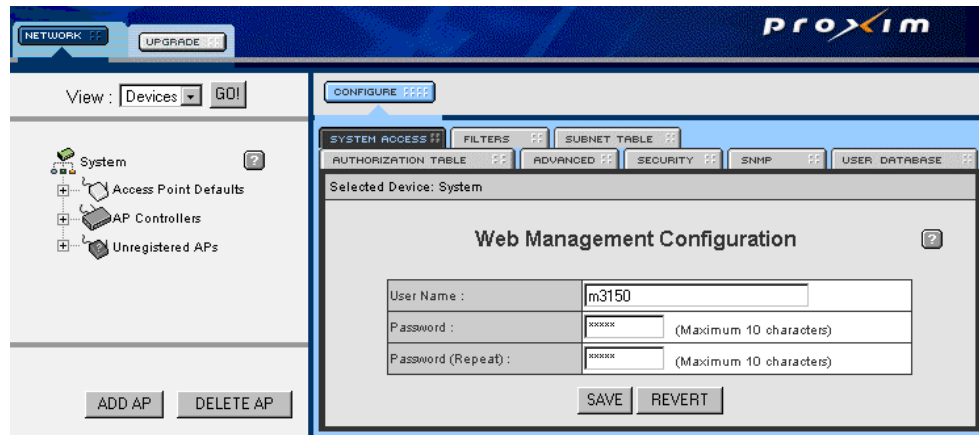
- t. Close the HyperTerminal session.

Step 2. Access the APC web interface (**All Controls -> Service -> Support Logs -> Network Statistics -> Select IP Address or Search by IP Address**), and configure the appropriate System parameter settings.

Note

The configurations settings defined below are the only required changes from the factory default configurations.

- a. Select the  icon to view the Web Management Configuration screen



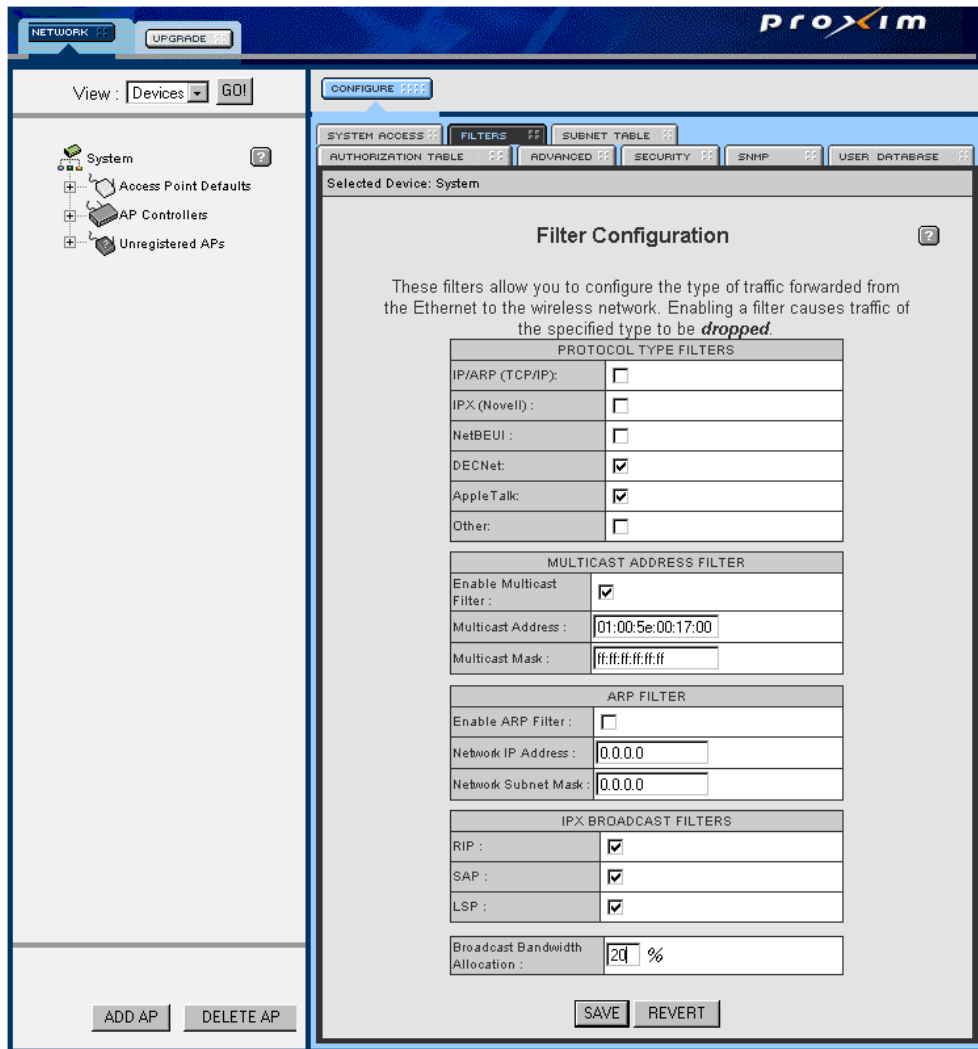
Change the settings as follows:

User Name
Password

Enter a name for this APC
Password (case sensitive)

Click the **Save** button.

b. Click on the **Filters** tab.




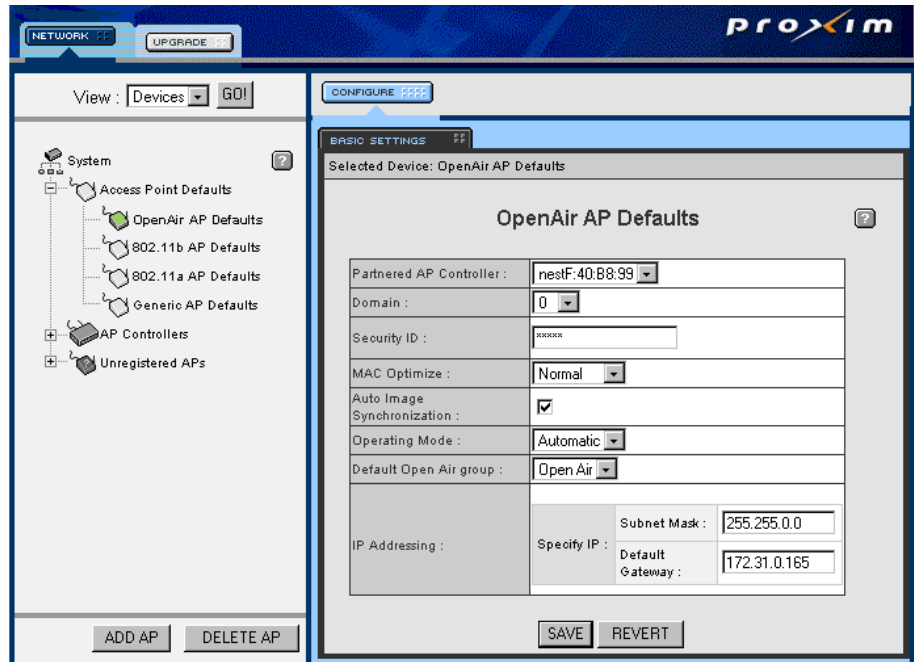
Change the settings as follows:

Enable MultiCast Filter	Enable
MultiCast Address	01:00:5e:00:17:00
Multicast Mask	ff:ff:ff:ff:ff:ff
Bandwidth Broadcast Allocation	20%

Click the **Save** button.

Step 3. Configure the appropriate Access Point Default settings.

- a. Select the  icon and then OpenAir AP Defaults to view the OpenAir AP Defaults screen:



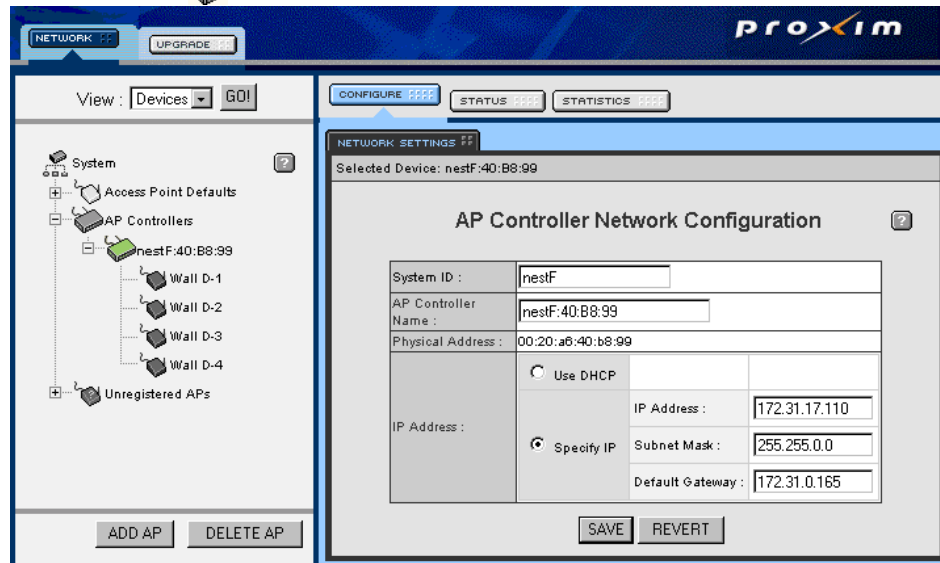
Change the settings as follows:

Partnered AP Controller	set to a configured APC (site specific)
Security ID	m3150
MAC Optimize	Normal
Subnet Mask	255.255.0.0
Click the Save button.	

Step 4. Configure the APC settings.

Network Component Installation

- a. Select the  icon to view the AP Controller Network Configuration screen



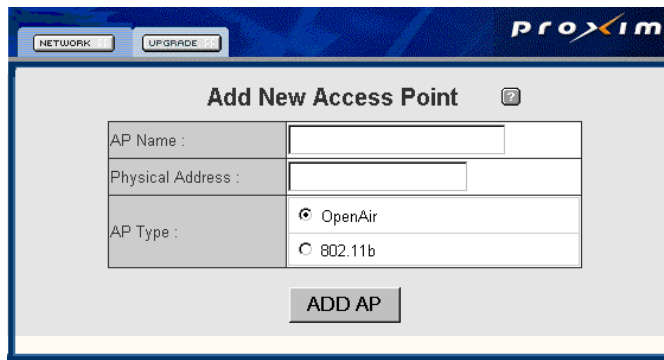
Verify the settings are as follows:

IP Address	set to IP Address (site specific)
Subnet Mask	255.255.0.0
AP Controller Name	Set to desired name (site specific)

Click the **Save** button.

Step 5. Add Harmony access points.

- a. Click on the **Add AP** button. The **Add New Access Point** screen opens.



- b. Add in the following settings:

AP Name	enter name (site specific)
---------	----------------------------

Physical Address

physical address taken from bottom label on access point:

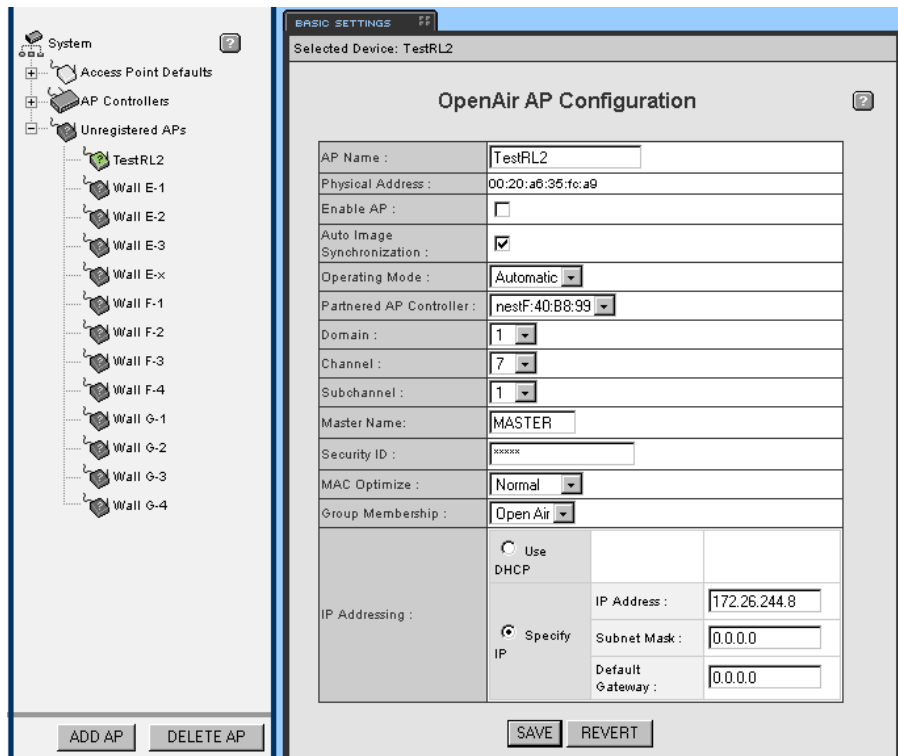


AP Type

Open Air

Click the **Add AP** button to add more Harmony access points, or the **Network** tab to close this window.

Step 6. After all Harmony access points have been added, click the to configure these unregistered access points.



a. Select the access point to be configured. Verify the following settings:

- AP Name
- Partnered AP Controller
- Domain
- Channel
- Security ID

- User defined name
- select APC from list
- select appropriate Domain*
- select appropriate Channel**
- m3150

MAC Optimize
IP Address

Normal
enter supported IP Address

Click the **Save** button.

***Domain:** A set of contiguous cells that covers all of the desired coverage area. All Access Points and associated wireless monitors must be configured with the same domain number. The valid range is 0-15. If there is more than one domain in an RF system, each domain must have a different domain number.

****Channel:** a number between 1 and 15. The bedside changes channels while roaming between access points. In order to roam properly, adjacent cells (i.e. access points) cannot have the same channel number. Also consider interference with access points in other domains, other systems, and in other areas of the hospital. To minimize interference, do not reuse channels.

Refer to Chapter 3 for Domain and Channel design considerations

Configuration Troubleshooting

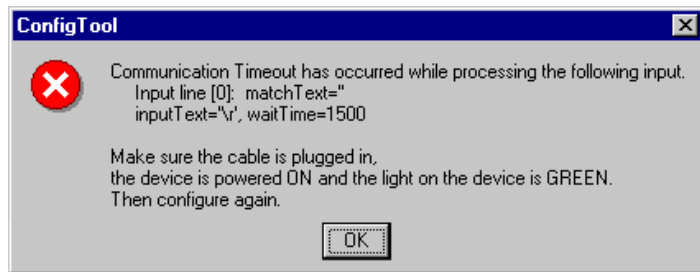
If an error should occur during the configuration process, one of the following troubleshooting procedures may resolve the problem.

If the **Read-only** attribute has not been removed from the configuration tool files, the following error message will be displayed.



- Click **OK** to exit the tool and remove the **Read-only** attribute following the procedure described in **Making the Config Files Writable**.

If the serial cable connecting the configuring PC to the device or the PC's **COM** port is inaccessible or not working, one of the following windows will be displayed:



RangeLAN2 Access Point




Wireless Bedside

Figure 4-17 Configuration Tool Error Window

- Check the serial cable and its connections carefully to assure that a good interconnection is being made
- Insure that no other applications in the configuring PC have control of its Serial Port (e.g. Hyperterminal). Close all other applications.
- Insure that the proper **COM** port is selected in the **Configuration Tool** window of Figure 4-5.
- Refresh the Hyperterminal application by logging off the console session, and then logging back in.

If configuring an **Access Point**:

- Turn the Access Point **Off** and then **On** and insure that it passes its self-test by waiting for the Status LED  on the top of the of the Access Point to turn green. Restart the **Configuration Tool** and try the procedure again.

If configuring a **Wireless Bedside**:

- Turn the Wireless M3/M4 Monitor **Off** and then **On** and insure that it passes its self-test. Restart the **Configuration Tool** and try the procedure again.

Using HyperTerminal Connection

A HyperTerminal Connection can be used to configure the Network switches (both HP2524 and Cisco1900). Based on the firmware revision of the switch, follow the appropriate procedure.

The **configuring PC** must meet the following requirements.

- Microsoft Operating System software (Windows 2000 or Windows NT)
- 200 MHz or faster
- RS 232 serial interface port (9-Pin D type connector)

HP2524 Switches

Verify a supported Firmware version is installed: F.02.02 or F.02.13. If another version of Firmware is installed, the Firmware must be restored, see **Restoring Switch Firmware - HP2524** on page 5-46. If the configuring PC is the Database Server using Hyperterminal from Port A, the UPS connection must be temporarily removed and disabled. The following steps describe the procedure.

Step 1. Plug one end of the 9-pin D female - 9-pin D female cable into the RS 232 connector of the configuring PC

Step 2. Plug the other end of the cable into the **CONSOLE** port on the front of the HP ProCurve 2524 switch. If you are NOT using the Database Server as a configuring PC, skip to step 11.

Step 3. Turn On the PC and Switch

If the Server's UPS service detects that the UPS is not connected to Serial Port A, a message indicating **At least one service failed to initialize...** may appear.

If this message appears:

Step 4. Click **OK** and proceed to **Step 11**.

If this message **does not** appear:

Step 5. Go to the **Control Panel** and double click on the **Services** icon (2 gears) to open the **Services** window.

Note Some steps (or paths) may differ slightly based on the Operating System and PC Setup.

Step 6. Scroll down the list of **Services** to **UPS**.

Step 7. Click on **UPS** to highlight it.

Step 8. Click on the **Stop** button to disable the UPS connection.

Step 9. Click **Yes** to the **Are you sure..** message. A momentary **Attempting to stop...** message will then appear.

When the UPS connection has been disabled:

Step 10. Close the **Services** window and **Control Panel**.

Step 11. Open **HyperTerminal**.

Note If a **Connection Description** window appears, click **Cancel** to close it.

Step 12. Click on **File** in the New Connection - HyperTerminal window to display its menu.

Step 13. Click on **Properties** to open the **New Connection Properties** window.

Step 14. Click on the **Connect to** tab to display its menu.

Step 15. Click on the **Connect Using** pull down arrow to display its menu.

Step 16. Click on **COM1** (or **Direct to COM1**).

Step 17. Click on **Configure** to display the **COM1 Properties** window.

Step 18. Configure the COM1 port to the following settings:

Bits per second: 9600
 Data bits: 8
 Parity: None
 Stop bits: 1
 Flow control: Xon/Xoff

Step 19. Press **Enter** twice to get to the command line. If the command line does not appear, recycle power on the switch (disconnect and connect power cable).

Step 20. Enter the following commands at the command line prompt:

Note If a prompt appears asking for a password, type in **m3150**.

- **erase startup-config** (press **Y** to confirm)
- **config**
- **console inactivity-timer 10**
- **hostname <<hostname>>** (where <<hostname>> is the name of the switch)
- **vlan 1 ip address 172.31.252.1/255.255.0.0**

Note The recommended IP Address for the **first switch** should be **172.31.252.0**
 The recommended IP Address for a **second switch** should be **172.31.252.1**, etc
 The recommended IP Addresses for the switches **must be different**

- **int e 1-<<xx> speed-duplex 10-half** (to set ports 1-xx to 10 Mb/s Half Duplex)
- **int e <<xx> speed-duplex 100-half** (to set port/s <<xx>> to 100 Mb/s Half Duplex)
- **int e <<xx> speed-duplex 100-full** (to set port/s <<xx>> to 100 Mb/s Full Duplex)
- **int e <<xx> speed-duplex auto** (to set port/s <<xx>> to Auto-Negotiate)

Note Ports 1-24 are the only ports on the HP2524 switch that can be configured for Auto-Negotiate

- **int e 1-24 broadcast-limit 20**
- **int e 25 broadcast-limit 20** (if fiber transceiver is installed in port 25)
- **int e 26 broadcast-limit 20** (if fiber transceiver is installed in port 26)

Note The following **spanning-tree priority** command is to be used for **Core switches only**. The Edge switch uses the default priority setting.

- **spanning-tree priority 8192** (for Core switch **only**)
- **spanning-tree ethernet 1-21 mode fast** (for ports set to 10 Mb/s Half Duplex, see above)
- write memory
- **boot system** (press **Y** to confirm)

To verify the configuration of the ports, press the **Mode** button on the front of the switch. When **FDx** is lit, all the ports configured as Full Duplex should be lit. When **Max** is lit, all the ports configured at 100 Mb/s should be lit. Auto-Negotiate ports default to 10 Mb/s half duplex until a device is connected and the speed and duplex are negotiated.

Cisco Switches

If the configuring PC is the Database Server using Hyperterminal from Port A, the UPS connection must be temporarily removed and disabled. The following steps describe the procedure.

- Step 1.** Connect one end of the RJ-45 Console cable supplied with the switch to the 9 pin adapter
- Step 2.** Plug the 9 pin adapter end of the Console cable into the RS 232 connector of Serial Port A on the rear of the PC. (If the UPS/Server communication cable has been connected, remove it first.)
- Step 3.** Plug the RJ-45 end of the Console cable into the **CONSOLE** port on the rear of the Cisco switch, as shown in Figure 4-18. If the Database Server is not the configuring PC, skip to step 12.

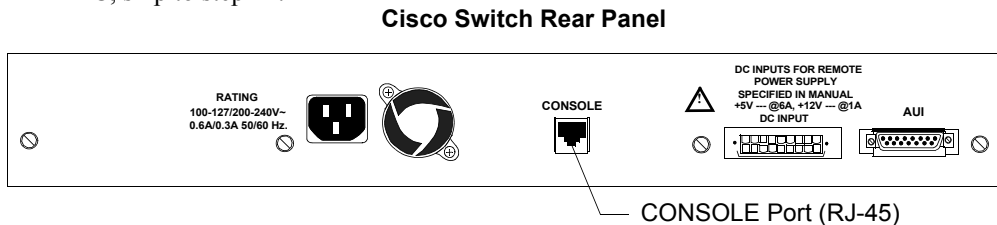


Figure 4-18 CONSOLE Port for Setting Cisco Switch IP Address

- Step 4.** Turn On the PC and Switch

If the Server's UPS service detects that the UPS is not connected to Serial Port A, a message indicating **At least one service failed to initialize...** may appear.

If this message appears:

Step 5. Click **OK** and proceed to **Step 12**.

If this message **does not** appear:

Step 6. Go to the **Control Panel** and double click on the **Services** icon (2 gears) to open the **Services** window.

Step 7. Scroll down the list of **Services** to **UPS**.

Step 8. Click on **UPS** to highlight it.

Step 9. Click on the **Stop** button to disable the UPS connection.

Step 10. Click **Yes** to the **Are you sure..** message. A momentary **Attempting to stop...** message will then appear.

When the UPS connection has been disabled:

Step 11. Close the **Services** window and **Control Panel**.

Step 12. Open **HyperTerminal**.

Note If a **Connection Description** window appears, click **Cancel** to close it.

Step 13. Click on **File** in the **New Connection - HyperTerminal** window to display its menu.

Note Some steps (or paths) may differ slightly based on the Operating System and PC Setup.

Step 14. Click on **Properties** to open the **New Connection Properties** window.

Step 15. Click on the **Connect to** tab to display its menu.

Step 16. Click on the **Connect Using** pull down arrow to display its menu.

Step 17. Click on **COM1**.

Step 18. Click on **Configure** to display the **COM1 Properties** window.

Step 19. Configure the COM1 port to the following RS 232 settings:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

Step 20. Click **OK** and the **Catalyst 1900 Management Console** window appears. If this window does not open, check the RS 232 settings on the COM port and verify cable connectivity.

Step 21. Reset the configuration to default values as follows:

- Type **M** to select **Menus** from the Management Console window
- Type **S** to select the **System Configuration** menu
- Type **F** to select the **Reset** configuration command. (This restores the factory configurations)
- Type **Y** to confirm the reset and then press **Enter**

Note The reset command can take up to one minute to complete before it returns to the Management Console window.

Determine the firmware revision of the switch. Type **M** to select **Menus**. Type **F** to select **Firmware**. Depending on the Firmware revision of the switch, the next few steps vary. If the Firmware version is 8.x, follow the steps in the section **Firmware Rev 8.0x.xx** on page 4-34. If firmware version is 9.xx and higher, follow the steps in the section **Firmware Rev 9.0x.xx** and higher on page 4-37.

Firmware Rev 8.0x.xx

Step 1. Set the Switch IP Address as follows:

- Type **I** to select the **IP Config** menu
- Type **I** to select the **IP Address**
- Type a **Required IP Address** for **Switches** from Table 4-1 in the **new setting** field and press **Enter**

Note The IP Address for the **first switch** should be **172.31.252.0**
The IP Address for a **second switch** should be **172.31.252.1**
The IP Addresses for the switches **must be different**

- Type **S** to select the **Subnet Mask**
- Type in the default Subnet Mask number (**255.255.0.0**) in the **new settings** field and press **Enter**

Note All other settings in this window should remain at their **default** settings and should not be changed.

Step 2. Set site specific values for the Switch as follows:

- Type **X** to return to the **Management Console** window
- Type **M** to select **Menus** in the Management Console window
- Type **S** to select the **System Configuration** menu
- Type **N** to select the **Name** of the switch
- Type in a **Name** for the Switch (e.g. switch #1) in the **new settings** field and press **Enter**. This field has a limit of 255 characters.
- Type **L** to select the **Location** of the Switch
- Type in a **Location** for the switch (e.g. ICU, 5th Floor) in the **new settings** field and press **Enter**. This field has a limit of 255 characters.

Step 3. Set the switching mode of the Switch as follows:

- Type **S** to select the **Switching Mode**
- Type **1** (Store and Forward) in the **new settings** field and press **Enter**

Step 4. Set SNMP Capabilities for the Switch as follows:

- Type **X** to return to the **Management Console** window
- Type **N** to select the **Network Management** menu
- Type **S** to select the **SNMP Management** menu
- Type **1** to select the 1st **Write Manager Name** or **IP Address**

Notes

The IP Address **172.31.241.0** should be used for all **Manager IP Addresses**. This IP Address is reserved for support devices that may be used in the future. All other **Write** and **Trap Manager IP Addresses** should be left **blank**.

- Type **172.31.241.0** in the **new settings** field of the 1st **Write Manger IP Address** and press **Enter**
- Type **A** to select the 1st **Trap Manager** or **IP Address**
- Type **172.31.241.0** in the **new settings** field of the 1st **Trap Manager Name** or **IP Address** and press **Enter**

Notes

public (lower case p) should be used for all of the following **community strings**. All other settings in these windows should remain at their **default** settings.

- Type **W** to select the **Write community string**
- Type **public** in the **new settings** field of the **Write community string** and press **Enter**

Note Unlike the IP Address entries, the word **public** will not appear adjacent to Write community string when the menu regenerates.

- Type **F** to select the first **Trap community string**
 - Type **1** in the **new settings** field of the first **Trap community string** and press **Enter**
-

Note The **1** will not appear adjacent to Trap community string when the menu regenerates.

Step 5. Set **Port configuration** to 100 Mbps or Auto-Negotiate as follows:

- Type **X** to return to the **Network Management** menu
 - Type **X** to return to the **Console Management** window
 - Type **P** to select the **Port Configuration** menu
 - Type **A** in the **Port** selection field to select **Port A** and press **Enter**
 - Type **F** to select the **Full Duplex/Flow Control** menu
 - Type **1** in the **new setting** field to select Full Duplex and press **Enter**
-

Note Port A on the Cisco switch cannot be configured for Auto-negotiate; it is not supported.

- Type **N** (Next port) to select **Port B** and press **Enter**
 - Type **F** to select the **Full Duplex/Flow Control** menu
 - Type **1** for Full Duplex in the **new setting** field and press **Enter**
-

Notes All other settings in these windows should remain at their **default** settings.

- Type **X** to return to the **Main Menu**

Step 6. Set **additional parameters** as follows:

- Type **S** to select the **System Menu**
- Type **U** to select **Use of Store-and-forward for multicast**
- Type **E** to enable this feature and press **Enter**
- Type **B** to select **Broadcast Storm Control**
- Type **A** to select **Action**
- Type **B** to select **Block** and press **Enter**

- Type **X** to return to the **System Menu**
- Type **X** to return to **Main Menu**
- Type **C** to return to **Console Menu**
- Type **T** to select **Console Timeout**
- Type **600** to set timeout to **600 seconds** (10 minutes) and press **Enter**
- Type **X** to return to the **Main Menu**
- Type **X** to exit the **Management Console** window
- Type **Y** and press **Enter**

Step 7. Wait 5 minutes for the settings to be stored.

Note

If you don't give the switch 5 minutes to store the settings before turning off the Switch, the configuration settings may be lost. No message will appear after 5 minutes, but the **5 minute wait period is required**.

Step 8. Validate the configurations. See the Step Validate the configurations using either (A) the CONSOLE/TERMINAL for firmware V8.xx, (B) the CONSOLE/TERMINAL for firmware V9.x or (C) the Network Statistics application as follows. on page 4-40

When the validation procedure is complete:

Step 9. Disconnect the crossover cable from the Server's Serial Port A and reconnect the UPS/Server communications cable.

Step 10. Reboot the Server to re-enable the UPS service.

Firmware Rev 9.0x.xx and higher

Step 11. Set the Switch IP Address as follows:

- Type **I** to select the **IP Config** menu
- Type **I** to select the **IP Address**
- Type a **Required IP Address** for **Switches** from Table 4-1 in the **new setting** field and press **Enter**

Note

The IP Address for the **first switch** should be **172.31.252.0**
 The IP Address for a **second switch** should be **172.31.252.1**
 The IP Addresses for the switches **must be different**

- Type **S** to select the **Subnet Mask**
- Type in the default Subnet Mask number (**255.255.0.0**) in the **new settings** field and press **Enter**

Note All other settings in this window should remain at their **default** settings and should not be changed.

Step 12. Set site specific values for the Switch as follows:

- Type **X** to return to the **Management Console** window
- Type **M** to select **Menus** in the Management Console window
- Type **S** to select the **System Configuration** menu
- Type **N** to select the **Name** of the switch
- Type in a **Name** for the Switch (e.g. switch #1) in the **new settings** field and press **Enter**. This field has a limit of 255 characters.
- Type **L** to select the **Location** of the Switch
- Type in a **Location** for the switch (e.g. ICU, 5th Floor) in the **new settings** field and press **Enter**. This field has a limit of 255 characters.

Step 13. Set the switching mode of the Switch as follows:

- Type **S** to select the **Switching Mode**
- Type **1** (Store and Forward) in the **new settings** field and press **Enter**

Step 14. Set SNMP Capabilities for the Switch as follows:

- Type **X** to return to the **Management Console** window
- Type **N** to select the **Network Management** menu
- Type **S** to select the **SNMP Management** menu
- Type **W** to select **Write Configuration**
- Type **1** to select the 1st **Write community string**

Notes **public** (lower case p) should be used for all of the following **community strings**. All other settings in these windows should remain at their **default** settings.

- Type **public** in the **new settings** field of the **Write community string** and press **Enter**
- Type **A** to select the 1st **Write Manager Name** or **IP Address**
- Type **172.31.241.0** in the **new settings** field of the 1st **Write Manager IP Address** and press **Enter**

Notes The IP Address **172.31.241.0** should be used for all **Manager IP Addresses**. This IP Address is reserved for support devices that may be used in the future.

All other **Write** and **Trap Manager IP Addresses** should be left **blank**.

- Type **X** to return to the previous menu
- Type **T** to select **Trap configuration**
- Type **1** to select the 1st **Trap community string**
- Type **1** in the **new settings** field of the 1st **Trap community string** and press **Enter**
- Type **A** to select the 1st **Trap Manager** or **IP Address**
- Type **172.31.241.0** in the **new settings** field of the 1st **Trap Manager Name** or **IP Address** and press **Enter**
- Type **X** to return to the previous menu

Step 15. Set Port configuration to 100 Mbps or Auto-Negotiate as follows:

- Type **X** to return to the **Network Management** menu
- Type **X** to return to the **Main Menu** window
- Type **P** to select the **Port Configuration** menu
- Type **A** in the **Port** selection field to select **Port A** and press **Enter**
- Type **F** to select the **Full Duplex/Flow Control** menu
- Type **1** in the **new setting** field to select Full Duplex and press **Enter**

Note Port A on the Cisco switch cannot be configured for Auto-negotiate; it is not supported.

- Type **N** (Next port) to select **Port B** and press **Enter**
- Type **F** to select the **Full Duplex/Flow Control** menu
- Type **1** for Full Duplex in the **new setting** field and press **Enter**

Notes All other settings in these windows should remain at their **default** settings.

- Type **X** to return to the **Main Menu**

Step 16. Set additional parameters as follows:

- Type **S** to select the **System Menu**
- Type **U** to select **Use of Store-and-forward for multicast**
- Type **E** to enable this feature and press **Enter**
- Type **B** to select **Broadcast Storm Control**

- Type **A** to select **Action**
- Type **B** to select **Block** and press **Enter**
- Type **X** to return to the **System Menu**
- Type **X** to return to **Main Menu**
- Type **C** to return to **Console Menu**
- Type **T** to select **Console Timeout**
- Type **600** to set timeout to **600 seconds** (10 minutes) and press **Enter**

Step 17. Set Console Password as follows:

- Type **M** to select the **Modify Password**
- Type **m3150** and press **Enter** (enter password)
- Type **m3150** and press **Enter** (re-enter password)
- Press any key to continue
- Type **X** to return to the **Main Menu** window
- Type **X** to exit the **Management Console** window
- Type **Y** and press **Enter**

Step 18. Wait 5 minutes for the settings to be stored.

Note

If you don't give the switch 5 minutes to store the settings before turning off the Switch, the configuration settings may be lost. No message will appear after 5 minutes, but the **5 minute wait period is required**.

Step 19. Validate the configurations using either (A) the **CONSOLE/TERMINAL** for firmware V8.xx, (B) the **CONSOLE/TERMINAL for firmware V9.x** or (C) the **Network Statistics** application as follows.

(A) Validation procedure using the CONSOLE/TERMINAL

- Turn the Switch **Off** and then **On** and **wait 3 minutes**
- Press **Enter** on the PC to bring up the **Management Console** window
- Type **I** to select the **IP Address**
- Verify that the current setting for the IP address for the first switch is **172.31.252.0** (or **172.31.252.1** for a second Switch)
- Type **X** to return to the **Management Console** window
- Type **M** to select **Menus** in the Management Console window

- Type **P** to select the **Port Configuration** menu
- Type **A** in the Port selection field to select Port A and press **Enter**
- Type **F** to select the **Full Duplex/Flow Control** menu
- Validate that the **Current Setting** is **Full Duplex** and press **Enter**
- Type **N** (Next port) to select Port B and press **Enter**
- Type **F** to select the **Full Duplex/Flow Control** menu
- Validate that the **Current Setting** is **Full Duplex** and press **Enter**
- Type **X** to return to the **Management Console** window
- Disconnect the RS 232 CONSOLE port cable from the Switch

(B) Validation procedure using the CONSOLE/TERMINAL

- Turn the Switch **Off** and then **On** and **wait 3 minutes**
- Press **Enter** on the PC to bring up the **Management Console** window
- Type **M** to select **Menus** in the Management Console window
- Type **m3150** and press **Enter**
- Type **N** to select **Network Management**
- Type **I** to select **IP Address**
- Verify that the current setting for the IP address for the first switch is **172.31.252.0** (or **172.31.252.1** for a second Switch)
- Type **X** to return to the **Main Menu** window
- Type **P** to select the **Port Configuration** menu
- Type **A** in the Port selection field to select Port A and press **Enter**
- Type **F** to select the **Full Duplex/Flow Control** menu
- Validate that the **Current Setting** is **Full Duplex** and press **Enter**
- Type **N** (Next port) to select Port B and press **Enter**
- Type **F** to select the **Full Duplex/Flow Control** menu
- Validate that the **Current Setting** is **Full Duplex** and press **Enter**
- Type **X** to return to the **Main Menu** window
- Type **X** to return to the **Management Console** window
- Disconnect the RS 232 CONSOLE port cable from the Switch

(C) Validation procedure using the Network Statistics application

- Launch **Microsoft Internet Explorer** on an Information Center, Client, or Server connected to one of the ports of the first Switch.
- Enter the **IP Address** of the first switch (**172.31.252.0**) in the **URL** field and press **Enter**. The **Network Statistics HOME** window should appear.
- Validate the following by clicking on its name in the menu bar at the top of the window.
 - In the **HOME** window: IP Address is **172.31.252.0**
 - In the **SYSTEM** window: **Switching Mode** is **Store and Forward**
 - In the **PORTS** window: Both 100 mbps ports (#26 and #27) are configured for **correctly (FULL DUPLEX)**

Step 20. If a second switch is being used, repeat the validation for the second switch, whose IP Address is **172.31.252.1**

When the validation procedure is complete:

Step 21. Disconnect the crossover cable from the Server's Serial Port A and reconnect the UPS/Server communications cable.

Step 22. Reboot the Server to re-enable the UPS service.

Physical Installation

Switches Install the switches according to the following steps:

Step 1. Mount the switches securely in their planned location. Mounting hardware for rack or wall mounting is provided with the switches, although they can be placed on a horizontal shelf or table. Refer to the mechanical mounting instructions included with the switch.

Step 2. Install a 650 VA UPS with the proper voltage for each switch as follows:

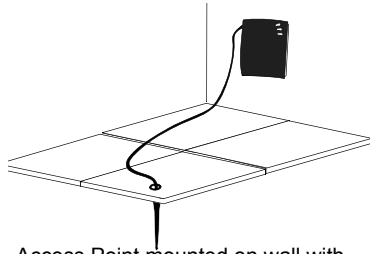
- **Connect the battery wire** of the UPS.
- **Set the dip switches** of the UPS to their correct settings (Figure 2-19).
- **Turn Off the UPS** On/Off switches.
- **Connect UPS input power cord** to a properly grounded electrical outlet.
- **Connect switch input power cords** to UPS outlets labeled **BATTERY BACKUP**.

RangeLAN2 Wireless Access Points Next, install all wireless access points as follows:

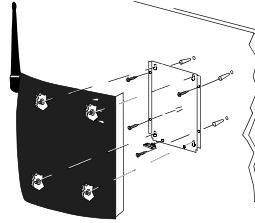
Step 1. Make sure each RangeLAN2 access point has been configured for Network operation.

Step 2. Mount all RangeLAN2 access points securely in their planned locations. Hardware for mounting an access point to a wall or ceiling is sold separately. Installation

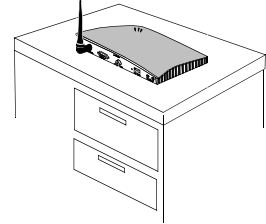
instructions are shipped with the mounting hardware. Figure 4-19 shows the various mounting options.



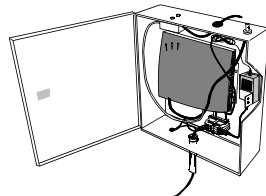
Access Point mounted on wall with Extended Antenna* facing down



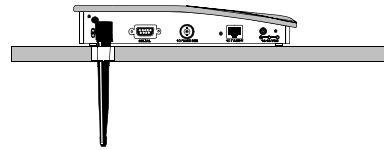
Access Point mounted Vertical on wall with Antenna facing up (M3180A-#A20)



Access Point placed on Horizontal Surface with Antenna facing up



Access Point in Plenum Box Mounting Kit

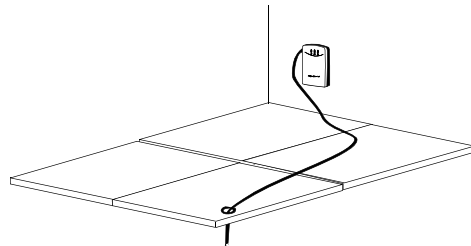


Access Point through hole in ceiling with Antenna facing down

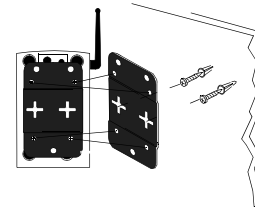
Figure 4-19 RangeLAN2 Access Points - Possible Mounting Options

* Antenna Extension kit part numbers are M3199AI #A20 3 ft. (0.9 m) & #A21 10 ft. (3 m)

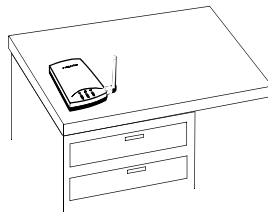
Step 3. Mount all Harmony access points securely in their planned locations. Hardware for mounting an access point to a wall or ceiling is sold separately. Figure 4-20 shows the various mounting options.



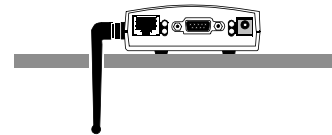
Harmony access point mounted on wall with Extended Antenna* facing down



Harmony access point mounted Vertical on wall with Antenna facing up



Harmony access point placed on Horizontal Surface with Antenna facing up



Harmony access point through hole in ceiling with Antenna facing down

Figure 4-20 Harmony Access Points - Possible Mounting Options

Warning

When installing the access point on a suspended ceiling, make certain the ceiling is structurally rated to support the weight of the access point, .7 kg (1.5 lbs) and any extra cable.

Media Translators

All media translators should then be installed as follows.

Step 1. Configure the Media Translator switch settings as shown in **10 Mbps Media Translator Switch Configuration on page 4-45.**

Step 2. With 10 Mbps media translators, the J2606A fiber transceiver must first be installed. **Install the J2606A fiber transceiver** into all 10 Mbps media translators as follows. See Figure 4-21.

Caution

When handling the J2606A fiber transceiver (or any PC board), follow all proper ESD protection guidelines, including grounding the equipment, the work surface, and yourself.

- **Remove the blank panel** on the front of the media translator
- **Place the J2606A fiber transceiver into the front panel opening** and push it back until it fits firmly into its socket
- **Tighten the transceiver thumb screws** securely to lock the transceiver into place.

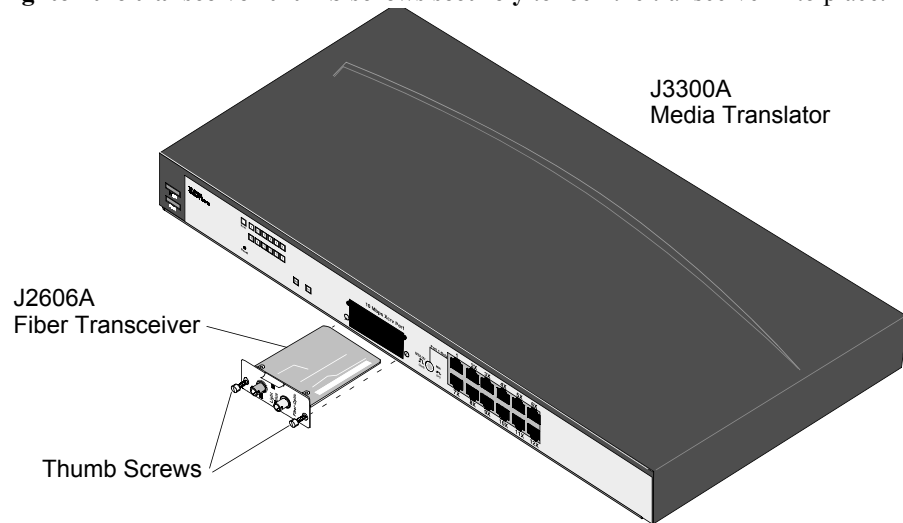


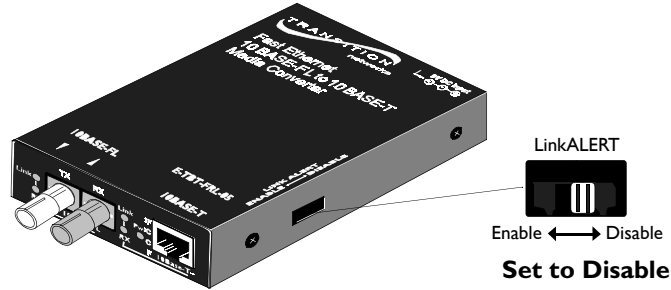
Figure 4-21 Installation of J2606A Fiber Transceiver in Media Translator

Step 3. Mount all repeaters and media translators securely in their planned locations.

Hardware for rack or wall mounting is provided with the devices, although they can be simply placed on a horizontal shelf or surface.

Step 4. **Install 650 VA UPSs** with the proper voltage for each repeater and media translator as described in **Step 2** for Switches on **page 4-42.**

10 Mbps Media Translator Switch Configuration



The **LinkALERT** feature is set to **Disable** to allow troubleshooting of device-to-device connectivity using the Link LEDs.

Note

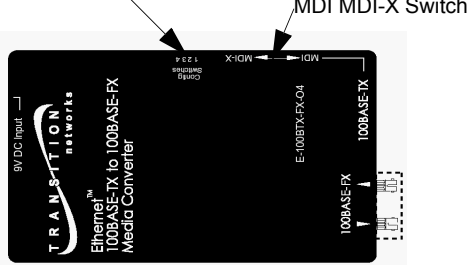
The LinkALERT switch on the side of the unit must be set to **Disable**.

100 Mbps Media Translator Switch Configurations

There are two supported versions of the 100 Mbps Media Translator. Use the following diagrams to determine the correct switch settings.

E-100BTX-FX-04

Configuration Switches

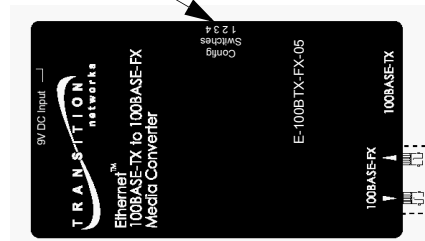


Configuration Switch Settings

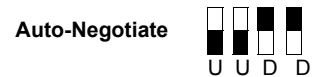


E-100BTX-FX-05

Configuration Switches



Configuration Switch Settings



Network Connections

Procedures for Network component interconnections are given on the following pages:

Switch to Switch page 4-48

Switch to 100 Mbps HALF Network Devices page 4-48

Notes As a general rule, each connection between devices (switch and media translator, switch and repeater, etc.) must be crossed on one end. Crossed ports are designated by an “X” on the port label.

The connection diagrams shown in this section give some tips on how achieve the crossover requirement for that particular connection type.

Figure 4-22 provides an overview of the components used in Network Connections (the components shown below are for illustration purposes only, newer hardware models may replace the ones shown here). These components are used in the next figure to show how devices connect to one another:

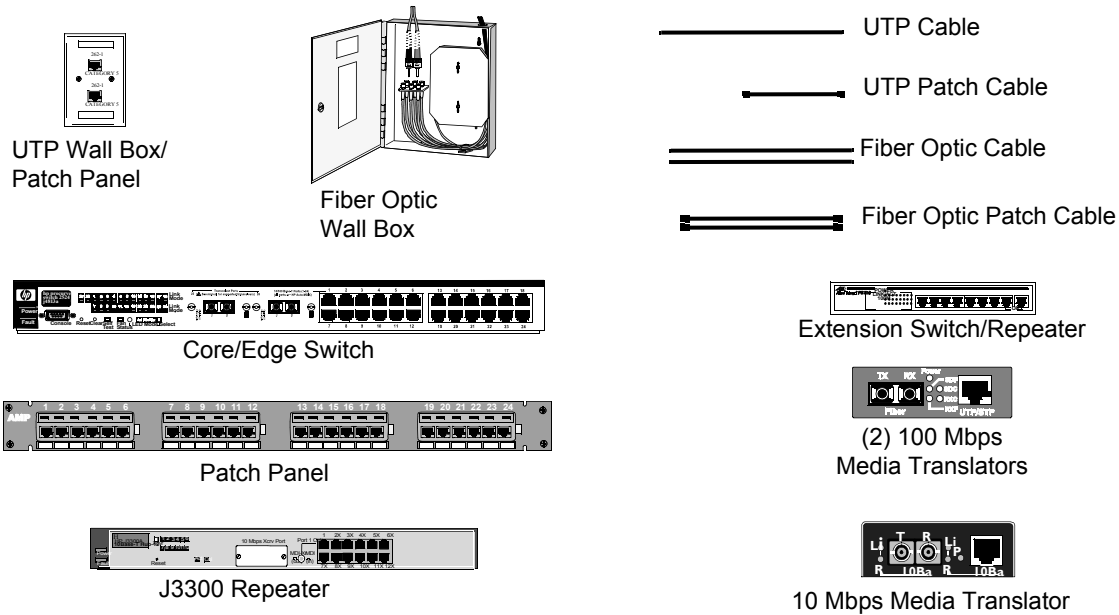
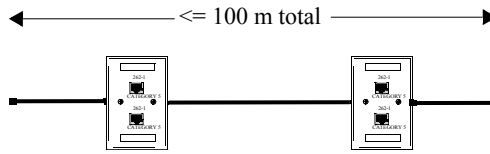


Figure 4-22 Network Connection Components

Figure 4-23 shows all the possible network connections between the system devices (cable lengths include patch cables). These are referenced by the Identifying Letter in the following sections.

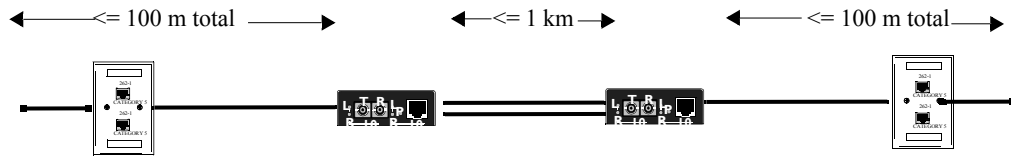
10Mbps Connections

A

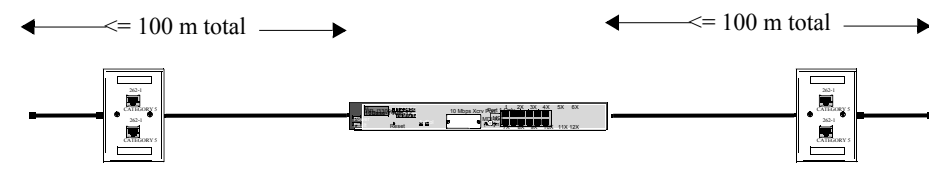


100 m = 328 ft
1 km = 3280 ft

B

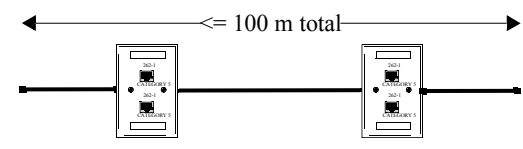


C

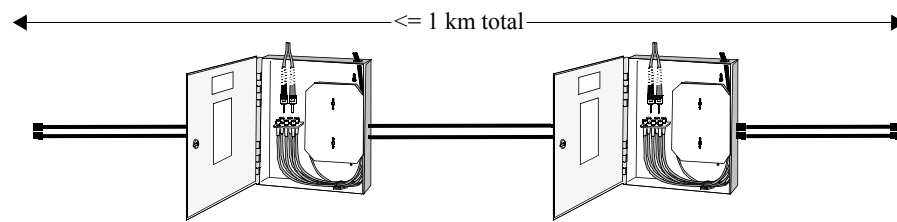


100Mbps Connections

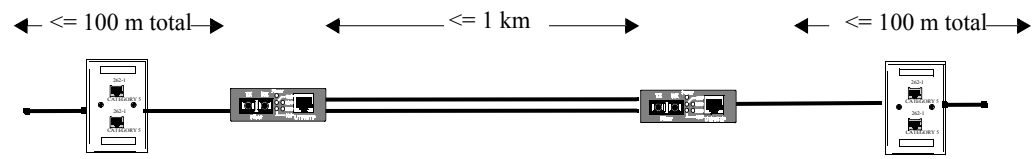
D



E



F



G

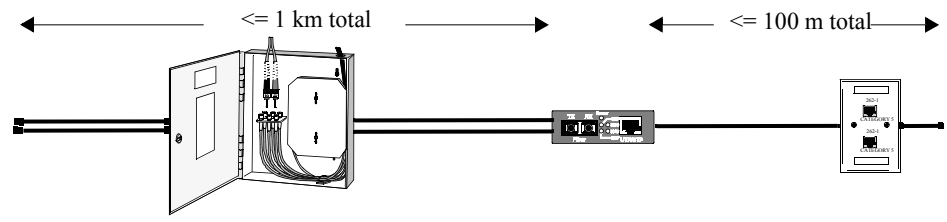


Figure 4-23 Network Connections Options

Notes **Fiber optic patch cables** use SC (square) terminations at switches and, in this example, ST (round) terminations at wall boxes.
Switches can also be connected directly by a single fiber optic patch cable, length permitting.

Switch to Switch Switch to Switch Connections are **100 Mbps Full Duplex**. Their connection types, as defined in **Table 3-2** as well as **Figure 4-23** are:

- Connection Type **D** - Single length UTP Cable
- Connection Type **E** - Single length Fiber Optic Cable
- Connection Type **F** - Fiber Optic and UTP Cable w/two 100 Mbps Media Translators
- Connection Type **G** - Fiber Optic and UTP Cable w/one 100 Mbps Media Translator

Some switch port configurations must match the port they are connecting to (see also, Connecting Devices on page 3-12).

- Auto-Negotiate ports must connect to an Auto-Negotiate port
- 100 Mbps FULL duplex ports must connect to a 100 Mbps FULL duplex port

When making switch to switch connections, consideration must be given to the cable type used. Depending on the connection, crossover cable or straight-through cable is required. The port on the Core/Edge switch that is connecting to the other switch must be configured for auto-negotiate for straight through cable to be used. If the port is configured for 100 Full, crossover cable is required. If no link activity is detected when the switches are connected, try using the other cable type, and verify the port configuration.

Switch to 100 Mbps HALF Network Devices Switch to **100 Mbps HALF** Information Center and Client devices. The only supported connection type, as defined in **Table 3-2** as well as **Figure 4-23** is:

- Connection Type **D** - Single length UTP cable

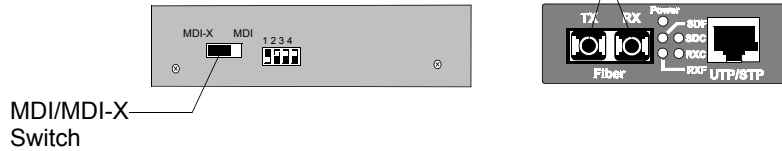
Switch to 100 Mbps FULL Network Devices Switch to **100 Mbps FULL** network devices (Database Server). Their connection types, as defined in **Table 3-2** as well as **Figure 4-23** are:

- Connection Type **D** - Single length UTP cable
- Connection Type **F** - Fiber Optic and UTP Cable w/Switch and two 100 Mbps Media Translators
- Connection Type **G** - Fiber Optic and UTP Cable w/one 100 Mbps Media Translator

Note **For upgraded systems:** when using Connection Type **G** and the older Media Translator, part number M3188-60100 (E-100BTX-FX-04(SC)), change the following settings at the Media

Translator to ensure that the necessary crossover occurs. This is not necessary for Media Translators shipped with new systems (part number M3188-60000, E-100BTX-FX-05).

Set switch to **MDI-X** and use **standard** UTP cable
or
 Set switch to **MDI** and use **crossover** UTP cable



See 10 Mbps Media Translator Switch Configuration on page 4-45 for the appropriate switch settings.

Note A **patch cable** can be used to connect the Switch to the Database Server if the devices are within the patch cable length.

Switch to 10 Mbps Network Devices

Switch to Network Devices Connections are **10 Mbps**. Their connection types, as defined in **Table 3-2** as well as **Figure 4-23** are:

- Connection Type **A** - Single length UTP cable
- Connection Type **B** - UTP cable, 2 10 Mbps media translators, fiber optic cable
 When using Connection Type **B**, change the following to ensure that the necessary cross over occurs:
 - Use Port 1 as input, depress the MDI button, and use the fiber output
 - Flip one Fiber Optic Patch Cable -- RX to TX and TX to RX
 - On the second Media Translator, use any port except Port 1 **or** use Port 1 and do not depress the MDI button
- Connection Type **C** - UTP Cable and 1 Repeater

As each device is connected to the switch, check the LEDs for link as well as proper operational speed and duplex. The LEDs are described in LED Diagnostics on page 5-28.

Clinical Network Devices: Names and IP Addresses

The next step is to identify the Clinical Network devices' names and locations on the Network. A variety of names and location identifiers are used for this purpose. The names and addresses for each Network device -- Switches, Information Centers, Clients, Application Servers, and Printers -- must be unique so they can be properly located by the Database Server and other Network devices.

IP Address

Internet Protocol (IP) Address is a 32 bit binary number that uniquely identifies the location of the device on the Network. The IP Address is generally in dotted decimal format, which consists of 4 sets of numbers separated by dots, e.g. 172.31.252.1. Part of the IP Address identifies the network and part identifies the device.

For the Clinical Network, a range of possible IP addresses has been set for each type of Network device. If separate systems are being installed today with an expectation of connecting them in the future, do not use the same names or IP addresses. This will save time later when they are connected together. The IP Address ranges are given in Table 4-1.

Warning

IP Addresses outside the ranges given in Table 4-1 have not been tested by Philips and are not supported by Philips software.

Table 4-1. Range of IP Addresses for Network Devices

Device	Range of IP Addresses	Recommended IP Addresses
M2/M3/M4/IntelliVue Patient Monitors	172.31.16.0 - 172.31.79.255	These IP Addresses are automatically allocated by Philips Software
M3150 Information Centers	172.31.101.0 - 172.31.150.255	172.31. 101.0 - 172.31. 101.7
M3151 Information Center Clients	172.31.151.0 - 172.31.199.255	172.31. 151.0 - 172.31. 151.7
T1/E1 Remote Switch (for Remote Client)	172.31.200.1 - 172.31.200.99	172.31.200. 1
T1/E1 Remote Information Center Client	172.31.200.100 - 172.31.200.199	172.31.200. 100
T1/E1 Local Router Connection - Ethernet Connection to Core Switch	172.31.0.1	172.31.0. 1
T1/E1 Remote Router Connection - Ethernet Connection to Core Switch	172.31.200.200 - 172.31.200.253	172.31.200. 200
M3154 Database Server/M3169 Small Database Server Clinical Network NIC	172.31.221.0 - 172.31.227.255	172.31. 221.0
M2385 Application Server Clinical Network NIC	172.31.211.0 - 172.31.220.255	172.31. 211.0
Information Center Web Card		Site Dependant
Core/Edge Switches	172.31.252.0 - 172.31.253.255	172.31. 252.0 - 172.31. 252.9

Table 4-1. Range of IP Addresses for Network Devices

Device	Range of IP Addresses	Recommended IP Addresses
Harmony Access Point Controllers (APC)	172.31.238.0 - 172.31.238.255	172.31. 238.0 - 172.31. 238.15
Wireless Access Points	172.31.234.0 - 172.31.237.255	172.31. 234.0 -172.31. 234.15
M3159 Networked LaserJet Printers	172.31.254.1 - 172.31.254.8	172.31. 254.1 - 172.31. 254.8

In addition to IP Address, there are several other identifiers given to Network devices so they can be uniquely identified by the network and in Philips software application windows. These include the following:

Subnet Mask

Because the last 4 digits of the IP Address are the key digits that uniquely identify a device, a Subnet Mask is applied to the IP Address to “mask” the first 5 IP Address digits. The **Subnet Mask** used for Philips software is **255.255.0.0**. For example, adding the Subnet Mask to the IP Address of the Database Server gives a “masked” address of 255.255.221.0, where the unique last 4 digits of the Server’s IP Address have been added to the Subnet Mask.

Almost all IP Address handling applications require the specification of a Subnet Mask. The Subnet Mask default value of 255.255.0.0 is used for all Network connected devices and will appear in Windows configuration applications. It is not necessary to know the “masked” IP Addresses of Philips devices, although it does appear in the **Network** category of the **Status Log**. In all other applications, the real IP Address for networked devices is shown.

The Subnet Mask for Remote Clients on a T1/E1 line must be set to 255.255.255.0.

Default Gateway

Default Gateway is another field that must be specified in many IP Addressing applications. The default gateway for all Information Centers and Clients must be set to the Database Server’s IP Address. The default gateway for the Database Server can be set to its default value.

If the network has Remote Clients on a T1/E1 line, the Default Gateway for the devices must follow the guidelines given in **Appendix B: Remote Clients on T1 Lines**.

MAC Address

Media Access Control (MAC) Address is a fixed, unique 12 digit HEX number that identifies each device. Part of the number identifies the device manufacturer. It is hard coded into the device’s network interface card and cannot be changed. It is **not necessary to know** the MAC Addresses of Network devices, although they will appear in some application windows. For instance, if the MAC address of the printer is needed, it is on the configuration page printed out during the printer installation.

Host Name

Host Name is an alphanumeric name assigned to each workstation -- Information Centers, Clients, Database Server -- and resides in its software. Philips assigns a Host Name to each PC before shipment; but it should be changed to a name that identifies its function, associated unit, and physical location. A Host Name for an Information Center in the CCU on the third floor, south wing of the hospital might be **ICCCU3S**. Or the Database Server might be **DBSRM96**.

Notes	Rules for Host Name for a device on the Network are: <ul style="list-style-type: none">– must be unique for the Server to identify it– must be no more than 15 characters– must use alpha-numeric characters only, no other characters acceptable (no spaces, hyphens, underscores, etc.)– cannot begin with a number– must be changed from factory settings during device installation
--------------	--

Device Name Device Name is another name given to a device -- Information Center, Client, Server, Switch -- when it is configured on the network. Device Name is generally the same as its Host Name.

Setting Host Names and IP Addresses After all Network devices have been installed, their **Host Names** and **IP Addresses** should be set. All Network devices -- Information Centers, Clients, Servers, Switches, Printers -- must also have their **Network IP Addresses** set before Philips software can be installed and configured.

Notes	IP Addresses for M3/M4/IntelliVue Patient Monitors are automatically assigned by Philips software. Network Installation Worksheets are provided in Appendix A to record Host and Device Names , hospital Locations , and IP Addresses . Complete these Network Installation Worksheets for all devices on the Network.
--------------	---

Verifying Network Connectivity Once the IP Addresses of the Server, workstations, switches, Access Points, and printers have been set, the network can be verified to assure the integrity of each network connection and that each device can be identified by the Server. The procedure is done at the Server and is as follows.

Step 1. Open the **MS DOS STARDATE: Console** window shown in Figure 4-24 (located in the Start->Programs menu)

```

STARDATE:Console
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>ping HPICU

Pinging HPICU [172.31.16.3] with 32 bytes of data:

Reply from 172.31.16.3: bytes=32 time<10ms TTL=128
Reply from 172.31.16.3: bytes=32 time<10ms TTL=128
Reply from 172.31.16.3: bytes=32 time<10ms TTL=128
Reply from 172.31.16.3: bytes=32 time<10ms TTL=128

C:\>ping HPCCU

Pinging HPCCU [172.31.16.4] with 32 bytes of data:

Reply from 172.31.16.4: bytes=32 time<10ms TTL=128
Reply from 172.31.16.4: bytes=32 time<10ms TTL=128
Reply from 172.31.16.4: bytes=32 time<10ms TTL=128
Reply from 172.31.16.4: bytes=32 time<10ms TTL=128

C:\>

```

Figure 4-24 Verifying Network Connectivity using Hostname

Step 2. Type **ping hostname** (or **ping IPAddress**) for one of the Network connected Information Centers after the **C:\>** prompt, as shown for Host Name = **HPICU** (and **HPCCU**) in Figure 4-24, and press Enter.

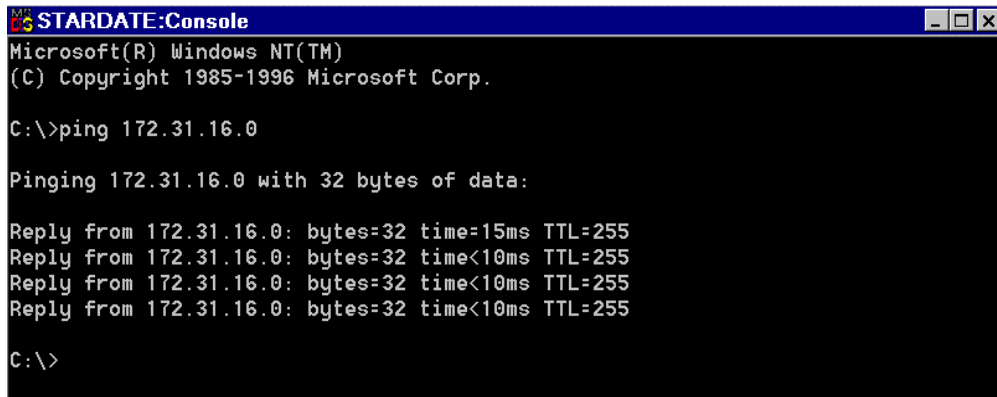
If the ping is successful, i.e. the network connection is complete and the Host Name is correct, a reply using the device's correct IP Address should appear, as shown in Figure 4-24.

If the ping fails, the reason for the failure (e.g. bad IP Address) will be shown. Identify the problem, correct it (e.g. use an IP Address instead of the Host Name), and repeat the process.

Step 3. Repeat **Step 2** for each Information Center, Client, Switch, Access Point, and Printer on the Network.

Note

Switches, Access Points, and Printers do not have Host Names so their IP Address should be used instead, as shown in Figure 4-25.



```
STARDATE:Console
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>ping 172.31.16.0

Pinging 172.31.16.0 with 32 bytes of data:

Reply from 172.31.16.0: bytes=32 time=15ms TTL=255
Reply from 172.31.16.0: bytes=32 time<10ms TTL=255
Reply from 172.31.16.0: bytes=32 time<10ms TTL=255
Reply from 172.31.16.0: bytes=32 time<10ms TTL=255

C:\>
```

Figure 4-25 Verifying Network Connectivity Using IP Address

The Clinical Network is now fully installed. The next steps are to reinitialize the database, install Philips software, and configure the Server and all Network connected Information Centers and Clients. Refer to the **Information Center Installation and Service Manual**.

Troubleshooting the Clinical Network

Overview

Chapter 5 describes the various troubleshooting options for the Clinical Network in the following sections:

Troubleshooting	page 5-4
Network Statistics	page 5-13
Diagnostics	page 5-26
LED Diagnostics	page 5-28
Repair	page 5-42

Maintenance

Network hardware is generally maintenance free. However, the equipment should be kept clean and dry and maintained within its environmental specifications. There are also several routine maintenance procedures that should be followed at regular interval. This section describes those procedures.

Routine Maintenance

For most network components recommended maintenance is described in **User's Manuals** provided with the unit. Refer to those documents for maintenance procedures and frequencies to assure reliable, trouble-free operation.

Note

All **Preventive Maintenance is the responsibility of the customer.**

Recommended frequency is **every 6 months**, or less in harsh environments.

Two areas of maintenance deserve special mention -- cleaning air intakes and regular replacement of UPS batteries.

Air Intakes

Fans used to cool electronic devices generally develop dust build-up in air intake areas that must be removed to assure proper cooling and circuit operation. Air intakes of workstations, switches, remote power system, and the server should be checked regularly and any dust buildup removed.

UPS

The UPS requires regular battery replacement. It also contains no serviceable parts except the battery and should not be opened by hospital personnel because it contains potentially hazardous voltages that can be dangerous to unskilled persons.

Warning

Do not attempt to disassemble the UPS. It contains no serviceable parts except for the battery, and interior voltages can be hazardous. Repair should be performed by factory trained service personnel only.

If battery replacement is done as recommended, regular testing of the UPS is not required.

To assure dependable UPS performance, regular replacement of UPS batteries is recommended. The replacement frequency depends somewhat on the environmental conditions experienced by the UPS.

- For ambient temperature normally **below 25°C (77°F)**, UPS batteries should be **replaced every 3 years**.
- For ambient temperatures regularly **above 25°C (77°F)**, UPS batteries should be **replaced every 2 years**.

Purchase of **spare batteries** is **Not Recommended**, since they need to be recharged at least every 6 months to maintain their capacity. Instead, batteries should be purchased a few weeks prior to their replacement schedule.

If spare emergency power is desired, purchase of a **spare UPS** is **Recommended** and should be maintained in a charged condition.

Order information and Philips Part Numbers are given in the **Replaceable Parts List**.

Refer to the UPS **User's Manual** for proper battery replacement.

Warning

UPS batteries are lead-acid and must be handled carefully and disposed of properly.

Step 1. Disconnect the power cord of the UPS from the wall outlet or Power Distribution Module for about **3 seconds**.

Step 2. Verify that the Philips system continues to operate and the UPS gives an audible tone.

Step 3. Restore the power cord connection.

Troubleshooting

Network problems present themselves to users through messages and operational problems observed at the Information Center and Patient Monitors. When troubleshooting network problems, tools accessed through the Information Center and Database Server should be used.

The Information Center software provides extensive troubleshooting functionality in its Embedded Management Services (EMS). To best use these tools, a **Troubleshooting Strategy** should generally be employed. The first section provides a systematic troubleshooting procedure for isolating system problems and identifying the proper tool for determining causes and corrective actions. **System Troubleshooting Tables** are also provided.

The EMS troubleshooting tools are then described. These include first level support for users from the **All Controls** menu during patient monitoring and more extensive troubleshooting applications for service personnel from the **Service** menu in non-monitoring mode

Information available for **User Troubleshooting** during patient monitoring include:

- **Error and Status Messages** on the Main Screen that indicate recorder conditions, status of print jobs, and monitor connections
- **Status Log (Quick Unit Status)** for identifying the operational status of devices in their clinical unit
- **Device Setup and Support Information** for determining who to call when a problem cannot be resolved and important identifying information about the device

More advanced resources available for **Service Personnel Troubleshooting** from the **Service** menu are as follows. Note that items with an ! require the device (Information Center or Server) to be taken out of monitoring.

- **Event Logs** for identifying system events and errors
- **Service Logs** for reviewing past service performed on the system
- **Status Log (All Data Categories)** for identifying the operational status of all hardware
- **Network Statistics** for information about network switches
- **Telemetry Services** for information from Telemetry Mainframes
- **!Diagnostic Tools** for troubleshooting Philips and Windows devices
- **!Configuration** tools to reconfigure the system
- **Remote Access Services (RAS)** for remote troubleshooting by Philips service personnel
- **!Shutdown** and restart for rebooting system software.

LED Diagnostics tables are also included that list symptoms displayed by LEDs on nonfunctioning hardware, possible causes, and corrective actions that can be taken to restore functionality.

Troubleshooting Strategy

The flow of information in Clinical Networked systems can be divided into 4 major connectivity components: (See Figure 5-1):

SDN connectivity - flow of real-time patient monitoring data from patient monitors through the SDN to Information Centers for display

Wireless connectivity - flow of real-time patient monitoring data from wireless M3/M4 monitors via Access Points to Information Centers for display

LAN connectivity - flow of real-time patient data from IntelliVue/M3/M4 Patient Monitors and from Information Centers to network-connected Information Centers and Clients for overviewing

Server connectivity - flow of stored patient monitoring data to the Server for storage and out to Information Centers and Clients for review

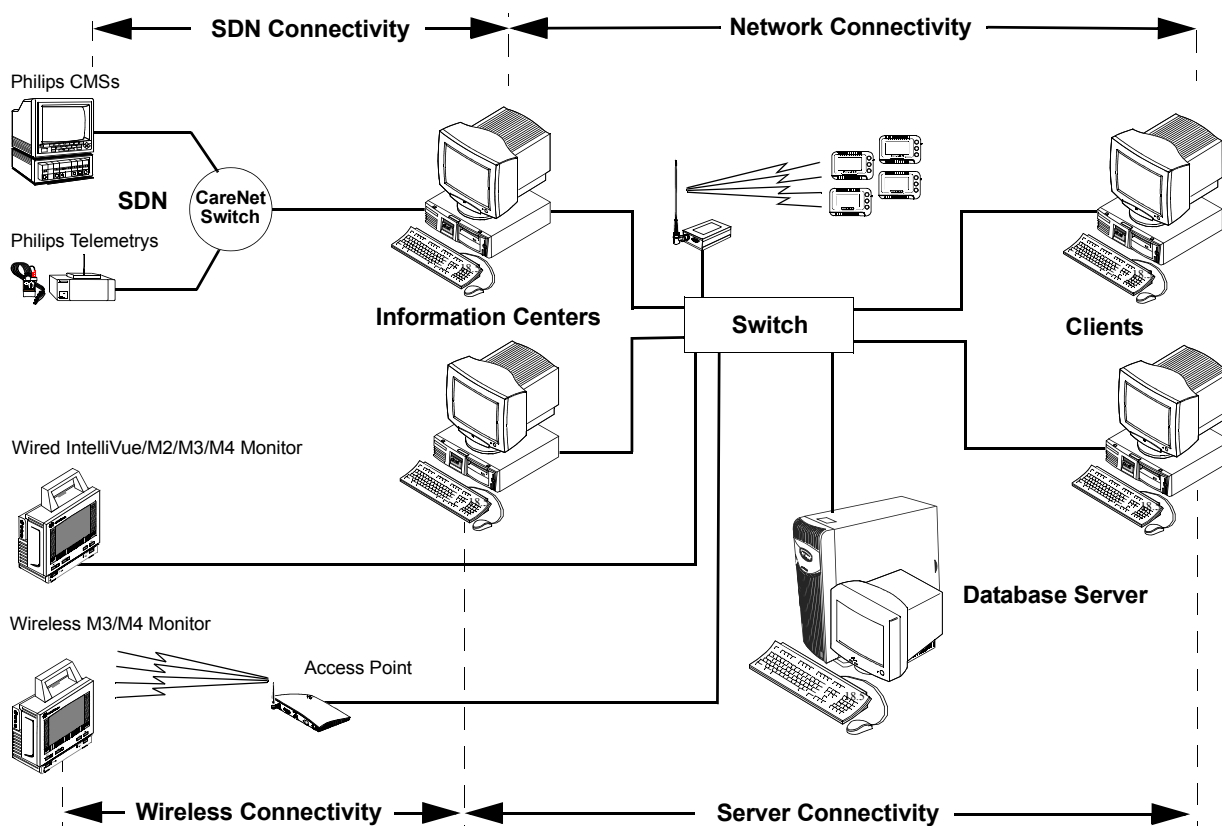


Figure 5-1 Network/Server Connectivity Components

Each connectivity component should be evaluated separately to identify the source of a problem. The following questions can be asked:

- What devices and functions **are working**?
- What devices and functions **are not working**?
- What **tools** can be used to diagnose devices or functions not working?
- What troubleshooting actions will **minimize intrusion** on the user?
- What actions will be the **quickest** to implement?

SDN Connectivity The first step is to investigate **SDN connectivity** -- are real-time patient monitoring data flowing from patient monitors connected to the SDN to Information Centers? Each SDN/Information Center connection should be checked to determine if patient monitoring data are correctly being received and displayed.

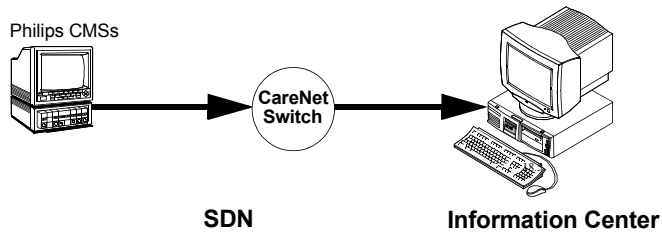


Figure 5-2 SDN Connectivity Investigation

The following table provides a brief guideline for identifying sources of SDN connectivity problems.

Table 5-1. SDN Connectivity Troubleshooting

Assessment	Investigation
Are patient data (waveforms and parameters) from the SCC being properly displayed on the Information Center?	- Check Patient Sectors for each connected patient
Are all devices operational?	- Check status LEDs on each device
Are all devices connected?	- Check Status Log (See Caution)
Is the SDN interface operating correctly?	- Check IC SDN interface card LEDs
Is the SDN configured correctly?	- Check !Bed Config application

Caution

Status Log information may not reflect the current status of other devices on the Network if it has disconnected from the Network, i.e. gone into local database mode.

Wireless Connectivity For networks with wireless Patient Monitors, the next step is to investigate **wireless connectivity** - are real-time patient monitoring data from wireless Patient Monitors being transmitted to Access Points and from Access Points to Information Centers? Each Wireless Patient Monitor/Access Point/Information Center connection should be

checked to determine if patient monitoring data are correctly being received and displayed.

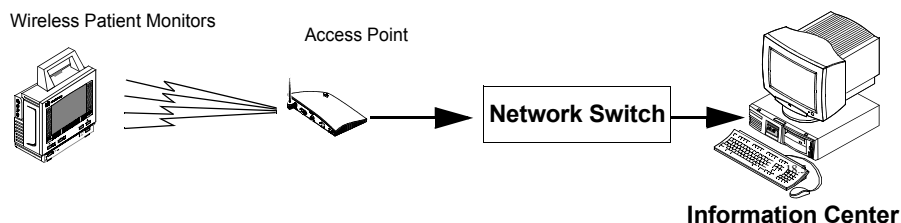


Figure 5-3 Wireless Connectivity Investigation

The following table provides a brief guideline for identifying sources of wireless connectivity problems.

Table 5-2. Wireless Connectivity Troubleshooting

Assessment	Investigation
Are patient data (waveforms and parameters) from each bedside being properly displayed on the Information Center?	- Check Patient Sectors for each connected patient
Are all devices operational?	- Check status LEDs on each device
Are all devices connected?	- Check Status Log (See Caution)
Is the Access Point connection to the Network operating correctly	- check all hard wired connections from the Access Point to the Switch - check Link LEDs on each device - switches, repeaters, media translators
Is the wireless Access Point interface operating correctly?	- Check Access Point LEDs - Check Access Point Network Statistics
Is the wireless network configured correctly?	- Check !Network and !Bed Config applications
For non-standard systems, is any access point or cell overloaded?	- Check Access Point associations in the HTML screens for the access points (Network Map)

Network Connectivity The next step is to investigate **Network connectivity** -- are real time patient monitoring data flowing through the Clinical Network to the Information Centers and from the Information Centers through the Clinical Network to each network-connected Information Center and Client? Each Information Center/device connection should be checked to determine if real time patient monitoring data can be viewed.

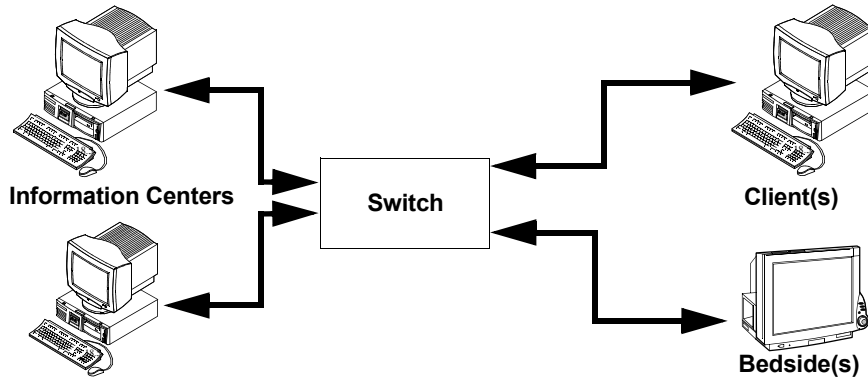


Figure 5-4 Network Connectivity Investigation

The following table provides a brief guideline for identifying sources of Network connectivity problems.

Table 5-3. Network Connectivity Troubleshooting

Assessment	Investigation
Are patient data (waveforms and parameters) from the Networked bedsides being properly displayed on the Information Center?	Check Patient Sectors for each connected patient
Can real-time patient data on Information Centers be overviewed by Clients and other Information Centers?	Check each Client and Information Center for real-time patient data from each Information Center
Can stored patient data on the Server be accessed by Clients and Information Centers?	Check Review Applications for patients on each Information Center and Client and verify their accuracy
Are all bedsides and Information Centers operational?	Check Status LEDs on each device
Are all Network devices operational?	Check Status LEDs on each Network device -- switch, repeaters, media translators
Are all devices connected?	<ul style="list-style-type: none"> • Check Status Log (See Caution) • Ping each device • Check Network Statistics
Are signals flowing properly to and from all Network devices?	<ul style="list-style-type: none"> • Check Link LEDs on each Network device -switches, repeaters, media translators, and LAN interface cards • Check Device LEDs to confirm proper operational speed and duplex • Check Switch Statistics for error conditions suggesting speed and duplex mismatch errors
Are all network devices configured correctly?	<ul style="list-style-type: none"> • Check !Network, !Bed Config applications • Check Network Statistics

Caution

Status Log information may not reflect the current status of other devices on the Clinical Network if it has disconnected from the Network, i.e. gone into local database mode.

Server Connectivity **Server connectivity** -- are patient monitoring data being correctly stored by the Server and accessible from the Server by Information Centers and Clients? Each Server/Device connection should be checked to determine if stored patient monitoring data can be reviewed.

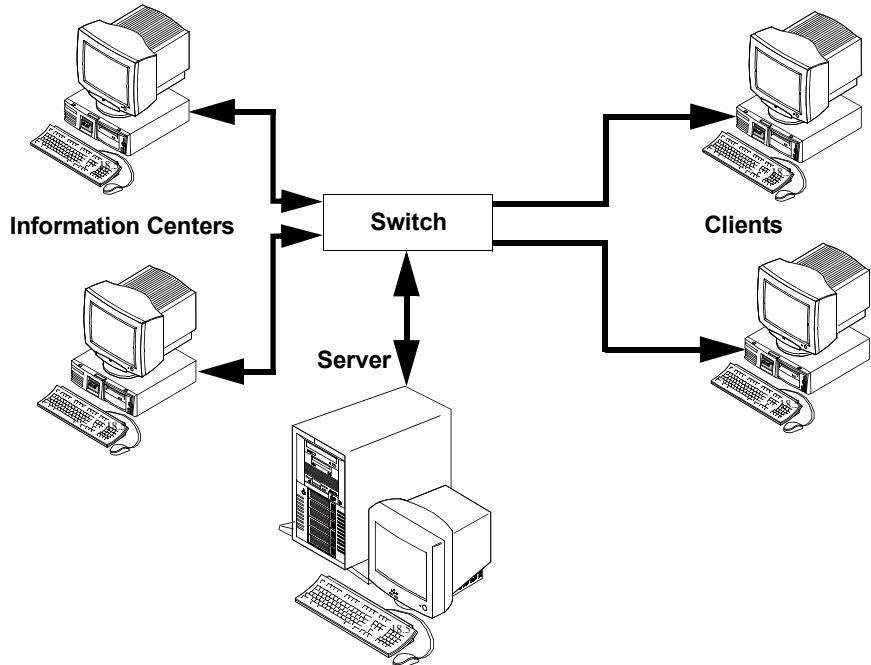


Figure 5-5 Server Connectivity Investigation

The following table provides a brief guideline for identifying sources of Server connectivity problems.

Table 5-4. Server Connectivity Troubleshooting

Assessment	Investigation
Are patient data (waveforms and parameters) being received by the Server?	<ul style="list-style-type: none"> • Check that Information Centers are not in Local Database Mode
Are patient data (waveforms and parameters) being stored correctly by the Server?	<ul style="list-style-type: none"> • Check Review Applications for each connected patient and verify that patient data have been correctly stored
Are all Network devices operational?	<ul style="list-style-type: none"> • Check Status LEDs on each Network device -- switch, repeaters, media translators • Check Device LEDs to confirm proper operational speed and duplex • Check Switch Statistics for error conditions suggesting speed and duplex mismatch errors
Are all devices connected?	<ul style="list-style-type: none"> • Check Status Log (See Caution) • Ping each device from the Server • Check Link LEDs

System Troubleshooting

The following **System Troubleshooting Tables** provide Symptoms, Possible Causes, Verifications, and Corrective Actions to take for problems identified in M3150 Information Centers, M3151 Clients, and the Network/Server System.

Table 5-5. Troubleshooting M3150 Information Centers

Symptom	Possible Cause(s)	Verification	Corrective Action(s)
Information Center - applications shut down - workstation goes to desktop for 10-20 seconds - reboots to local database mode	Information Center has lost connection to network or Server due to: - bad connection to Switch, including cabling - failed component (Repeater, or Media Translator) between Information Center and Switch - loss of Server connection to network	Determine if problem is on the device or the network by observing functionality - check whether Clients are receiving data from Information Center. - determine if other Information Centers are in local database mode - look at Link LEDs on device ports of Network interfaces If only Information Center is affected, problem is likely its network connection If other Information Centers or Clients are affected, problem is likely a network or Server connection Review Event Log, Application Log. An "SDProcess" error message is logged, either - Warning 3257 "System restarted using the local database mode because the server is not available" or - Warning 4208 "Restarting applications because the database server connection is unavailable. System will come up in Local DB."	Test UTP and fiber optic cable connections Re-establish Information Center connection to the network NOTE: When connection is reestablished, Information Centers display "Press Restart Network" at top of display. Use Restart button to reboot the Information Center. For network problems, see Network/Server System Troubleshooting Table
Information Center/Client - Sluggish or slow performance when accessing review applications	Operational Speed and Duplex mismatch settings	Check Device LEDs and Switch Statistics for proper settings	Connect the Information Center/Client to a port configured for 100 Mbps HALF duplex

Table 5-6. Troubleshooting M3151 Information Center Clients

Symptom	Possible Cause(s)	Verification	Corrective Action(s)
<p>Information Center Client</p> <ul style="list-style-type: none"> - waveforms drop out for 15-60 seconds - applications shut down - PC goes to Desktop for 10-20 seconds - reboots to local database mode - displays patient waveforms in sectors where patients were assigned 	<p>Client has lost connection to Server, but still has active network connection to Information Center sourcing data to it.</p> <p>Problem probably also affects other devices on the network</p> <p>Possible causes:</p> <ul style="list-style-type: none"> - bad connection between Switch and Server. May include in-wall and patch cables - failed component (Repeater, or Media Translator) between Server and Switch - Server down - Server in Config mode 	<p>Isolate problem by observing functionality on rest of network.</p> <p>Determine if other Information Centers can receive data from Server</p> <p>If Server’s network connection is lost, then other devices (Information Centers and Clients) should not be able to retrieve stored data and should be in local database mode.</p> <p>Review Event Viewer, Application Log. An “SDProcess” error message is logged, either</p> <ul style="list-style-type: none"> - Warning 3257 “System restarted using the local database mode because the server is not available” or - Warning 4208 “Restarting applications because the database server connection is unavailable. System will come up in Local DB.” <p>Look at Link LEDs on device ports of LAN interfaces to identify the failed connection</p> <p>Test UTP and fiber optic cable connections</p>	<p>Reestablish Server connection to network</p> <p>Reboot Clients if necessary (Clients may reboot automatically)</p>
<p>M3151 Client</p> <ul style="list-style-type: none"> - waveforms dropout for 15-120 seconds - applications shut down - PC goes to Desktop for 10-20 seconds - reboots to local database mode - displays “Monitoring lost for this patient” in sectors where patients were assigned 	<p>Client has lost connection to network due to:</p> <ul style="list-style-type: none"> - bad connection between Client and Switch including in-wall and patch cables - failed component (Repeater or Media Translator) between Client and Switch - network Switch down 	<p>Isolate problem by observing functionality present on rest of network.</p> <p>Determine if Information Centers are operational and can receive data from Server</p> <p>Review Event Log, Application Log. An “SDProcess” error message is logged, either</p> <ul style="list-style-type: none"> - Warning 3257 “System restarted using the local database mode because the server is not available” or - Warning 4208 “Restarting applications because the database server connection is unavailable. System will come up in Local DB.” <p>If problem is isolated to Client connection, then other devices (ICs and Clients) should all be operating normally</p> <p>Look at Link LEDs on device ports of LAN interfaces to identify the failed connection</p> <p>Test UTP and fiber optic cable connections</p>	<p>Reestablish Client connection to network</p> <p>Reboot Client if necessary (Client may reboot automatically)</p>

Table 5-7. Troubleshooting the Network/Server System

Symptom	Possible Cause(s)	Verification	Corrective Action(s)
All M3150 Information Centers and M3151 Clients reboot and go into local database mode	Connection between Switch and Server is lost	All Information Centers and Clients are in local database mode , and Information Centers do not show “Restart Network” message with button Review Event Log, Application Log on Information Centers and Clients. An “SDProcess” error message is logged, either - Warning 3257 “System restarted using the local database mode because the server is not available” or - Warning 4208 “Restarting applications because the database server connection is unavailable. System will come up in Local DB.” If Server connection is lost, Information Centers and Clients will still show Server “offline/idle” in their Status Logs Ping connections between devices and Server to test connectivity	Identify failed link or device Correct failed link or device Reestablish Server connection to Switch Reboot Information Centers and Clients if necessary (Clients may reboot automatically)
	Switch down	Inspect the Switch front panel LEDs for indications of - power loss - device failure - Link LEDs off Review Event Log, Application Log on Information Centers and Clients. An “SDProcess” error message is logged, either - Warning 3257 “System restarted using the local database mode because the server is not available” or - Warning 4208 “Restarting applications because the database server connection is unavailable. System will come up in Local DB.” Ping connections between devices and Server to test connectivity Ping Switch by its IP Address	Identify failed link or Switch Correct failed link or Switch Reestablish Server connection to Switch Reboot Information Centers and Clients if necessary (Clients may reboot automatically)
Clients boot to operating mode but display “Data Lost for this Patient”	Information Centers sourcing data is in Local Database Mode (common during system startup)	Server connectivity must be operational or Client will boot to local database mode	Complete all configurations of data sourcing Information Center Reboot data sourcing Information Center
	Client configuration wrong on Server , e.g. it could be looking for a non-existent SDN source	Review Client’s configuration in Server’s Bed Configuration-Read Only application to confirm	Correct Client’s configuration on Server Reboot all Information Centers and Clients
Some or all Information Centers and Clients reboot and return to normal operating mode	Intermittent network interruption	This condition is difficult to verify. If the network problem is transient, the problem may have cleared after devices reboot	Call Philips Service Representative or Response Center

Network Statistics

The **Network Statistics** tool provides access to operational information from switches and access points on the Clinical Network. This information allows service personnel to determine if network switches and access points are operating within normal bounds, troubleshoot network component failures, and correlate observed application events to network communication problems. **Network Statistics** runs in monitoring mode and is available on the Server and all Clinical Network connected Information Centers and Clients.

Note

If you purchased a new Database Server system, the Network Statistics screen is the HP 2524 as shown below. If you upgraded from an earlier release, you may have a Cisco 1900 switch.

Warning

Do Not Load HP TopTools or any other network management software on the system - it will adversely affect system performance and may result in loss of monitoring.

Switches

Clicking on **Network Statistics** in the Support Logs menu in the Service window brings up the **Network Statistics** window. There are 5 selection options -- **Switches, Access Points, Search by IP, Stop, Print**.

HP 2524 Switch

Select a Switch from the pull-down menu (shows all configured switches) in the Network Statistics window displays the Status Overview window shown in Figure 5-6.

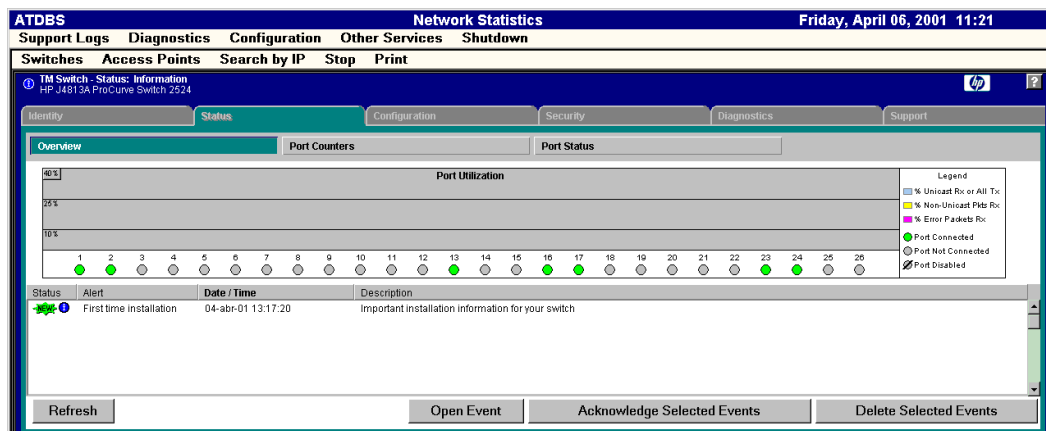


Figure 5-6 Network Statistics for HP 2524 Switch

The **HP2524 Status Overview** window provides the following information about the switch and a switch image:

Status: the level of severity of the event generated.

Alert: the specific event identification. “Excessive CRC/alignment” errors alerts indicate speed and duplex mismatches.

Date/Time: the date and time the event was received by the web browser interface. This value is shown in the format: DD-MM-YY HH:MM:SS AM/PM, for example, 19-04-01 09:15:26 AM.

Description: a short narrative statement that describes the event.

Click on the **Identity** tab to open the window shown in Figure 5-7.

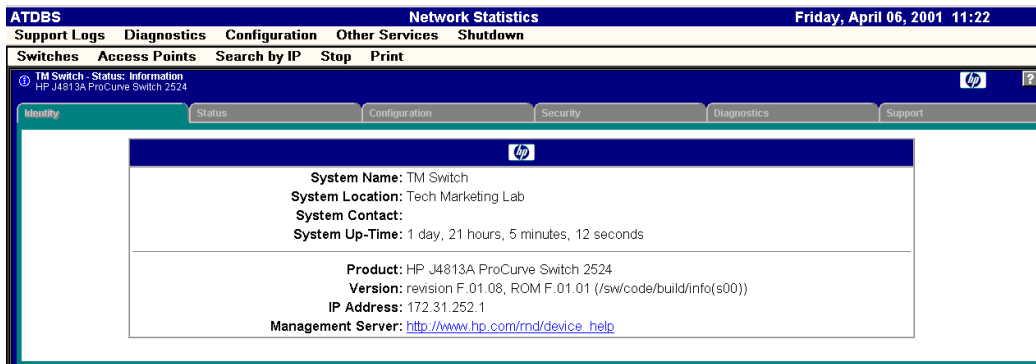


Figure 5-7 Identity Window - HP2524 Switch

The Identity window provides the following information:

System Name: name of the selected switch.

System Location: where the switch is located.

System Contact: person to contact if the system experiences trouble.

System Up-Time: how long the system has been active

Product: displays the HPJ4813A ProCurve Switch 2524 information

Version: firmware version installed

IP Address: IP Address assigned to switch

Management Server: website URL to go to for help

For information on network traffic quality, go to the **Status** tab, and then Port Counters. See Figure 5-8

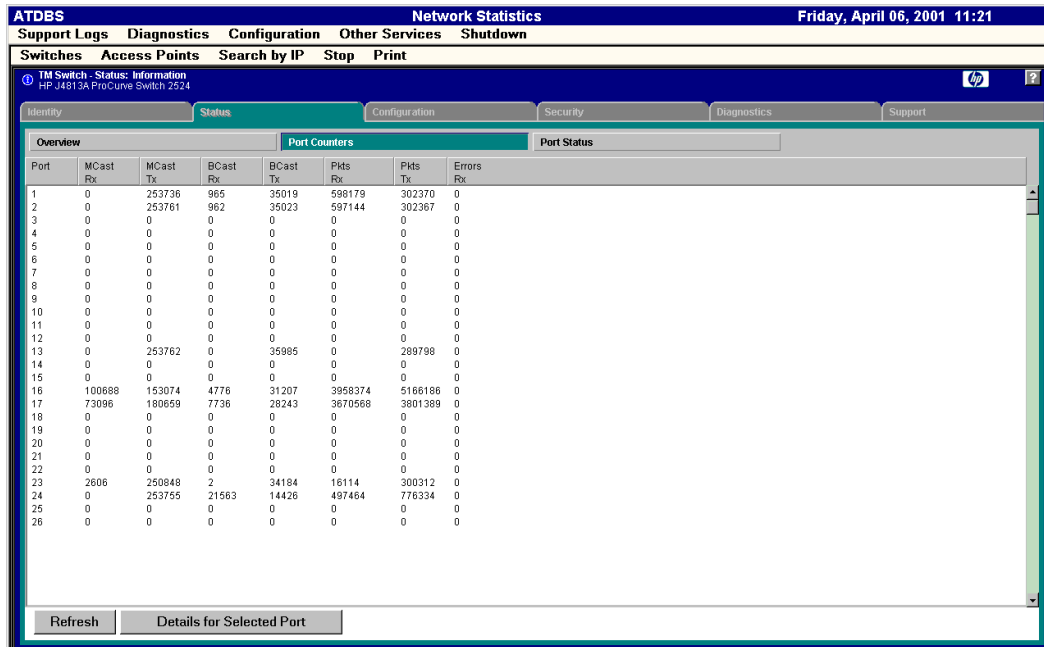


Figure 5-8 Status/Port Counters - HP 2524 Switch

The Device View under Configuration tab (this window gives another visualization of the switch port status - Figure 5-9).

Caution

Do not use the Configuration screens to make modifications to the Switch configuration. Use the Network Configuration Tool described in Chapter 4 to ensure that all parameters are set properly.

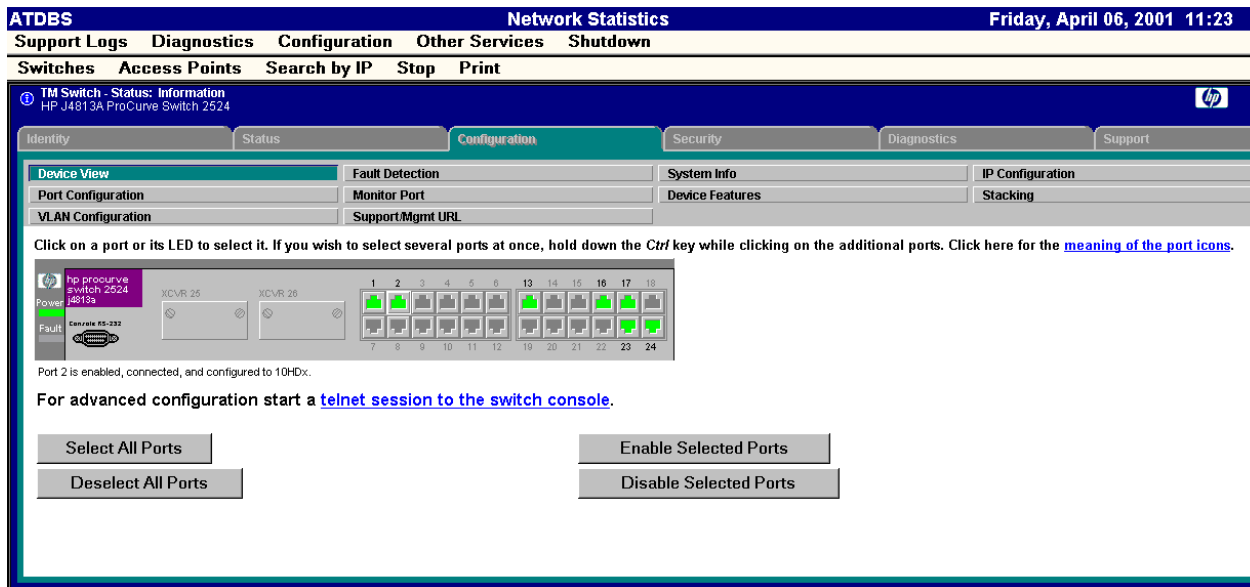


Figure 5-9 Device View - HP 2524 Switch

The System Info window under the Configuration tab is an area where you can give or view the location of the switch and a contact name which will be viewed in the Identity window (Figure 5-7). Enter any information and then click **Apply Changes**. See Figure 5-10.

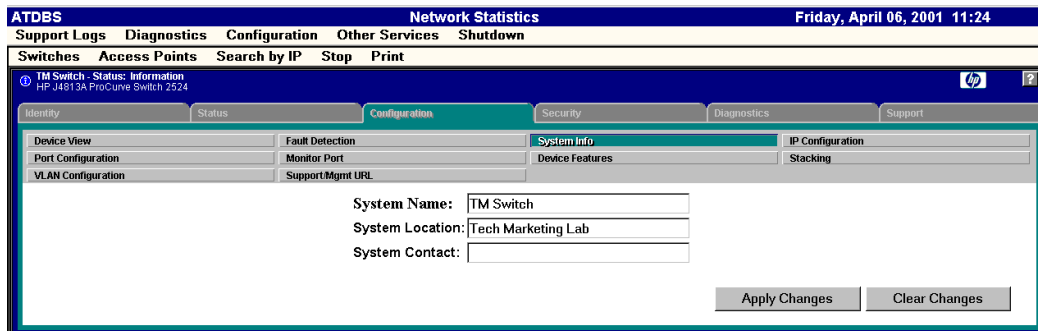


Figure 5-10 System Info - HP 2524 Switch

You can **ping** network devices using the HP 2524 web browser. Click on the **Diagnostics** tab and then the Ping/Link Test to get to the window shown in Figure 5-11. Type in the IP address of the device and press **Start**.

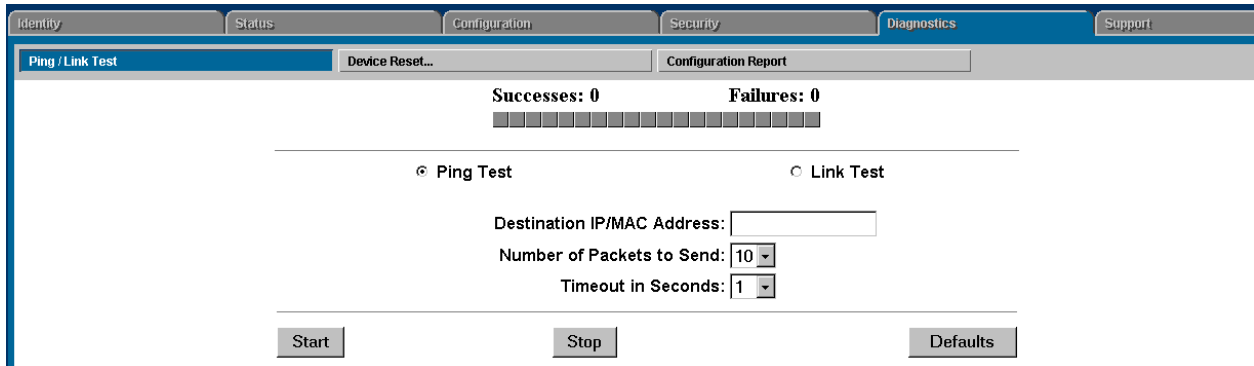


Figure 5-11 Ping/Test Window - HP 2524 Switch

Another diagnostic tool for the HP2524 switch is to view the Port Configuration settings that can be used to determine if speed and duplex mismatches are configured. Click on the **Configuration** tab, and then press the **Port Configuration** button. The window displays the current port configuration settings on the HP2524 switch, as shown in Figure 5-12.

Device View		Fault Detection			
Port Configuration		Monitor Port			
VLAN Configuration		Support/Mgmt URL			
Port	Port Type	Enabled	Config Mode	Flow Control	Bcast Limit
1	10/100TX	Yes	10HDx	Disable	20
2	10/100TX	Yes	10HDx	Disable	20
3	10/100TX	Yes	10HDx	Disable	20
4	10/100TX	Yes	10HDx	Disable	20
5	10/100TX	Yes	10HDx	Disable	20
6	10/100TX	Yes	10HDx	Disable	20
7	10/100TX	Yes	10HDx	Disable	20
8	10/100TX	Yes	10HDx	Disable	20
9	10/100TX	Yes	10HDx	Disable	20
10	10/100TX	Yes	10HDx	Disable	20
11	10/100TX	Yes	10HDx	Disable	20
12	10/100TX	Yes	10HDx	Disable	20
13	10/100TX	Yes	10HDx	Disable	20
14	10/100TX	Yes	10HDx	Disable	20
15	10/100TX	Yes	10HDx	Disable	20
16	10/100TX	Yes	10HDx	Disable	20
17	10/100TX	Yes	10HDx	Disable	20
18	10/100TX	Yes	Auto	Disable	20
19	10/100TX	Yes	100HDx	Disable	20
20	10/100TX	Yes	100HDx	Disable	20
21	10/100TX	Yes	100FDx	Disable	20
22	10/100TX	Yes	100FDx	Disable	20

Figure 5-12 Port Configuration Window - HP2524 Switch

Another diagnostic tool for the HP2524 switch is to view the Configuration settings. To do this, click on the **Diagnostics** tab, and then press the **Configuration Report** button. The resulting text displays the current configuration settings on the HP2524 switch. The following table compares the HP2524 default settings and configured HP2524 (using the ConfigTool, Chapter 4) settings:

Table 5-8. Configuration Parameters

Setting	Factory Default	Recommended (Configured)
System Name	HP ProCurve Switch 2524	Name given to switch
Inactivity Timeout (min)	0	10
Port/Trunk settings (Ports 1-26)		
<i>Type</i>	All set to 10/100TX	All set to 10/100TX
<i>Enabled</i>	All set to Yes	All set to Yes
<i>Mode</i>	All set to Auto	Ports configured to specific mode and speed via the ConfigTool. 10HDx for 10 Mbps Half Duplex devices, 100HDx for 100 Mbps Half Duplex devices, 100FDx for 100 Mbps Full Duplex devices, or Auto for devices set for Auto-Negotiate <i>Example:</i> For a system with a DBS and two extension switches, one port (24) must be set to 100FDx since the DBS requires a 100 Mbps Full Duplex connection. Two ports (22-23) must be set to 100HDx since extension switches require 100 Mbps Half Duplex connections.
<i>Flow Ctrl</i>	All set to Disable	All set to Disable
IP Address		IP Default 172.31.252.0 through 172.31.253.255 Subnet Mask 255.255.0.0
Console/Serial Link		
<i>Inbound Telnet Enabled</i>	Yes	Yes
<i>Web Agent Enabled</i>	Yes	Yes
<i>Terminal Type</i>	VT100	ANSI
<i>Screen Refresh Interval (sec)</i>	3	3
<i>Displayed Events</i>	All	All
<i>Baud Rate</i>	speed-sense	speed-sense
<i>Flow Control</i>	XON/XOFF	XON/XOFF
<i>Session Inactivity Time (min)</i>	0	10
Spanning Tree Operation*		

* The Spanning Tree Operation values are not shown in this window. To see the Spanning Tree values, you must use a HyperTerminal connection. The PC must meet the following requirements.

- Microsoft Operating System software (Windows 2000 or Windows NT)
- 200 MHz or faster
- RS 232 serial interface port (9-Pin D type connector)

If the PC is the Database Server using Hyperterminal from Port A, the UPS connection must be temporarily removed and disabled. The following steps describe the procedure.

Note

Some steps may differ slightly depending on the PC Setup and Operating System.

Step 1. Plug one end of the 9-pin D female - 9-pin D female cable into the RS 232 connector of the configuring PC

Step 2. Plug the other end of the cable into the **CONSOLE** port on the front of the HP ProCurve 2524 switch.

Step 3. Turn On the PC and Switch

If the Server's UPS service detects that the UPS is not connected to Serial Port A, a message indicating **At least one service failed to initialize...** may appear.

If this message appears:

Step 4. Click **OK** and proceed to **Step 11**.

If this message **does not** appear:

Step 5. Go to the **Control Panel** and double click on the **Services** icon (2 gears) to open the **Services** window.

Step 6. Scroll down the list of **Services** to **UPS**.

Step 7. Click on **UPS** to highlight it.

Step 8. Click on the **Stop** button to disable the UPS connection.

Step 9. Click **Yes** to the **Are you sure.** message. A momentary **Attempting to stop...** message will then appear.

When the UPS connection has been disabled:

Step 10. Close the **Services** window and **Control Panel**.

Step 11. Open **HyperTerminal**.

Note

If a **Connection Description** window appears, click **Cancel** to close it.

Step 12. Click on **File -> Properties** to open the **New Connection Properties** window.

Step 13. Click on the **Connect to** tab to display its menu.

Step 14. Click on the **Connect Using** pull down arrow to display its menu.

Step 15. Click on **COM1**

Step 16. Click on **Configure** to display the **COM1 Properties** window.

Step 17. Configure the COM1 port to the following RS 232 settings:

Bits per second:	9600
Data bits:	8
Parity:	None

Stop bits: 1
 Flow control: Xon/Xoff

Step 18. Press **Enter** twice to get to the command line. If the command line does not appear, recycle power on the switch (disconnect and connect power cable).

Step 19. At the command line prompt, enter the following:

- Type **2** for **Switch Config**
- Type **4** for **Spanning Tree operation**

The first 8 ports are displayed. To view the other ports, go to **Edit** and press **Enter**. Use the down arrow navigate.

The ports configured to **10/100 Mb/s half duplex** should be set to **FAST** mode, and the **100 Mb/s full duplex** ports should be set to **NORM**.

- When done, press **Enter**
- Press **Cancel**

Step 20. Close the Hyperterminal session.

Cisco 1900 Switch

Clicking on Switch in the Network Statistics window on upgraded systems displays the list of switches (and their IP Address configured in Network Configuration). Clicking on a switch in the list displays the **Catalyst 1900 Switch Manager** window shown in Figure 5-13. If asked for a user name and password, enter the Console Password, **m3150**.

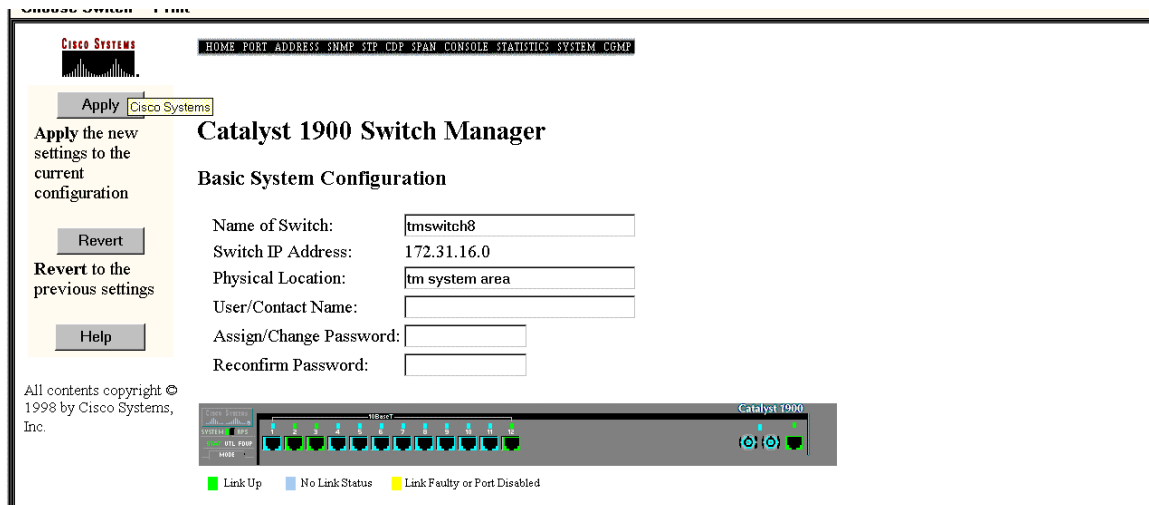


Figure 5-13 Network Statistics Window for Cisco Switch

The **Catalyst 1900 Switch Manager** window provides the following information about the switch and a switch image:

Host Name of the Server the switch is connected to is in the upper left corner of the window.

Name of Switch: the Device Name assigned to the switch in Network Configuration.

Switch IP Address: the IP Address of the switch on the network.

Physical Location: the location of the switch as entered in Network Configuration.

The **Help** button provides access to Windows help information. Help screens may cause temporary color changes to the Philips monitoring screens but do not otherwise effect patient monitoring display or storage.

Note

This application allows the user to change switch settings. However, **changing switch settings should only be done by a with the Network Configuration Tool described in Chapter 4 to ensure all parameters are set properly.**

The **Switch Manager** window also provides an image of the selected switch. Clicking on a port in the switch image brings up a **Ports Table** with statistical information about each port on the switch. Figure 5-14 shows the **100 Base T Ports Table** for ports used by another switch (0/26) and the Server (027).

100 Base-T Ports Table:

Module	Port	Status: Requested Actual	Duplex Mode: Requested Actual	Flood Unknown MACs	Enhanced Congestion Control	Port Name/ Description	Statistics
System	FastEthernet 0/26	<input checked="" type="checkbox"/> Enable suspended- linkbeat	Full duplex Full duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast	Disabled		Stats...
	FastEthernet 0/27	<input checked="" type="checkbox"/> Enable enabled	Full duplex Full duplex	<input checked="" type="checkbox"/> unicast <input checked="" type="checkbox"/> multicast	Disabled		Stats...

Figure 5-14 100 Base T Ports Table

Clicking on **Stats...** in the **Statistics** column of a port brings up a **Detailed Port Statistics Report** for that port. Figure 5-15 shows the Detailed Port Statistics Report

for port 0/27, which is used by the Database Server. Report statistics are cumulative from the time the device was started or since the Report was last cleared.

Detailed Port Statistics			
FastEthernet 0/27 Statistics Report			
Receive Statistics		Transmit Statistics	
Total good frames:	3963738	Total frames:	5213256
Total octets:	547988387	Total octets:	2836851515
Broadcast/multicast frames:	108060	Broadcast/multicast frames:	724259
Broadcast/multicast octets:	15491082	Broadcast/multicast octets:	50863645
Good frames forwarded:	3963727	Deferrals:	0
Frames filtered:	11	Single collisions:	0
Runt frames:	48	Multiple collisions:	0
No buffer discards:	0	Excessive collisions:	0
		Queue full discards:	0
Errors:		Errors:	
FCS errors:	0	Late collisions:	0
Alignment errors:	0	Excessive deferrals:	0
Giant frames:	0	Jabber errors:	0
Address violations:	0	Other transmit errors:	0

Figure 5-15 Detailed Port Statistics Report for the Database Server

Access Points

Access Points provides a list of the networked access points configured in Network Configuration. Clicking on Access Points in the Network Statistics window displays the list of Access Points (and their IP Address). Clicking on an Access Point in the list displays the **RangeLAN2 Manager** window shown in Figure 5-16, which is Proxim's **web manager for wireless networks**. This window provides a variety of status and statistical information about the selected access point.

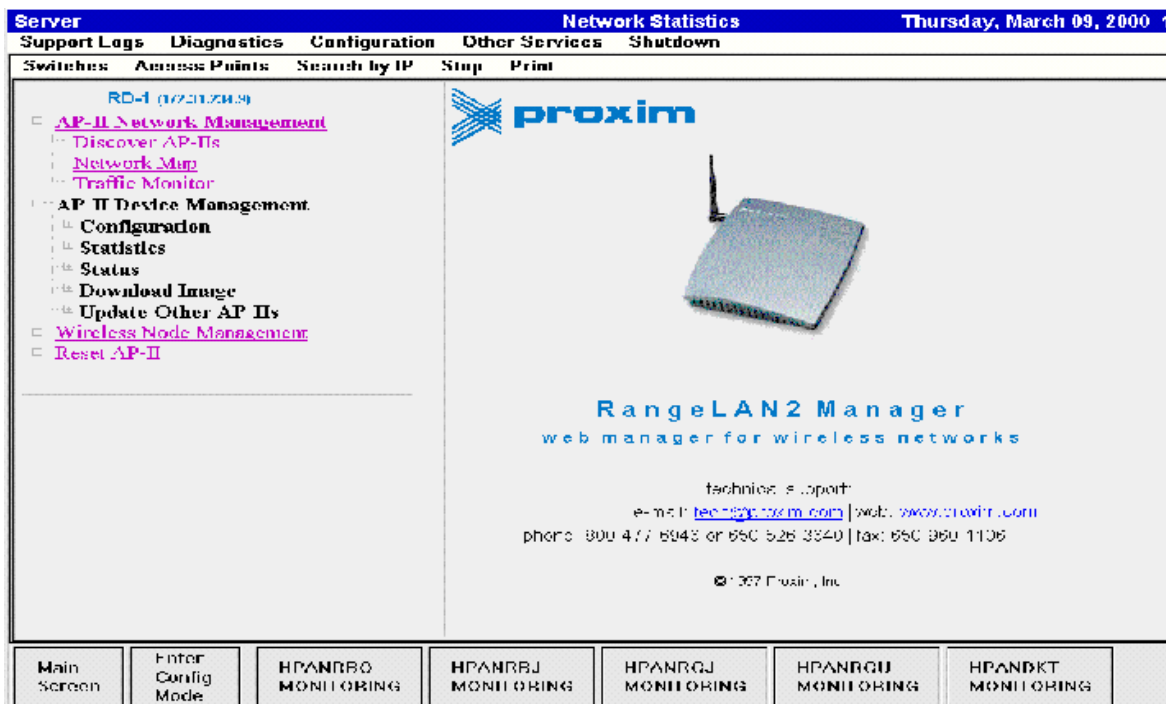


Figure 5-16 RangeLAN2 Manager Window

The left section of this window provides a menu of tools for reviewing and troubleshooting the performance of Access Points on the network. Tools for reviewing the performance of selected Access Points include:

In the **AP-II Network Management** menu:

Discover AP-IIs displays all Access Points detected on the network, including their **Master Name**, **IP Address**, **MAC Address**, **Domain**, **Channel**, and **Subchannel**. See Figure 5-17.









Switches		Access Points		Search by IP	Stop	Print	
A11 (172.31.234.70)		RangeLAN2 AP-IIs					
<ul style="list-style-type: none"> AP-II Network Management <ul style="list-style-type: none"> Discover AP-IIs Network Map Traffic Monitor AP-II Device Management <ul style="list-style-type: none"> Configuration Statistics Status Download Image Update Other AP-IIs Wireless Node Management <ul style="list-style-type: none"> Reset AP-II 		Master Name	IP Address	MAC Address	Domain	Channel	Subchannel
		 B36	172.31.234.75	00:20:A6:33:A1:0F	3	6	1
		 A47	172.31.234.76	00:20:A6:34:B4:EC	4	7	1
		 A11	172.31.234.70	00:20:A6:38:5E:4A	1	1	1
		 A23	172.31.234.72	00:20:A6:38:B2:E4	2	3	1
		 B12	172.31.234.71	00:20:A6:38:B4:3A	1	2	1
		 B48	172.31.234.77	00:20:A6:38:C7:DB	4	8	1
		 C610	172.31.234.79	00:20:A6:38:F1:82	6	10	1
		 C711	172.31.234.80	00:20:A6:38:F2:93	7	11	1

Figure 5-17 Discover AP-IIs Window

Network Map displays the **Access Points** configured to the network and the **MAC Address** of the M3/M4 monitors presently transmitting to each Access Point. See Figure 5-18.






Switches		Access Points		Search by IP	Stop	Print
A11 (172.31.234.70)		RangeLAN2 AP-IIs				
<ul style="list-style-type: none"> AP-II Network Management <ul style="list-style-type: none"> Discover AP-IIs Network Map Traffic Monitor AP-II Device Management <ul style="list-style-type: none"> Configuration Statistics Status Download Image Update Other AP-IIs Wireless Node Management <ul style="list-style-type: none"> Reset AP-II 		 A11	 A47	 A23	 B12	
		172.31.234.70	172.31.234.76	172.31.234.72	172.31.234.71	172.31.234.80
		00:20:A6:38:5E:4A	00:20:A6:34:B4:EC	00:20:A6:38:B2:E4	00:20:A6:38:B4:3A	00:20:A6:38:F2:93
		00:10:83:19:1B:2C	00:10:83:19:1B:4B	00:10:83:19:0A:BB	00:10:83:19:1B:2A	00:10:83:19:1B:2A
		00:10:83:19:7A:06	00:10:83:19:6A:8E	00:10:83:19:7A:41	00:10:83:19:1B:A8	00:60:B0:7F:BB:B5
		00:60:B0:7F:BB:B5	00:10:83:19:7A:00	00:10:83:19:7A:46	00:10:83:19:2B:E0	00:10:83:19:7A:85
			00:10:83:19:0A:3F	00:10:83:19:7A:A6	00:10:83:19:7A:85	00:10:83:19:7A:85
					00:60:B0:7F:BB:B4	00:20:A6:38:F2:93
		<input type="button" value="Update"/>				

Figure 5-18 Network Map Window

Clicking on the picture of an Access Point displays the configuration page for that device. An **update** button refreshes the fields to current information.

Traffic Monitor displays a real-time graph of the traffic processed by each Access Point.

In the **AP-II Device Management** menu:

Statistics displays a menu of statistical tools

Ethernet provides Ethernet statistics and error information for Access Point data reception and transmission.

Status displays a menu of status tools.

Radio provides information on the current configuration and status of Access Points.

The **other three options** in the menu of **Network Statistics** do the following:

Search by IP displays a window for selecting a Switch or Access Point by typing in its IP Address:

- Type in the **IP Address** of the device whose statistics are desired.
- Click **OK** and the **Statistics** window for that device will display.

Stop terminates a search for the **Statistics** window of a Switch or Access Point before it has completed.

Print brings up the **Print Manager** window for printing the information on the page being viewed to a networked printer.

Diagnostics

The **Diagnostics** menu provides two types of troubleshooting diagnostic tools -- Philips Software Tools and Windows Tools.

Service Portal Support

One useful diagnostic capability that can be accessed from the **Diagnostics** menu of the Database Server is **Service Portal Support**. This application provides direct access to most of the **Support Logs** for all devices on the network -- Information Centers, Clients, Switches and Access Points.

Note

The **Event Log** and its Application and System log files are not available when using Service Portal Support.

Click on **Windows Explorer** in the **Diagnostics** menu of the Database Server and display the **D:** drive, as shown in Figure 5-19.

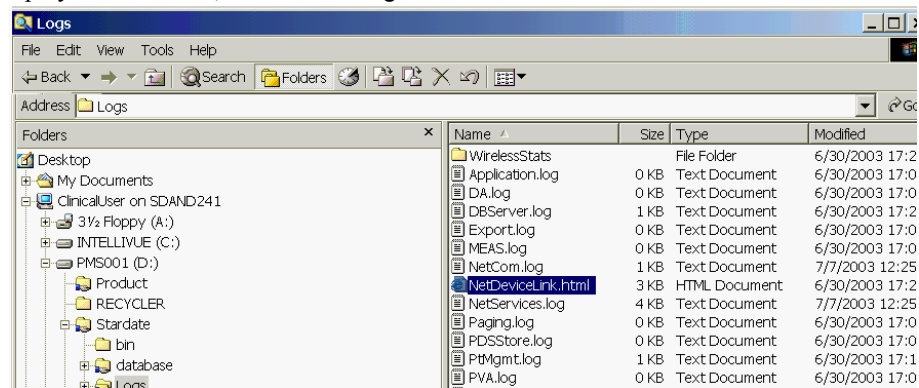


Figure 5-19 D:\ Directories of the Database Server

To start Service Portal Support, double-click on **NetDeviceLink.html** in the **Logs** directory of the **Startdate** directory of the Server's **D:** drive. This opens the **RAS Link to Network Devices** window shown in Figure 5-20.

Note

Service Portal Support capability is also available to a remote PC accessing the Server through **Remote Access Services**. See the **Information Center/Database Server Installation and Service Manual, Appendix D**.

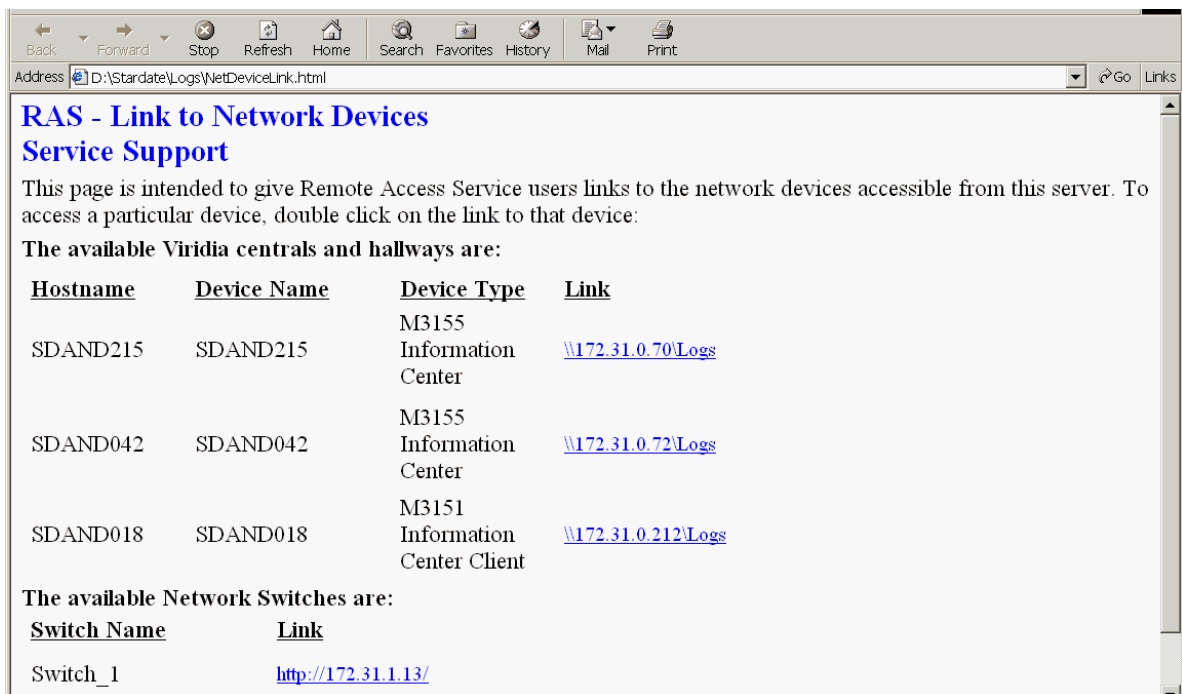


Figure 5-20 Link to Network Devices Window

Clicking on the **Link** next to each device will display a menu of available **Logs** for that device. For example, clicking on the Link <\\172.31.0.70\Log> next to the **Device Type M3155**, brings up a **Logs** window where icons for each of the logs available through Service Portal Support are displayed.

Clicking on an icon will display the logs from that application. Similarly, clicking on a **Switch Link** or **Access Point Link** will bring up the **Network Statistics** windows for that device as described in **Network Statistics**.

Files can also be printed to a floppy disk by clicking on **File** in the upper row menu and then **Send To** and **3 1/2 Floppy (A)**, as shown in Figure 5-21. This will cause the files to be printed to a floppy disk in the Server's **A:** drive.

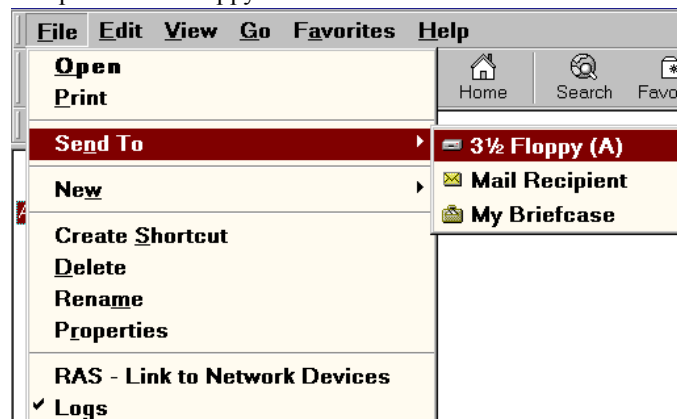


Figure 5-21 Printing Files to a Floppy Disk

LED Diagnostics

When investigating signal flow, many hardware components have diagnostic LEDs that can be used to determine whether they are functioning properly and are receiving and passing data. These include:

- LAN Interface Card
- RangeLAN2 Access Point
- HP2524 Switch
- Cisco Switch
- Allied Telesyn AT-FS708 switch
- 10 Mbps Media Translator
- 100 Mbps Media Translator

Brief description of these LED diagnostic tools and the meaning of their lighting codes are presented in this section as a guide for determining operational status, identifying hardware problems, and tracing signal continuity in the Patient Care Network. For more detailed discussions of the use of these LEDs in troubleshooting, consult their User's Manuals.

LAN Interface Card

Continuity of signal flow in LAN cards can be determined by **Link LEDs** on the rear of the card. The locations of these LEDs on LAN cards for Workstations and the Server are shown in **Figure 5-22**.

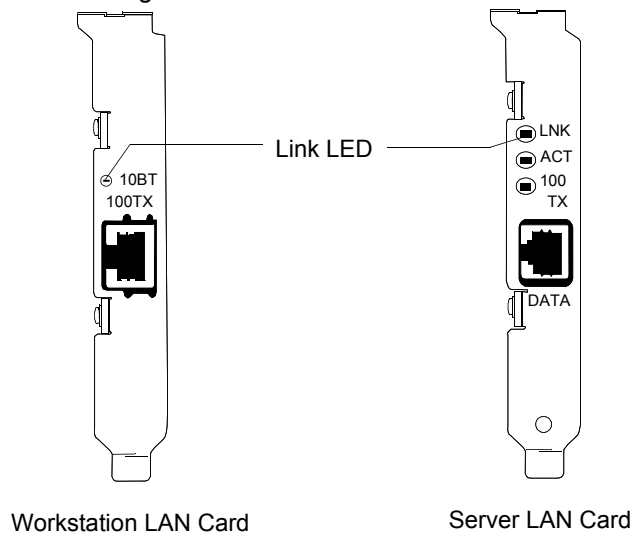


Figure 5-22 LAN Card Link LEDs

Table 5-9 shows the meaning of the green Link LED that can be viewed through the hole in the rear of the card.

Table 5-9. LAN Card LED Diagnostics

LED Condition	Description	Possible Cause
Off	No Link	- no connection - device at other end of cable is Off - faulty cable - inverted TX/RX
Solid Green Flashing Green	Operational	- proper operation with or without activity

Harmony Access Point LED Diagnostics

The Harmony Access Point has LEDs on its top panel and rear panel that indicate Access Point functional and data transmission status. The three top panel LEDs are shown in Figure 5-23.

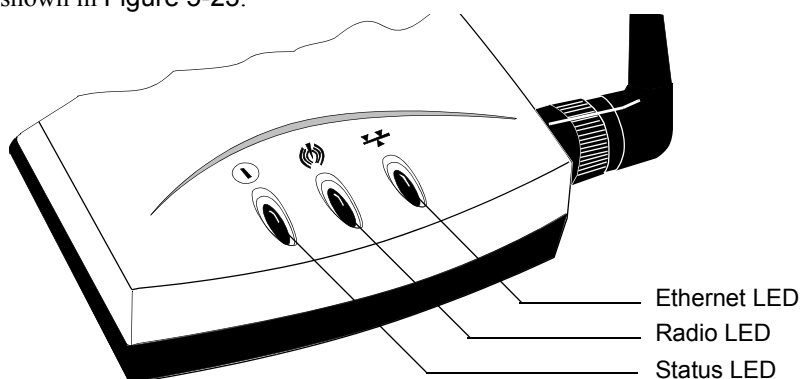


Figure 5-23 Top Panel Harmony Access Point LEDs

Table 5-10 shows the meaning of the top panel LEDs.

Table 5-10. Harmony Access Point Top Panel LED Diagnostics

LED	LED Condition	Description
Status	off	no power to unit
	orange	power-on diagnostics are running not connected with Harmony Access Point Controller
	green	Harmony Access Point is functioning normally
	blinking red	failure during operation
Radio	off	- no power to unit - power-on diagnostic running - power-on diagnostics failed
	blinking orange	- Access Point is transmitting data normally on the wireless link
Ethernet	off	- no power to unit - power-on diagnostic running - power-on diagnostics failed
	blinking green	Harmony Access Point is transmitting data normally over the Ethernet Port

The rear panel LEDs are shown in Figure 5-24

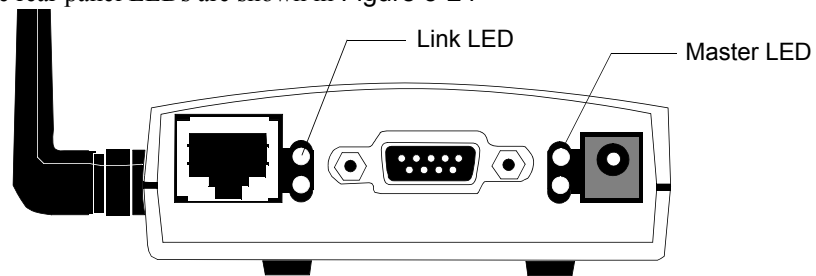


Figure 5-24 Rear Panel Harmony Access Point LEDs

Table 5-11 shows the meaning of the rear panel LEDs.

Table 5-11. Harmony Access Point Rear Panel LED Diagnostics

LED	LED Condition	Description
Master	off	no power to unit
	steady green	Harmony Access Point powered on and operational
Link	off	Normal Operation
	steady green	Harmony Access Point is physically connected to the Ethernet network. May blink momentarily during Ethernet activity.

**RangeLAN2
Access Point**

The Access Point has LEDs on its top panel and rear panel that indicate Access Point functional and data transmission status. The three top panel LEDs are shown in Figure 5-25.

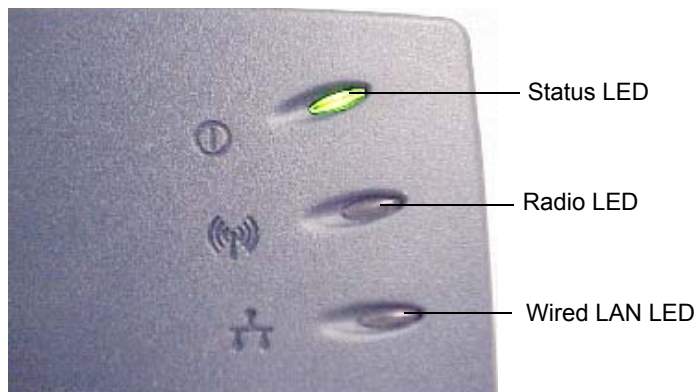


Figure 5-25 Top Panel Access Point LEDs

Table 5-12 shows the meaning of the top panel LEDs.

Table 5-12. Access Point Top Panel LED Diagnostics

LED	LED Condition	Description
Status	off	no power to unit
	orange	power-on diagnostics are running
	green	Access Point is functioning normally
	red	power-on diagnostics failed indicating a hardware problem
Radio	off	<ul style="list-style-type: none"> no power to unit power-on diagnostic running power-on diagnostics failed no wired or RF activity
	blinking yellow	Access Point is transmitting data normally on the wireless link
Wired LAN	off	<ul style="list-style-type: none"> no power to unit power-on diagnostic running power-on diagnostics failed no wired or RF activity
	blinking green	Access Point is transmitting data normally over the wired LAN

The rear panel LEDs are shown in Figure 5-26.



Figure 5-26 Rear Panel Access Point LEDs

Table 5-13 shows the meaning of the rear panel LEDs.

Table 5-13. Access Point Rear Panel LED Diagnostics

LED	LED Condition	Description
Master	off	no power to unit
	steady green	Access Point is configured as a Master (normal operation)
Synchronized to Master LED	off	Normal Operation
	steady green	Access Point is a Station, synchronized to a Master. Fault condition, access point must be configured as a Master
10BASE-T Link Indicator	off	<ul style="list-style-type: none"> no power to unit 10BASE-T cable is not plugged in or is mis wired
	steady green	10BASE-T cable is plugged in and an active network component is detected at the other cable end (normal operation)

Access Point Controller LED Diagnostics

The Harmony Access Point Controller has LEDs on its front panel and rear panel. These LEDs are shown in Figure 5-27 and Figure 5-28.

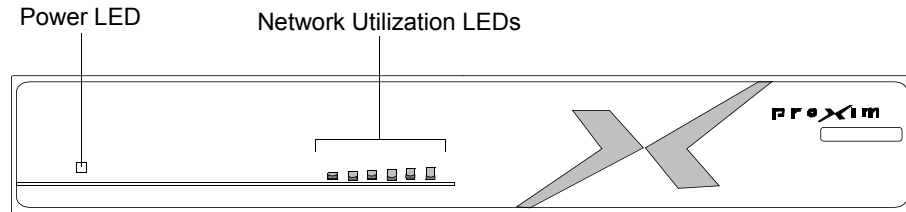


Figure 5-27 Access Point Controller Front Panel LEDs

Table 5-14 shows the meaning of the top panel LEDs.

Table 5-14. Access Point Controller Front Panel LED Diagnostics

LED	LED Condition	Description
Power	off	no power to unit
	orange	initializing
	green	Access Point Controller is functioning normally
	red	failure during operation (try recycling power)
Network Utilization		Indication of network traffic: left LED shows less than 20% utilization, as traffic increases, more LEDs turn on. When all 6 LEDs are on, network utilization is > 90%. The utilization is updated 10 times/second.

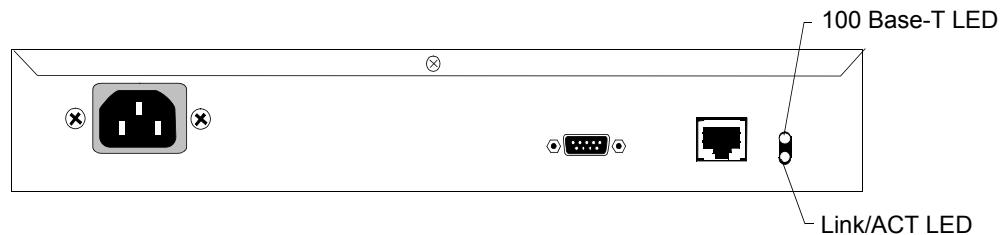


Figure 5-28 Access Point Controller Rear Panel LEDs

Table 5-15 shows the meaning of the rear panel LEDs

Table 5-15. Access Point Controller Rear Panel LED Diagnostics

LED	LED Condition	Description
100 Base-T	off	no network connectivity or connectivity to 10 Base-T network
	green	connected successfully to 100 Base-T network
Link/ACT	yellow	APC has physical connection to network
	blinking yellow	APC is transmitting data normally on the wireless link
	off	failure with network link

Remote Power System LED Diagnostics

The Power System has LEDs on its front panel. These LEDs are shown in Figure 5-29.



Figure 5-29 Remote Power System LEDs

Table 5-16 shows the meaning of the LEDs.

Table 5-16. Remote Power System Port LED Diagnostics

LED Condition	Description
Off	Non-active load or unplugged port; Power to port is disconnected
Green	Active load is plugged in and complies with normal conditions
Orange	Overload conditions; Power to port is disconnected
Blinking Green	Transitional mode in which load detection is in process; Power to the port is disconnected
Blinking Orange	Total aggregated power exceeds pre-defined power budget; Power to the port is disconnected

HP2524 Switch

The HP 2524 Switch contains a number of LEDs on its front panel that can be used for diagnosing switch problems. Figure 5-30 shows the locations of these LEDs.

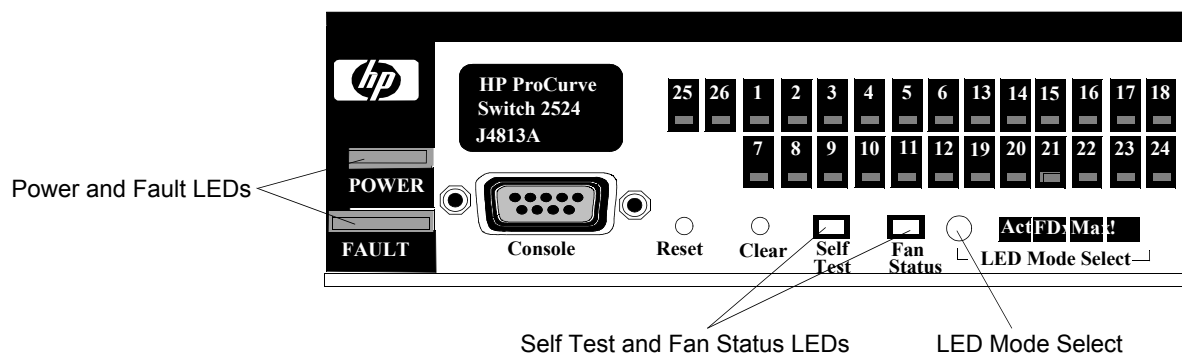


Figure 5-30 HP 2524 Switch LEDs

These LEDs indicate the following information:

Table 5-17. Switch LED Descriptions

Switch LED	LED Condition	Description
Power (green)	On	Switch is receiving power
	Off	Switch is NOT receiving power
Fault (orange)	Off	The normal state; indicates that there are no fault conditions on the switch
	Blinking	A fault has occurred on the switch, one of the switch ports, or the fan. The Status LED for the component with the fault will blink simultaneously.
	On	On briefly after the switch is powered on or reset, at the beginning of switch self test. If this LED is on for a prolonged time, the switch has encountered a fatal hardware failure, or has failed its self test.
Self Test (green)	Off	The normal operational state; the switch is not undergoing self test
	On	The switch self test and initialization are in progress after you have power cycled or reset the switch. The switch is not operational until this LED turns off. the Self Test LED also comes on briefly when you “hot swap” a transceiver into the switch; the transceiver is self tested when it is hot swapped.
	Blinking	A component of the switch has failed its self test. The status LED for the component, for example, an RJ-45 port, and the switch Fault LED will blink simultaneously.
Mode Select (3 green LEDs)	Act	Indicates that the port Mode LEDs are displaying network activity information.
	FDx	Indicates that the port Mode LEDs are lit for ports that are in FULL DUPLEX mode
	Max	Indicates that the port Mode LEDs are lit for ports that are operating at their maximum possible link speed (100 Mbps).
	!	Indicates that the port Mode LEDs are displaying network events that could require operator attention, for example, CRC errors or late collision.
Fan Status (green)	On	The cooling fan is operating normally
	Blinking	The cooling fan has failed. The switch Fault LED will be blinking simultaneously.

Refer to the HP2524 **Installation and Getting Started Guide** for additional information on the HP2524 ProCurve Switch.

Cisco Switch

The Switch contains a number of LEDs on its front panel that can be used for diagnosing switch problems. Figure 5-31 shows the locations of these LEDs.

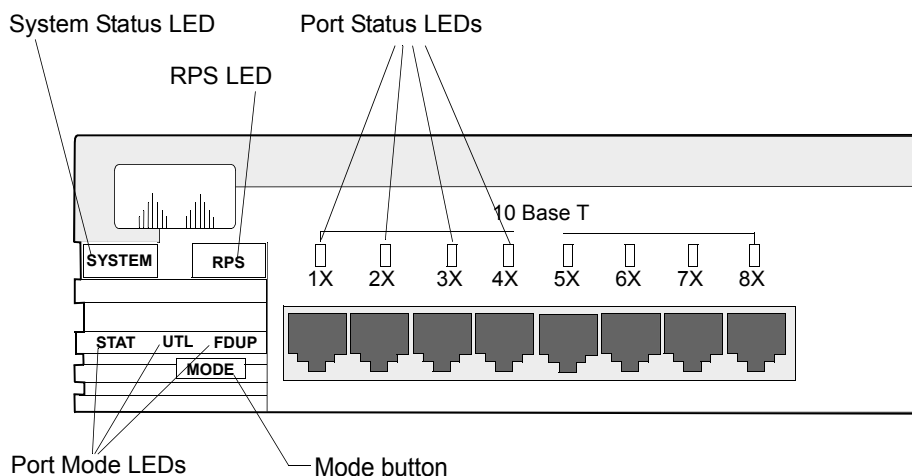


Figure 5-31 Cisco Switch LEDs

These LEDs indicate the following information:

- **System status LED** indicates the operational status of the switch
- **Redundant Power System (RPS) LED** indicates the status of the RPS system (not used in this application)
- **Port mode LEDs** indicate the mode selected using the MODE button
- **Port Status LEDs** above each Switch port indicate the network activity and performance of that port. Their meaning depends on the Port Mode selected by the MODE button, as described below.

The **MODE** button selects the mode of detection of the Port Status LEDs. **Port Mode LEDs** indicate the MODE button selection.

STAT = Port status mode - Port Status LEDs indicate the link beat and activity status of each port

UTL = Bandwidth utilization mode - Port Status LEDs indicate the current and peak bandwidth utilization of the switch

FDUP = Full-duplex status mode - Port Status LEDs indicate if the port is operating in half (off) or full (solid green) duplex mode

Table 5-18 summarizes **Port Status LED** indications in STAT mode.

Table 5-18. Port Status LED Diagnostics

LED Condition	Description	Possible Cause
Off	Link beat signal not being received	- no connection - device at other end of cable is Off - faulty cable
Solid Green	Link operational	- no link activity
Flashing Green	Link beat signal being received	- link activity

Table 5-18. Port Status LED Diagnostics

LED Condition	Description	Possible Cause
Solid amber	Port is not forwarding	- disabled by management - redundant path (loop)
Alternating green/ amber	Link fault	- excessive collisions - CRC errors - alignment/jabber errors

Table 5-19 summarize **System Status LED** indications.

Table 5-19. System Status LED Diagnostics

LED Condition	Description	Possible Cause
Off	Switch is not powered up	- no power to switch
Solid Green	Operational	- proper operating condition
Solid Amber	Switch powered up but not functioning properly	- one or more non-fatal power-on self-test (POST) errors occurred. Refer to the Management Console Logon Screen for messages identifying which POST failed

Allied Telesyn AT-FS708 switch

The Allied Telesyn switch only supports auto-negotiation. It can be used to interconnect a variety of devices. As a result, the auto-negotiated speed and duplex setting of each port depends on the devices it is connected to. See the port speed and duplex requirements in “Device Requirements with Applicable Port Settings” on page 3-12. This switch contains a number of LEDs on its front panel that can be used for diagnosing switch problems. Figure 5-32 shows the locations of these LEDs

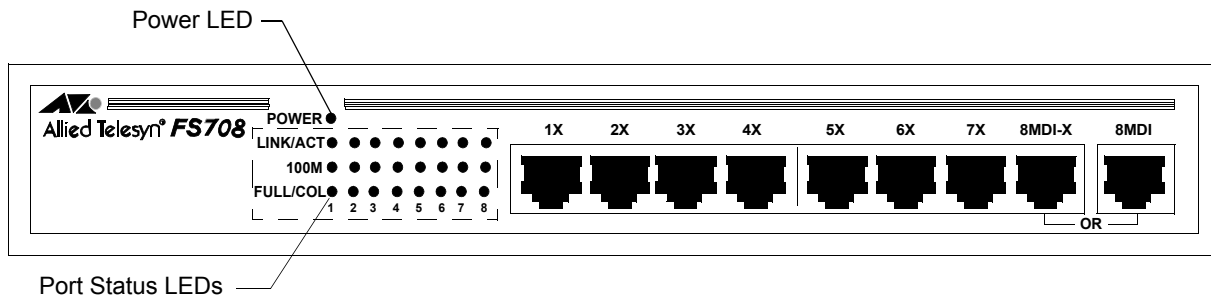


Figure 5-32 Front Panel LEDs of the Extension Switch

LED Status Indicators

The front panel has a POWER LED and 3 status LEDs for each port - LINK/ACT, 100M, FULL/COL. Table 5-20 describes the meaning of each LED indication.

Table 5-20. LED Status Indications

LEDs	Color	Description
POWER	Green	On indicates there is power to the switch OFF indicates there is no power to the switch

Table 5-20. LED Status Indications

LEDs	Color	Description
LINK/ACT	Green	On indicates a valid physical link on the port Blinking indicates data are being transmitted or received Off indicates no link
100M	Green	On indicates the bandwidth is 100 Mbps Off indicates the bandwidth is 10 Mbps
FULL/COL	Green	On indicates full-duplex operation mode Blinking indicates data collisions in half-duplex mode Off indicates half-duplex transmission mode

Ports 1 - 7 LED Status Indications Status LED indications for Ports 1 - 7 for each of these network devices are given in Table 5-21.

Table 5-21. Port 1 LED Indications for Various Network Devices

Ports 1 - 7 LEDs	Patient Monitor	Wireless Access Point	Network Printer
LINK/ACT	On or Blinking	On or Blinking	On or Blinking
100M	Off	Off	Off
FULL/COL	Off	Off	Off

Port 8MDI LED Status Indications To properly operate with an Extension Switch, the port on a Core and Edge Switch should be configured for **Auto Negotiate**. The Extension switch will then auto-negotiate to **100 Mbps, Full duplex**.

Note The switch port on a Core or Edge Switch must be configured for **Auto Negotiate**. If it is not, the AT-FS708 will not properly negotiate with the switch and will default to 100Mbps, half-duplex. The duplex mismatch results in many Frame Check Sequence (FCS) errors, which will degrade network performance.

Status LED indications for Port 8MDI on the Extension Switch for the two switches connected to Port 8MDI are given in Table 5-22.

Table 5-22. Port 8MDI LED Indications for Various Switches

Port 8MDI LED	Core Switch	Edge Switch
LINK/ACT	On or Blinking	On or Blinking
100M	On	On
FULL/COL	On	On

J3300 10Base-T Hub

The J3300A also contains a number of front panel LED indicators. See Figure 5-33.

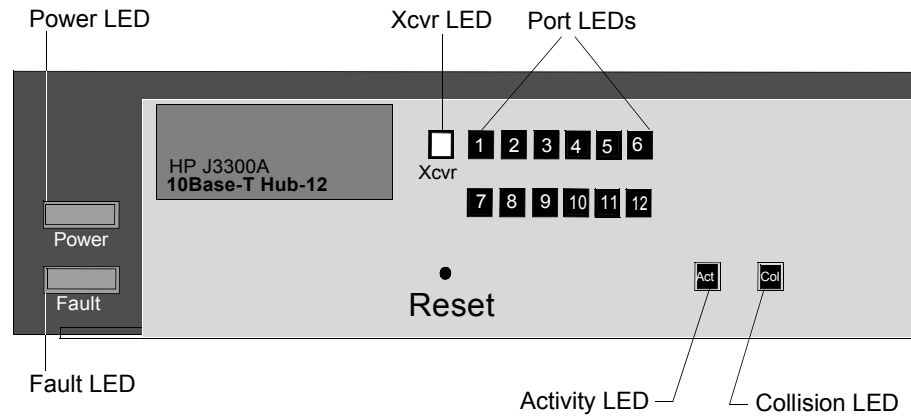


Figure 5-33 J3300A Repeater LEDs

Table 5-23 summarizes the Repeater **Port LED** indications:

Table 5-23. Repeater Port LED Diagnostics

LED Condition	Description	Possible Cause
Off	Link beat signal not being received	- no connection - device at other end of cable is Off - faulty cable
Solid Green	Link beat signal is being received	- proper operating condition
Flashing Green	Port has been automatically partitioned	- excessive collisions

Table 5-24 summarizes the meaning of the Repeater's **other LEDs** signals:

Table 5-24. Other Repeater LED Diagnostics

LED	LED Condition	Description
Power	Off	- no power supplied to Repeater
	On	- power being supplied to Repeater
Fault	Off	- proper operating condition, no fault detected
	On	- internal failure, try to clear by disconnecting and reconnecting power cord
Xcvr	Off	- no transceiver module installed
	On	- transceiver module installed
	Flashing	- Xcvr port has been auto-partitioned
Activity	Off	- no signal packet transmitted to or from a port
	Flashing or On	- signal packets being transmitted to or from a port
Collision	Off	- no collisions detected
	On briefly	- collision detected
	On continuously	- network fault or faulty cable

10 Mbps Media Translator

The **E-TBT-FRL-05** front panel LEDs can be used to monitor Media Translator operation as shown in Table 5-25.

Table 5-25. 10 Mbit/s Media Translator LED Diagnostics

LED	LED Condition	Description
PWR	steady light	ac power supplied to unit, normal operation
	off	- no power to unit - power adapter improperly installed in Media Translator or ac outlet - wrong voltage or frequency supplied to unit
Link (left) (Fiber)	steady light	Fiber cable is connected to the device and an active network component is detected at the other cable end
	off	- Fiber cable improperly connected - TX and RX Fiber cables on Media Translator are connected to the wrong TX and RX ports on the other Media Translator
RX (left) (Receive Fiber)	flashing light	data transmission packets are seen on the Fiber port and an active network component is detected at the other cable end
Link (right) (UTP)	steady light	RJ-45 UTP cable is connected to the device
	off	UTP cable is improperly connected
RX (right) (Receive UTP)	flashing light	data transmission packets are seen on the RJ-45 UTP port

For troubleshooting guidelines for the 10Mbit/s Media Translator, refer to the **User's Guide** that comes with the unit.

The **J2606A Transceiver** of the **10 Mbps Media Translator** contains a single Light Status LED as shown in Figure 5-34.

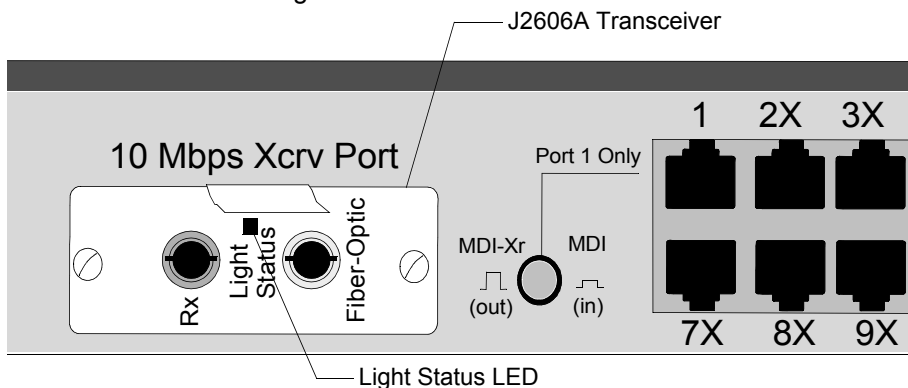


Figure 5-34 J2606A Transceiver LED

Table 5-26 summarizes the Transceiver's **Light Status LED** indications:

Table 5-26. Transceiver Light Status LED Diagnostics

LED Condition	Description	Possible Cause
Off	Link not operational	<ul style="list-style-type: none"> - no connection - faulty cable - inverted Tx/Rx - device at other end of cable not operating properly or is powered Off - internal failure
Solid Green	Link operational	- proper operating condition whether receiving signal or not

100 Mbps Media Translator

The 100 Mbps Media Translator has 5 LEDs on its front panel that indicate Media Translator functionality and data transmission status. These 5 LEDs are shown in Figure 5-35.

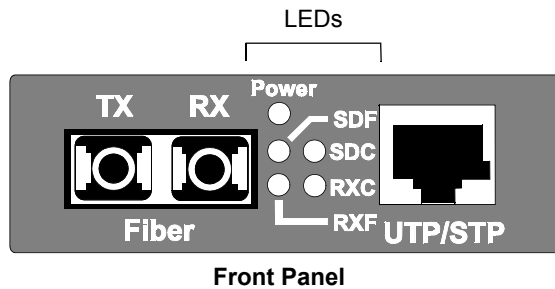


Figure 5-35 100 Mbps Media Translator LEDs

Table 5-27 shows the meaning of the Media Translator's front panel LEDs:

Table 5-27. 100 Mbps Media Translator LED Diagnostics

LED	LED Condition	Description
Power	steady green	ac power supplied to unit, normal operation
	off	<ul style="list-style-type: none"> - no power to unit - power adapter improperly installed in Media Translator or ac outlet - wrong voltage or frequency supplied to unit
SDF (Signal Detect/Fiber) (Link - Fiber)	steady green	Fiber cable is connected to the device and an active network component is detected at the other cable end
	off	<ul style="list-style-type: none"> - Fiber cable improperly connected - TX and RX Fiber cables on Media Translator are connected to the wrong TX and RX ports on the other 100BASE-FX device
RXF (Receive/Fiber) (Activity - Fiber)	flashing green	data transmission packets are seen on the Fiber port and an active network component is detected at the other cable end

Table 5-27. 100 Mbps Media Translator LED Diagnostics

LED	LED Condition	Description
SDC (Signal Detect/Copper) (Link - UTP)	steady green	RJ-45 UTP/STP cable is connected to the device
	off	<ul style="list-style-type: none"> - UTP cable improperly connected - MDI/MDI-X switch in wrong position for this application - power supply is switched to the wrong line voltage
RXC (Receive/Copper) (Activity - UTP)	flashing green	data transmission packets are seen on the RJ-45 UTP/STP port

Repair

Once the problem has been localized to a specific hardware device or software application, causes of the problem can be identified and corrective actions taken.

Philips Hardware

For most Philips system hardware -- processing units, displays, printers, switches, repeaters, media translators -- the **User's Manual** provided with the unit is the primary source of repair information. Refer to the User's Manual for proper troubleshooting, maintenance, and repair procedures for these units.

UPS One exception is troubleshooting and repair of the UPS. The following table gives **Symptoms, Possible Causes, and Corrective Actions** to be followed for problems with the UPS.

Notes

The following table departs slightly from a similar table given in the **APC UPS User's Manual** and should be followed instead of that table.

The most common problems encountered are:

- tripped UPS circuit breaker due to excessive loads. Remove the excess loads and reset the circuit breaker.
- incorrect rear panel switch settings. Switch settings for 120V models are shown in Chapter 2.

Table 5-28. Troubleshooting the UPS

Symptom	Possible Cause	Corrective Action
UPS will not turn on (lamp within power I/O switch is not illuminated), but beeps when power I/O switch is on.	Rear panel circuit breaker is tripped (Circuit breaker is tripped when button is extended.)	Unplug excessive loads and press button to reset breaker.
	Line cord plug is not properly connected	Check line cord plug and engage it properly
	No power at wall socket	Check power at wall socket and establish proper power
UPS operates normally, but SITE WIRING FAULT indicator is illuminated	Building wiring error, such as a missing ground, hot and neutral polarity reversed, or overloaded neutral wiring.	A qualified electrician should be called to correct the building wiring problem. The UPS will not provide rated noise and surge suppression with incorrect building wiring.
	Ground not connected, e.g. "cheater" plug or adapter installed on line cord plug	Plug the UPS into a proper 3 wire grounded outlet only
UPS occasionally emits a beep, but connected equipment operates normally	The UPS is briefly transferring the equipment to its alternate power source due to incoming power spikes or sags	This operation is normal. The UPS is protecting connected equipment from abnormal line voltages. If the audible alarm becomes annoying, set option switch #1 to its up position.

Table 5-28. Troubleshooting the UPS

Symptom	Possible Cause	Corrective Action
UPS emits a beep very often (more than once or twice an hour), but connected equipment operates normally.	Utility voltage is distorted or branch circuits are too heavily loaded.	Have the line power checked by an electrician and corrected if not adequate.
		Operate UPS from an outlet on a different branch fuse or circuit breaker with adequate power.
		Change the transfer voltage of the UPS using option switches #2 and #3 on the rear of the UPS (if the equipment will operate normally for the line power being supplied). See Figure 1-18 or the UPS User's Manual for switch positions for different transfer voltages.
UPS emits loud tone. Power I/O switch is on, but connected equipment is not powered. UPS's rear panel circuit breaker is tripped (button extended). Normal utility voltages are known to be supplied	UPS has shut down due to severe overload.	Turn off the UPS and unplug excessive loads. Laser printers will overload the UPS and should not be connected to the UPS. When overload is removed, press the button to reset the circuit breaker.
UPS emits loud tone during utility failure. Power I/O switch is on, but connected equipment is not powered. Rear panel circuit breaker is not tripped	UPS has shut down due to overload.	Turn off UPS and unplug excessive loads. UPS may be turned on when line power is restored.
UPS does not provide expected run time. Low battery warning is sounded prematurely.	Excessive loads connected to UPS.	Unplug excessive loads from UPS
	Battery is weak due to wear or recent operation during utility power outage.	Recharge battery by leaving UPS plugged in for 12 hours without use. Test control during recharge. If UPS sounds low battery warning prematurely when retested, replace battery or UPS.
UPS beeps continuously. Lamp within I/O power switch is illuminated. Line power has not failed.	Circuit breaker is tripped	Unplug excessive loads and press button to reset circuit breaker.
	Line cord plug is not properly connected	Check line cord plug and engage it properly
UPS does not shut down when RS-232 HI level is applied to computer interface port pin 1.	Signal not applied during line power failure.	UPS responds to this signal only during utility failures (load is operating from the UPS's internal power source).
	Signal is not referenced to the UPS common.	Signal must be referenced to the UPS's common at pins 4 or 9.

Table 5-28. Troubleshooting the UPS

Symptom	Possible Cause	Corrective Action
Low battery warning interval is <i>shorter</i> than 2 or 5 minutes, according to rear panel option switch #4 setting: down = 2 minutes up = 5 minutes	Excessive loads connected to UPS	Excessive loading may shorten run time to less than the 2 or 5 minute low battery warning interval. Remove excessive loads.
	Battery capacity low due to wear or consecutive line power failures	Consecutive line power failures may not allow time for the battery to recharge, thereby causing shortened run time. Recharge as described above.
Low battery warning interval is <i>much longer</i> than 2 or 5 minutes, according to rear panel option switch #4 setting: down = 2 minutes up = 5 minutes	UPS is loaded to less than 10% of rated capacity	This operation is normal. The low battery warning interval is adjusted at the factory for consistent operation at loads above 10% of rated capacity.

If the problem cannot be resolved, note the UPS model, serial number, and date of purchase and contact the UPS Customer Service Department at the phone number given in the **UPS User’s Manual**. While waiting for corrective action, replace the UPS on the Philips system to assure continuous patient monitoring.

UPS Configuration

Philips PCs, including the Server, have been preconfigured for proper UPS operation when shipped from Philips. This section describes the UPS configuration procedure so that configurations can be reset if they are lost. The UPS configuration application can be accessed from the **Windows Main Menu**.

Note

The **UPS** configuration window can also be accessed from the **Control Panel** menu of the **Other Services** menu of Service.

The procedure for opening the **UPS** configuration window from the Windows Main Menu is as follows:

Step 1. Open the **Control Panel** to display the Control Panel menu of icons.

Step 2. Click on the **UPS icon** to open the **UPS** configuration window of Figure 5-36.

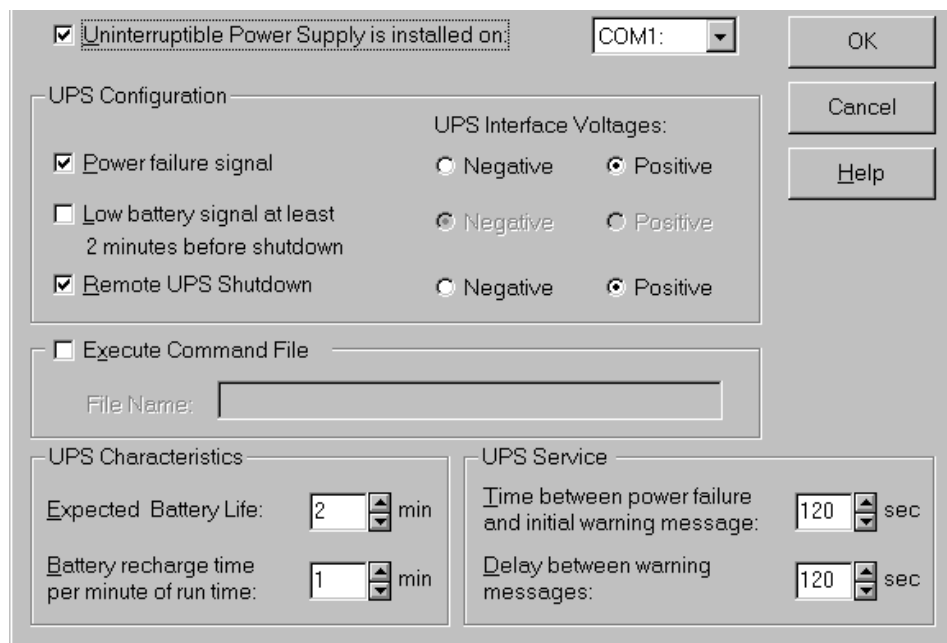


Figure 5-36 UPS Configuration Window

Step 3. Verify (or enter) the following information in the fields of the UPS configuration window.

Uninterruptible Power Supply is installed on: **COM1:**

<p>UPS Configuration</p> <p><input checked="" type="checkbox"/> Power failure signal</p> <p><input type="checkbox"/> Low battery signal at least 2 minutes before shutdown (Disabled)</p> <p><input checked="" type="checkbox"/> Remote UPS Shutdown</p> <p><input type="checkbox"/> Execute Command File (Disabled)</p>	<p>UPS Interface Voltages:</p> <p><input checked="" type="radio"/> Positive</p> <p><input type="radio"/> Negative</p> <p><input checked="" type="radio"/> Positive</p> <p><input type="radio"/> Negative</p> <p><input checked="" type="radio"/> Positive</p> <p><input type="radio"/> Negative</p> <p><input checked="" type="radio"/> Positive</p>
--	--

UPS Characteristics

Expected battery Life: **2 min.**

Battery Recharge time
per minute of run time: **1 min.**

UPS Service

Time between power failure
and initial warning message: **120 sec.**

Delay between warning
messages: **120 sec.**

Step 4. When the UPS Configuration settings have been verified, click **OK** to return to the **Windows Main Menu**.

Restoring Switch Firmware - HP2524

The following procedures describes how to restore firmware on the HP2524 Core/Edge Switch:

- Single Switch Firmware restore
- Switch to Switch Firmware Restore

Materials required for these procedures are the following:

- **Computer** (workstation, server, or laptop) with the following capabilities:
 - Microsoft Operating System software (Windows 2000 or NT)
 - 200 MHz or faster
 - RS 232 serial interface (9-pin D type connector)
 - LAN Cable
 - CD ROM drive
- Information Center Release E.01 Application SW CD ROM
- **9-pin Female to 9-pin Female null modem cable**, (PN RS232-61601, HP PN 5182-4794 or 5184-1894)

Single Switch Firmware restore

Copy the Firmware to the Configuring Computer

The first step is to copy the firmware from the Information Center Release E.01 Application SW CD ROM to the configuring computer.

Note

If the complete **Viridialtools\FirmwareFiles** directory has already been copied from the **Application SW CD ROM** to the configuring computer, the HP2524 firmware may already be stored in the computer’s hard drive and this section can be skipped.

Step 1. Turn on the configuring computer to display the Windows Main Menu.

Step 2. Insert the **Application SW CD ROM** into the CD ROM drive of the configuring PC.

Step 3. Open **Windows Explorer** and find the **Viridialtools** directory on the CD ROM shown in Figure 5-37

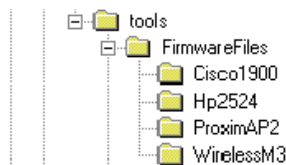


Figure 5-37 tools Directory on the CD ROM

Step 4. Copy the entire **Viridial\tools\FirmwareFiles\Hp2524** directory to the drive to be used for storing this directory on the configuring computer as follows:

- Open the directory to be used on the configuring computer.
- Click on, hold, and drag the **FirmwareFiles\Hp2524** directory to the open directory

Note The **FirmwareFiles\Hp2524** directory file is less than 1.4 Mb so it can be stored on a 1.4 Mb floppy disk for later use or for transfer to a PC without a CD ROM drive.

Run HyperTerminal

When the **FirmwareFiles\Hp2524** directory has been transferred:

Step 1. Close **Windows Explorer** and return to the Windows Main Menu

Step 2. Open the **HyperTerminal** application.

Note If a **Connection Description** window appears, click **Cancel** to close it.

Step 3. Click on **Files->Properties** to open the **New Connection Properties** window and click on the **Connect to** tab to display its menu.

Step 4. Click on the **Connect Using** pull down arrow to display its menu.

Step 5. Click on **COM1** or **Direct to COM1**.

Step 6. Click on **Configure** to display the **COM1 Properties** window.

Step 7. Configure the **COM1** port to the following RS 232 settings:

Bits per second:	19200
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

Step 8. Click **OK** twice to complete the COM1 port configuration.

Step 9. Turn off the switch and disconnect cables from all switch ports.

Step 10. Interconnect the switch and computer using the **RS 232 cable**. One end of the cable connects to the **serial port** on the rear of the computer and the other end connects to the **CONSOLE** port on the front of the HP2524 Switch.

Step 11. Power on the Switch.

It takes about 2 minutes for the switch to reset, during which all port lights turn green.

Install the Firmware

Note When connecting to HyperTerminal at 19200, garbage characters may appear. This is due to the default connection speed of the switch, which is 9600. If the garbage characters appear, press **Enter** until it resets.


Step 1. In the **HyperTerminal Window**, press **Enter** twice, and follow the onscreen directions to display the **Main Menu**. If there is a command prompt, type **Menu** and the **Main Menu** appears.

Step 2. Type **7** (Download OS) after Enter a selection number and **Enter**.

Step 3. Use the Spacebar to select **Xmodem** in the **Method** field.

Step 4. Press **Enter** and then **X** (for eXecute) to begin the download. The following message appears:

Press enter and then initiate Xmodem transfer from the attached computer.....

Step 5. Press **Enter** and then press the Send icon  to open the dialog box. See Figure 5-38

Step 6. In the Filename field, enter the path where the firmware files were copied to in Step 4. The file extension for the HP2524 firmware file is *.swi. Verify the Protocol is set to Xmodem.

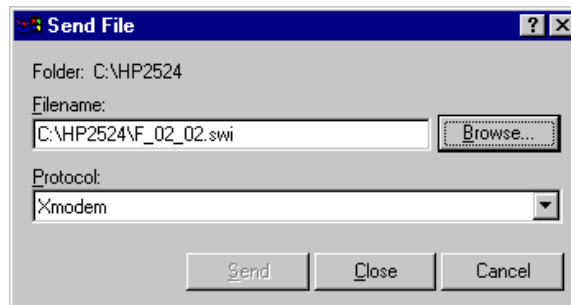


Figure 5-38 HyperTerminal Send Firmware dialog

Note You can use Windows Explorer to browse to find the correct *.swi file. Only one *.swi file should appear.

Step 7. Click **Send** to transfer the *.swi firmware file to the HP2524. The **Xmodem file send** window will appear displaying the progress of the firmware transfer.

Note The file transfer process takes approximately 15 minutes.

When the progress window closes, the **HyperTerminal** window reappears with **Done**.

Step 8. When the firmware installation is complete, the switch automatically reboots.

Step 9. Close the current Hyperterminal session.

Step 10. Open a new Hyperterminal session.

Step 11. Confirm the firmware revision in the welcome screen: F.02.02 or F.02.13

Note If asked for a password, type **m3150**.

- From Main Menu, select:
 - **1. Status and Counters**
 - **1. General System Information**

- Check the **Firmware Revision** line
The switch is now ready for configuration as described in Chapter 4.

Step 12. Close the **HyperTerminal** session.

**Switch to Switch
Firmware Restore**

Switch to Switch firmware restore can be done when at least one HP2524 switch has the supported revision of firmware on it (F.02.02 or F.02.13). This procedure references the HP2524 switch with the correct firmware loaded as the host switch. The switch to be loaded with the firmware is referenced as the secondary switch. The following tasks will be performed:

- Downgrade the host switch to the supported firmware revision (see “Single Switch Firmware restore” on page 5-46)
- Configure the host switch using the Config Tool
- Connect the devices
- Configure the secondary host switch with an IP address
- Transfer the firmware
- Configure the secondary switch using the Config Tool

Note

If problems are encountered during this procedure, refer to “Troubleshooting Tips” on page 5-51.

Step 1. Follow the Xmodem procedure to downgrade the host switch firmware to a supported revision (see “Single Switch Firmware restore” on page 5-46)

Step 2. Using the Config Tool, configure the IP address on the host switch and configure at least one port as auto-negotiate (see “Network Switches” on page 4-11).

Step 3. Make the appropriate connections as shown in Figure 5-39:

- Connect port 24 on the secondary switch to port 24 on the Host switch
- Connect the PC to the console port on the secondary switch using the RS-232 cable. Note: If the secondary switch is straight from the factory, all of the ports are set as Auto-negotiate
- Power cycle the Switches

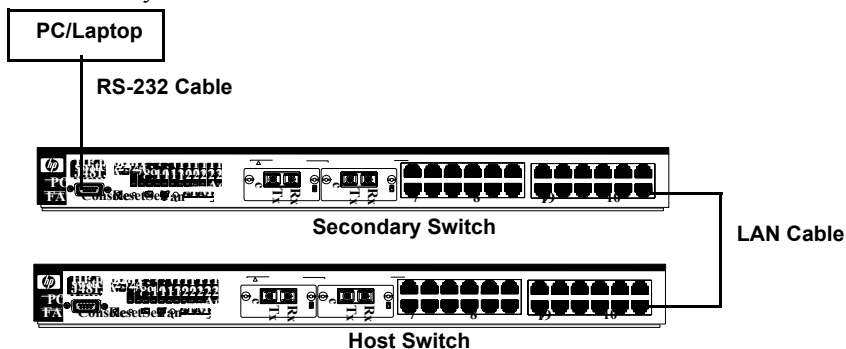


Figure 5-39 Switch to Switch Firmware Setup

Step 4. Open the **HyperTerminal** application.

Note

If a **Connection Description** window appears, click **Cancel** to close it.

Step 5. Click on **Files->Properties** to open the **New Connection Properties** window and click on the **Connect to** tab to display its menu.

Step 6. Click on the **Connect Using** pull down arrow to display its menu.

Step 7. Click on **COM1** or **Direct to COM1**.

Step 8. Click on **Configure** to display the **COM1 Properties** window.

Step 9. Configure the **COM1** port to the following RS 232 settings:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

Step 10. Click **OK** twice to complete the COM1 port configuration.

Step 11. In the **HyperTerminal Window**, press **Enter** twice and follow any onscreen directions to bring you to the Manager Level command prompt (e.g. HP ProCurve Switch 2524#)

Step 12. Type **config** to enter configuration mode

Step 13. Set the IP address on the Secondary switch by entering the following commands at the command line prompt (press Enter after each line):

- **vlan 1 ip address sss.sss.sss.sss/255.255.0.0** (where **sss.sss.sss.sss** is the IP Address of the **secondary** switch)
- **write memory**

Step 14. Type **copy tftp flash hhh.hhh.hhh.hhh flash** where **hhh.hhh.hhh.hhh** is the IP Address of the **Host** switch. See Figure 5-40.

Step 15. Answer **y** at the **Device will be rebooted, do you want to continue?**

- The transfer begins. Text appears stating that Verification and Writing System Software to FLASH. The status information is displayed.

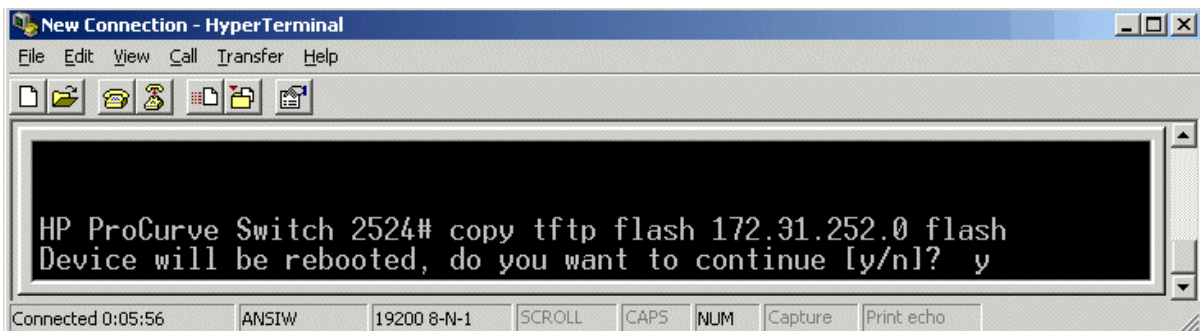


Figure 5-40 Copy tftp flash command

Step 16. The switch reboots. When prompted, press **Enter** twice.

Step 17. Verify the switch firmware revision is either F.02.2 or F.02.13, displayed in the upper left corner of the welcome screen shown in Figure 5-41.

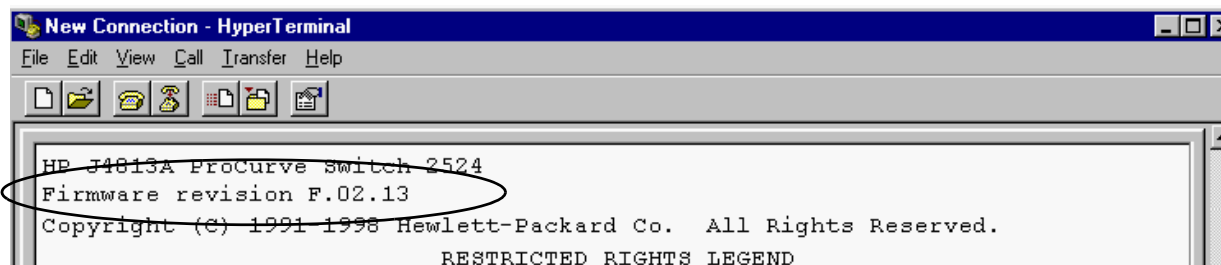


Figure 5-41 Verify Firmware

Step 18. Logout of the switch. To logout, press **Enter**, and then type **Logout** at the command prompt. Type **y** at the confirmation prompt, as shown in Figure 5-42

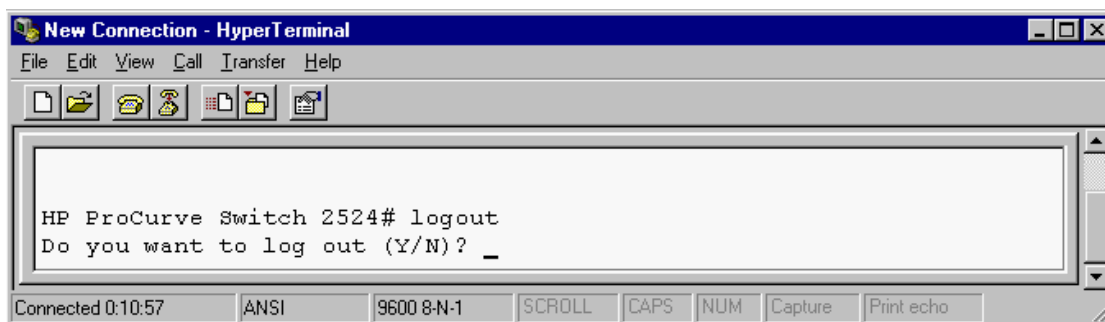


Figure 5-42 Logout

Step 19. Close HyperTerminal.

Step 20. Using the Config Tool, configure the Secondary switch. See “Network Switches” on page 4-11.

Troubleshooting Tips

- COM1 Error - error when executing the Config Tool indicating that something else is using COM1 (see Figure 5-43). Close HyperTerminal or “disconnect” in HyperTerminal (Call->Disconnect) after logging out of the switch



Figure 5-43 COM1 error

- Invalid Input: vlan (see Figure 5-44). You are not in configuration mode, type **config** at the command prompt to enter into configuration mode.

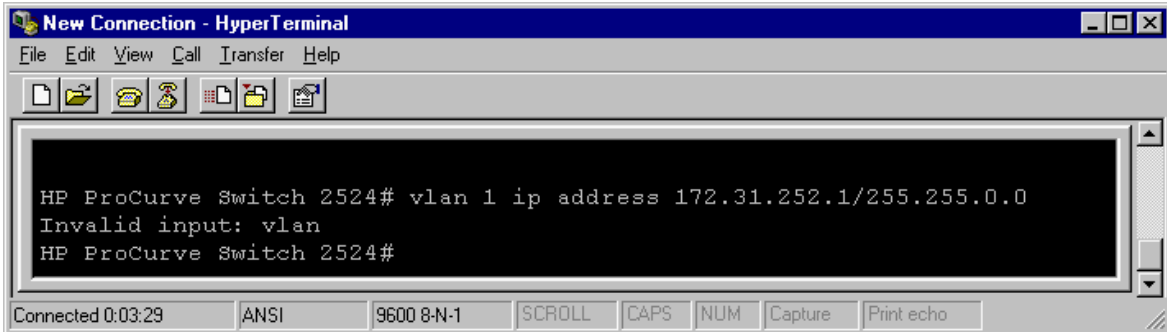


Figure 5-44 Invalid input message

- To return the switch to factory defaults, type **erase startup-config** at the command prompt.

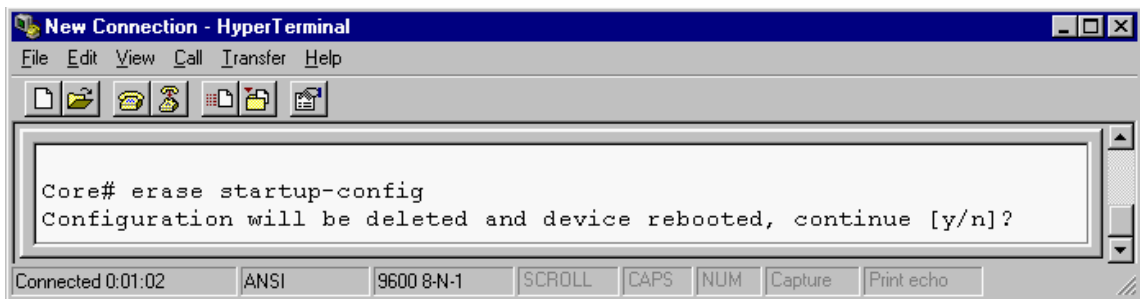


Figure 5-45 startup-config

- If the switch opens in Operator level prompt ">", type **enable** at the command prompt to change to Manager level, as shown in Figure 5-46.

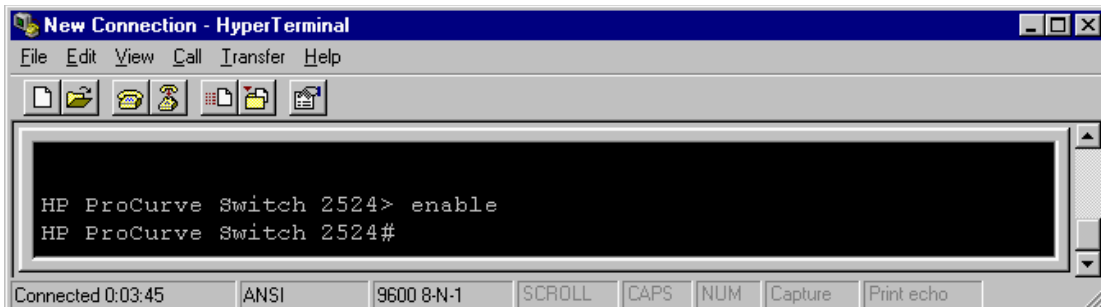


Figure 5-46 Operator level prompt

- **Peer unreachable** - something is wrong with the IP addresses or the LAN cable. The host and the secondary switch both need unique IP addresses, and they must be on the same network. If the switches are connected using auto-negotiate ports, any CAT5 patch cable can be used to interconnect them. If the

switches are connected using ports that have been configured for a specific speed and duplex, then a crossover cable must be used.

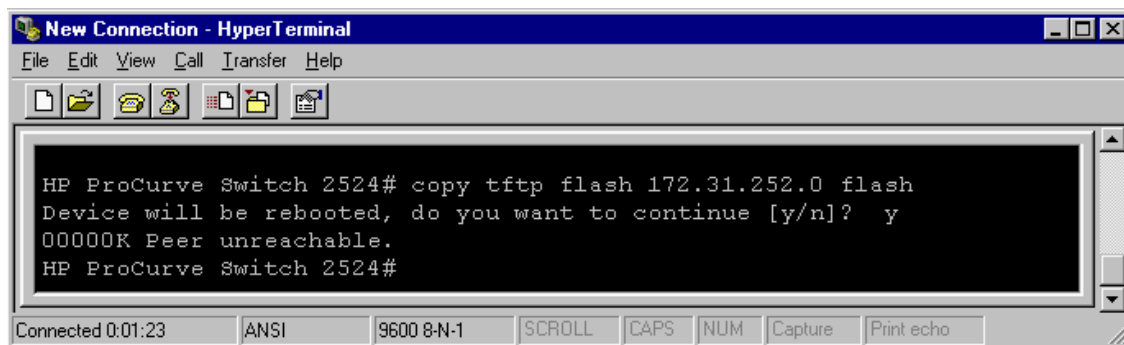


Figure 5-47 Peer unreachable message

Restoring Switch Firmware - Cisco

The following procedures describe how to restore firmware on a Cisco Switch. Firmware restoration may be required if switch firmware is lost or for a new switch.

Materials required for this procedure are the following:

- Computer (workstation, server, or laptop) running Windows 2000 or NT to supply the firmware to the switch
- RS-232 cable, included with the Cisco Switch, for connecting the computer to the switch
- 10Base-T LAN patch cable (direct, not crossover), for connecting the computer to the switch
- **Information Center Network Switch Configuration Utilities** floppy disks (2) (PN M3187-10000), included with Release C M3187-60100 Network Switch orders

The upgrade procedure involves **Installing the Firmware Upload Utility** on the computer and then **Upgrading Switch Firmware** on the switch.

Procedures for **Copying Switch Configuration Tools** to a floppy disk and **Uninstalling Firmware Upload Software** from the computer are also given.

Installing the Firmware Upload Utility

The following procedure describes how to install the Network Switch Firmware Upload Utility on the computer used to install the firmware on the switch.

Step 1. Exit all programs on the computer used to load switch firmware.

Step 2. Place Network Switch Configuration Utilities floppy **Disk 1** in the **A:** drive of the computer.

Step 3. Run **Setup1.bat** as follows:

- click **Start** to open the **Windows** menu
- click **Run** to open the Run window
- select **A:\Setup1.bat** from the Open: field

- click **OK** and Setup1.bat will run

When the reminder Close all other programs before running appears:

Step 4. Press **any keyboard key** and a **C:\WINNT\System32\CMD.exe** window of instructions for running Cisco TFTP Server Setup appears. The instructions on this window are included below.

When the prompt Press any key to continue . . . appears:

Step 5. Press **any keyboard key** and the **Cisco TFTP Server Setup** program will run.

Wait for the Cisco TFTP Server Setup program to run completely. This takes a few minutes during which progress bars appear.

When the **Welcome** window appears in the **Cisco TFTP Server v1.1** window:

Step 6. Click **Next** and the **Choose Destination Location** window appears.

Step 7. If the Destination Folder given is: **C:\...\Cisco Systems\Cisco TFTP Server:**

- click **Next** and the **Select Program Folder** window appears

If any other folder is displayed:

- click the **Browse** button
- click the cursor in the **Path:** field
- edit the **Path:** field to read **C:\Program Files\Cisco Systems\Cisco TFTP Server**
- click **Yes** to the question Create Directory?
- click **OK**
- click **Next** and the **Select Program Folder** window appears

Step 8. Click **Next** in the Select Program Folder window and the **Setup Complete** window appears.

Step 9. Click **Finish** in the Setup Complete window and the MSDOS window reappears.

After a few seconds, a second Press any key to continue . . . prompt appears.

Step 10. Press **any keyboard key** and return to the Windows Main Menu.

Step 11. Remove **Disk 1** from the **A:** drive.

Note

It is not necessary to install Disk 2 to run utility. Disk 2 contains the firmware files. The the firmware files are available on the Information Center Application SW CD.

The Network Switch Firmware Upload Utility is now loaded on the computer and ready for upgrading the switch.

Upgrading Switch Firmware

The following procedure describes how to upgrade switch firmware from the computer.

Step 1. Determine (or set) the **IP address** for the computer. The IP Address can be found as follows:

- open the **Control Panel**

If you are using a Windows NT PC:

- double-click on the **Network** icon to open the **Network** window
- click on the **Protocols** tab to display the **Network Protocols:** field
- select **TCP/IP Protocols** in the Network Protocols: field and click **Properties** to bring up the **Microsoft TCP/IP Properties** window

If you are using a Windows 2000 PC:

- click on the **Network and Dial Up Connections** icon
- right-click on the **Local Area Connection** icon and select **Properties**
- select **Internet Protocols** and click **Properties**
- Select the **IP Address** tab and **Specify an IP address** in the Test Station range (172.31.241.0 to 172.31.241.127) not already in use on the network, e.g. **172.31.241.127**.
- set the **Subnet Mask** to **255.255.0.0**. (A Default Gateway is not required)
 - click **OK** twice and then close the Control Panel window

Step 2. Turn off the switch and disconnect cables from all switch ports.

Step 3. Interconnect the switch and computer using the Cisco-supplied **RS 232 cable**. The **9 pin adapter** end of the cable connects to the **serial port** on the rear of the computer and the **RJ-45** end connects to the **CONSOLE** port on the rear of the Cisco Switch.

Step 4. Interconnect the switch and computer using a **10Base-T LAN cable**. (A standard patch cable can be used, but **do not use a crossover cable**.) One end connects to any **10Base-T port** on the switch and the other end connects to the **LAN interface card** on the rear of the computer.

Step 5. Power on the Cisco Switch.

It takes about 2 minutes for the switch to reset, during which all port lights turn green. After the switch is reset, only the light for the computer LAN cable port will turn green.

Step 6. Start the **Cisco TFTP Server** by double-clicking on its icon in the computer Windows Main Menu or from the Start menu as follows:

- click **Start** to display the **Windows** menu
- click **Programs** to display its menu
- click **Cisco TFTP Server** to start the Cisco TFTP Server. The **Cisco TFTP Server** window appears indicating that it has started.

Caution

DO NOT MINIMIZE OR CLOSE THE Cisco TFTP Server WINDOW!

With the Cisco TFTP Server window open:

Step 7. Open HyperTerminal

Note

If a **Connection Description** window appears, click **Cancel** to close it.

Step 8. Configure the RS232 settings on the COM1 port as follows:

- click **File** in the New Connection - HyperTerminal window to display its menu.
- click **Properties** to open the **New Connection Properties** window.
- click the **Connect To** tab to display its menu.

If **COM1** does not appear in the Connect Using field:

- click the **Connect Using** pull down arrow to display its menu.
- click on (highlight) **COM1**.
- click on **Configure** to display the **COM1 Properties** window.
- configure the **COM1** port to the following **Port Settings**:

```

Bits per second: 9600
Data bits:      8
Parity:         None
Stop bits:      1
Flow control:   None
    
```

Step 9. Click OK and the Catalyst 1900 Management Console window of Figure 5-48 appears. If this window does not open, check the Port Settings on the COM1 port and verify cable connectivity.

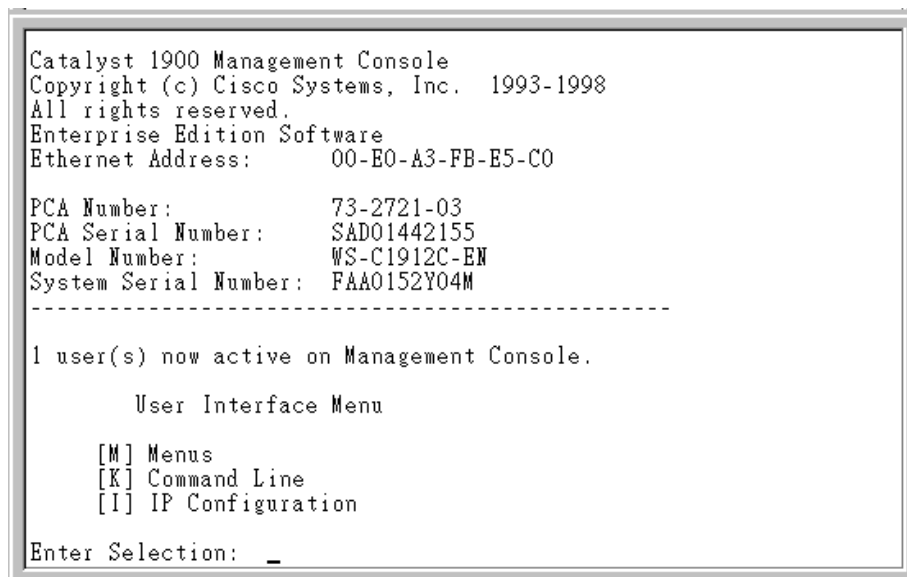


Figure 5-48 Catalyst 1900 Management Console Window

Step 10. Set the **IP Address** and **Subnet Mask** as follows

- type **I** to display the **IP Configuration** menu.
- type **I** to set the **IP address**.
- type the IP address of the switch in the **New Setting** field and press **Enter**.
- verify that the correct IP Address appears in the **IP Address** field.
- type **S** to set the **Subnet Mask**.
- type the default Subnet Mask (**255.255.0.0**) in the **New Setting** field and press **Enter**.
- verify that the correct Subnet Mask appears in the **Subnet Mask** field.

Step 11. Type **X** to return to the **Management Console** window.

Step 12. Type **M** for Menus.

Step 13. Type **F** for Firmware.

Note

The TFTP server address shown under **Settings** should already be set to the IP Address of the computer doing the download and set in Step 1.

If no IP address appears to the right of **TFTP Server name** or **IP Address**, no IP has been set in the utility. You must type **S** to specify the correct IP Address.

The current firmware revision will be displayed in the **System Information** field, e.g. cat80101.bin.

Step 14. If the correct binary firmware file appears in the System Information field, press **Enter**.

If the correct binary firmware file does not appear in the System Information field:

- type **F** to enter the filename of the binary firmware file you wish to use to upgrade the switch.(e.g., cat80101.bin)
-

Note

You can use Windows Explorer to browse the directory **C:\Program Files\Cisco Systems\Cisco TFTP Server** to find the correct *.bin file.

Step 15. Type **T** to request the download and then **Y** and **Enter** to continue with the upgrade process.

Note

It may be useful to arrange both the **Management Console** window and the **TFTP Server** window so that both can be seen during the upgrade.

The download can take as much as a minute. The TFTP Server window will display the progress of the upgrade and then a **Successful** message when the download completes successfully.

Once the switch has determined that it has a proper file, it will program the firmware memory. This will take about a minute, during which the switch **Console** port is inactive.

When the download is complete, the switch resets and returns to the **Management Console** menu. This indicates that the **Switch Firmware Upload** is now finished.

Step 16. Close the **HyperTerminal** session.

Step 17. Close all windows to return to the **Windows Main Menu** and disconnect the cables.

The switch is now ready for configuration as described in **Chapter 4**.

Uninstalling Firmware-Upload Software

The following procedure describes how to uninstall the firmware-upload software from the computer if it is desired to remove these files.

Step 1. Open the **Control Panel** window.

Step 2. Double-click on the **Add/Remove Programs** icon to bring up the **Add/Remove Programs Properties** window.

Step 3. Click on the **Install/Uninstall** tab.

Step 4. Click on (highlight) **Cisco TFTP Server v1.1** in the software list.

Step 5. Click on the **Add/Remove** button.

Step 6. Click **Yes** in the **Continue File Deletion** window to remove the Firmware Upload Software

After the UnInstall shield runs, the message **Uninstall Successfully Completed** appears at the bottom of the window

Step 7. Click **OK**.

Step 8. Close the **Add/Remove Programs Properties** window and the **Control Panel** window

Step 9. Open **Windows Explorer**.

Step 10. Click on (highlight) the **C:\Program Files\Cisco Systems** folder and delete it using the keyboard **Delete** key.

Step 11. Click **Yes** in the **Continue File Deletion** window to remove the **C:\Program Files\Cisco Systems** folder

Step 12. Close the **Windows Explorer** window to return to the **Windows Main Menu**.

Firmware upload software has now been removed from the computer files.

Copying Switch Configuration Tools

The following procedure describes how to copy the Network Switch Configuration Utility from the computer to blank floppy disks if a second set is desired.

Step 1. Label 2 blank 3 1/2 inch floppy disks as **M3187-10000 Disk 1** and **M3187-10000 Disk 2**.

Step 1. Place blank **Disk 1** in the **A:** drive of the Computer.

Step 1. Run **C:\Program Files\Cisco Systems\Cisco TFTP Server\Copy1.bat** as follows:

- click **Start** to open the **Windows** menu
- click **Run** to open the Run window
- select **C:\Program Files\Cisco Systems\Cisco TFTP Server\Copy1.bat** from the Open: field
- click **Open**.

Step 2. Click **OK** in the **Run** window and Copy1.bat will run

Step 3. When the copying is complete, return to the Windows Main Menu.

Step 4. Remove **Disk 1** from the **A:** drive.

Step 5. Repeat **Step 2 - Step 5** with **Disk 2** running **Copy2.bat**.

Restoring Wireless M3/M4 Wireless Adapter Firmware

The following procedure describes how to restore firmware on the Wireless Adapter Board of an M3/M4 patient monitor. Restoration may be required if monitor firmware is lost, corrupted, or not the current revision.

Materials required for this procedure are the following:

- **Computer** (workstation, server, or laptop) with the following capabilities:
 - Microsoft Operating System software (Windows 98 or NT)
 - 200 MHz or faster
 - RS 232 serial interface (9-pin D type connector)
 - CD ROM drive
- **interconnecting cable** (PN M1360-61675) 9-pin D female - 1/8 in. male stereo phono
- **Information Center Release E.01 Application SW CD ROM**

Copy the Firmware to the Configuring Computer

The first step is to copy the firmware from the CD ROM to the configuring computer.

Note

If the complete **tools** directory has already been copied from the **Release E.01 Application SW CD** to the configuring computer, M3/M4 firmware may already be stored in the computer's hard drive and this section can be skipped.

Step 1. Turn on the configuring computer to display the Windows Main Menu.

Step 2. Insert the **Application SW CD** into the CD ROM drive of the configuring PC.

Step 3. Open **Windows Explorer**.

Step 4. Find the **Viridia** directory on the Application SW CD ROM shown in Figure 5-49 and click on it to display the **tools** directory.

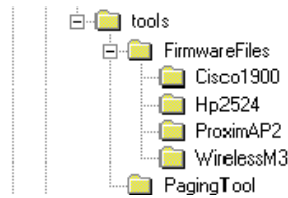


Figure 5-49 tools Directory on the CD ROM

Step 5. Copy the entire **tools\FirmwareFiles\WirelessM3** directory to the drive to be used for storing this directory on the configuring computer as follows:

- Open the directory to be used on the configuring computer.
- Click on, hold, and drag the **tools\FirmwareFiles\WirelessM3** directory to the open directory

Note

The **tools\FirmwareFiles\WirelessM3** directory file is less than 1.4 Mb so it can be stored on a 1.4 Mb floppy disk for later use or for transfer to a PC without a CD ROM drive.

Run HyperTerminal

When the **tools\FirmwareFiles\WirelessM3** directory has been transferred:

Step 1. Close **Windows Explorer** and return to the Windows Main Menu

Step 2. Open **HyperTerminal** to bring up the **New Connection - HyperTerminal** window.

Note

If a **Connection Description** window appears, click **Cancel** to close it.

Step 3. Click on **File** in the New Connection - HyperTerminal window to display its menu.

Step 4. Click on **Properties** to open the **New Connection Properties** window.

Step 5. Click on the **Connect to** tab to display its menu.

Step 6. Click on the **Connect Using** pull down arrow to display its menu.

Step 7. Click on **COM1**.

Step 8. Click on **Configure** to display the **COM1 Properties** window.

Step 9. Configure the **COM1** port to the following RS 232 settings:

Bits per second:	9600
Data bits:	8
Parity:	None

Stop bits: 1
 Flow control: None

Step 10. Click **OK** to complete the COM1 port configuration.

Interconnect the computer and M3/M4 Monitor

When the COM1 port has been configured:

Step 11. Turn **OFF** the Wireless M3/M4 Monitor and disconnect any cable connected to the RJ-45 port on its rear panel.

Step 12. Unsnap the gray cover on the upper right side of the M3/M4 Monitor housing to expose the female stereo phono plug on the Wireless Adapter, as shown in Figure 5-50.



Figure 5-50 Stereo Phono Plug on Wireless Adapter of M3/M4 Monitor

Step 13. Connect the phono plug end of the 9-Pin D female - 1/8 in. male Stereo Phono cable into the phono plug connector on the Wireless Adapter as shown in Figure 5-50 and the 9-pin D end of the cable into the 9-Pin D Serial Port connector on the configuring computer.

Step 14. Turn **ON** the M3/M4 Monitor and insure that it passes its self-test.

Install the Firmware

When the M3/M4 Monitor has passed its self-test:

Step 15. Put the M3/M4 Monitor in Service mode. The password is **32441**.

Step 16. Press the keyboard **Enter** key and the **2.4 GHz ETHERNET ADAPTER MAIN MENU** of Figure 5-51 will appear.

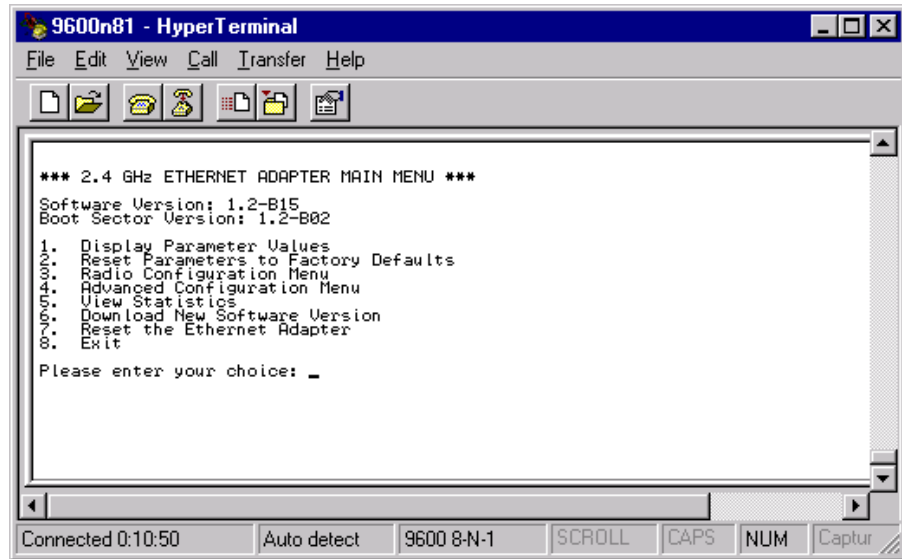


Figure 5-51 2.4 GHz ETHERNET ADAPTER MAIN MENU

Step 17. Type **6** (Down load New Software Version) after Please enter your choice: and **Enter** to display the download a new software version information shown in Figure 5-52.

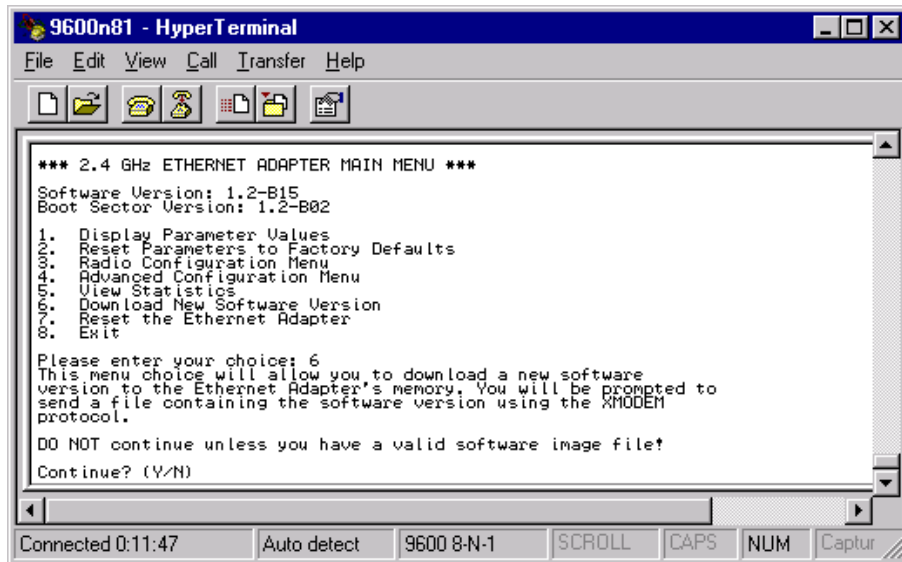


Figure 5-52 Download New Software Information

Step 18. Type **Y** to initiate Start Binary File Transfer. See Figure 5-53.

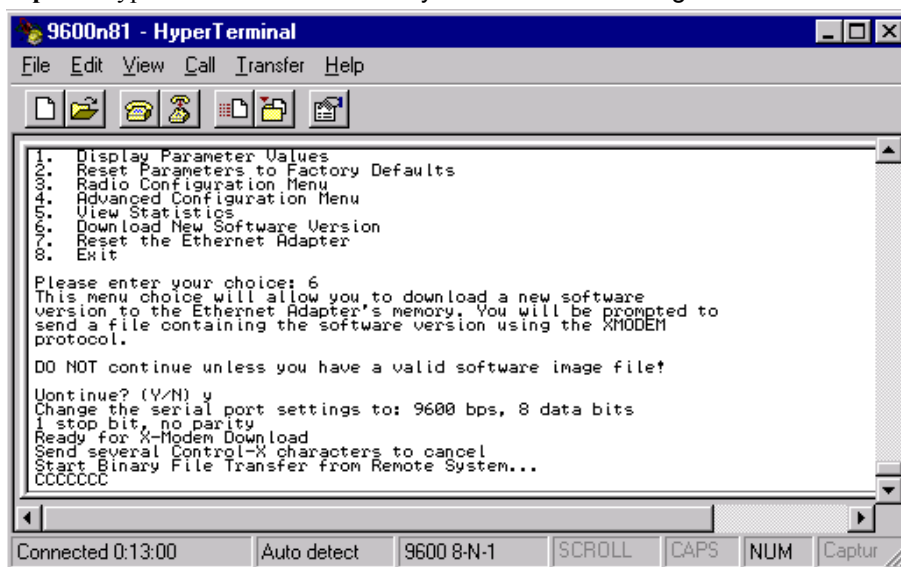


Figure 5-53 Start Binary File Transfer Information

The M3/M4 monitor will send the ASCII character **C** as a prompt to initiate the transfer. When the **Cs** appear:

For computers running Windows NT:

Step 19. Click **Transfer** in the upper row menu of the HyperTerminal window to display the **Send File** window of Figure 5-54.

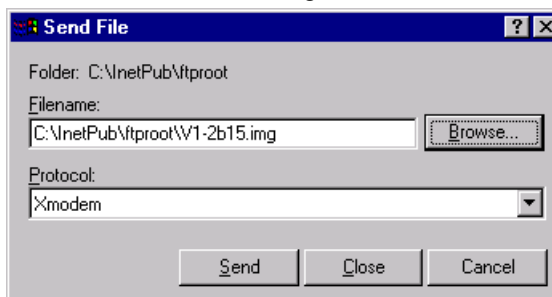


Figure 5-54 HyperTerminal Send File Window

Step 20. Find the file ***.img** in the directory it was transferred to and click on it to display it in the **Filename** field.

Note

The **Browse** button can be used to display the file directories on the computer's drives to locate this file.

Step 21. Select **Xmodem** in the **Protocol:** field. Use the arrow to the right of the field to display the Protocol: options.

Step 22. Click **Send** to transfer the *.img firmware file to the M3/M4 Wireless Adapter. The **Xmodem file send** window of Figure 5-55 will appear displaying the progress of the firmware transfer.

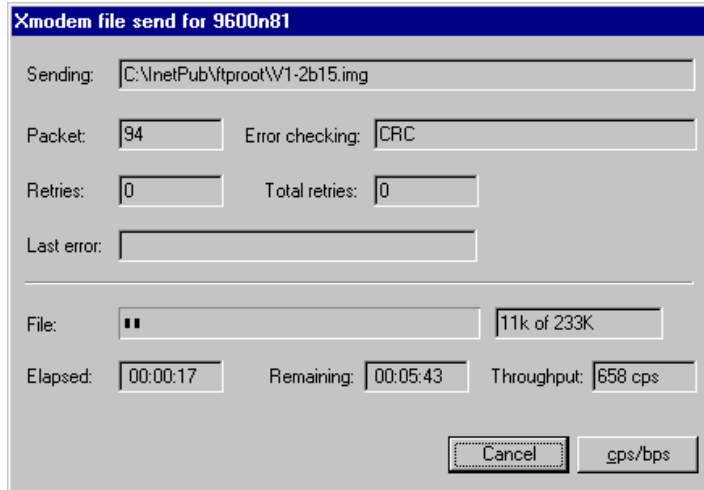


Figure 5-55 Xmodem file send Window

When the progress window closes, the **HyperTerminal** window reappears with **Done** following the **C** sequence, as shown in Figure 5-56.

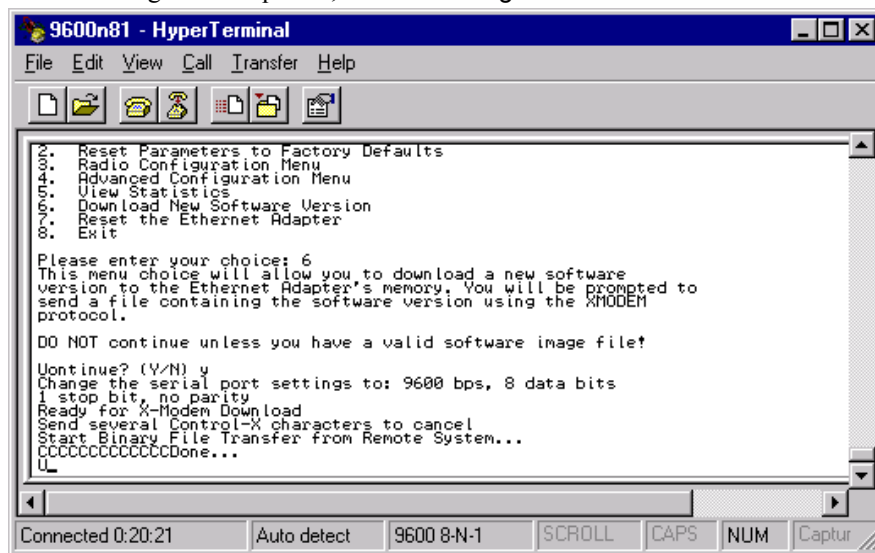


Figure 5-56 HyperTerminal Done Window

Step 23. Press **Enter** and verify that the software Version is **1-2b15**.

Step 24. Press **8** (Exit) to exit.

The M3/M4 monitor will then reboot. After the reboot:

Step 25. Turn **OFF** the M3/M4 monitor, remove the phono plug, and replace the Wireless Adapter cover.

Step 26. Click **X** in the upper right of the **HyperTerminal** window to close it.

Note

After the firmware on the Wireless M3/M4 monitor has been restored, it **must be reconfigured**. See the **Device Configuration** in **Chapter 4**.

**Restoring Access
Point Firmware**

The following procedure describes how to restore firmware on an Access Point. Restoration may be required if Access Point firmware is lost or if it is possible that it is not the current revision.

Materials required for this procedure are the same as for the previous procedure for **Restoring Wireless M3/M4 Monitor Firmware** except that the following cable is required:

- **Serial cable** (PN RS232-61601, or HP PN 5182-4794)

Copy the Firmware to the Configuring Computer

The first step is to copy the firmware from the Application SW CD to the configuring computer.

Note

If the complete **tools\FirmwareFiles\ProximAP2** directory has already been copied from the **Release E.01 Application SW CD ROM** to the configuring computer, M3/M4 firmware may already be stored in the computer's hard drive and this section can be skipped. See **Device Configuration** in **Chapter 4**.

Step 1. Follow the procedure to **Copy the Firmware to the Configuring Computer** described in the previous section for **Restoring Wireless M3/M4 Monitor Firmware**.

Run HyperTerminal


When the **tools** directory has been transferred, the **HyperTerminal** application should be run on the configuring computer.

Step 2. Follow the procedure to **Run HyperTerminal** described in the previous section for **Restoring Wireless M3/M4 Monitor Firmware**.

Interconnect the computer and M3/M4 Monitor

When the COM1 port has been configured:

Step 3. Connect one end of the 9-Pin D Female - 9-Pin D Female cable to the 9-pin D Male Serial Port connector on the configuring computer and the other end to the **Serial** port on the rear panel of the Access Point to be configured. See Figure 5-57.

Step 4. Turn on the Access Point and insure that it passes its self-test by waiting for the Status LED  on the Access Point top to turn green.

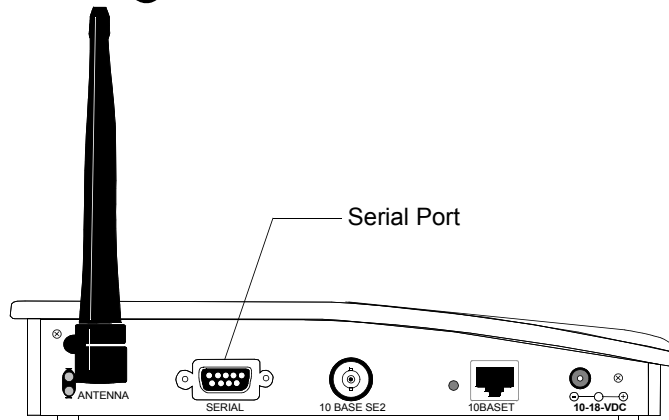


Figure 5-57 Rear Panel of Access Point

Install the Firmware

Step 5. Press **Enter** and the **Main Menu** of Figure 5-58 will appear.

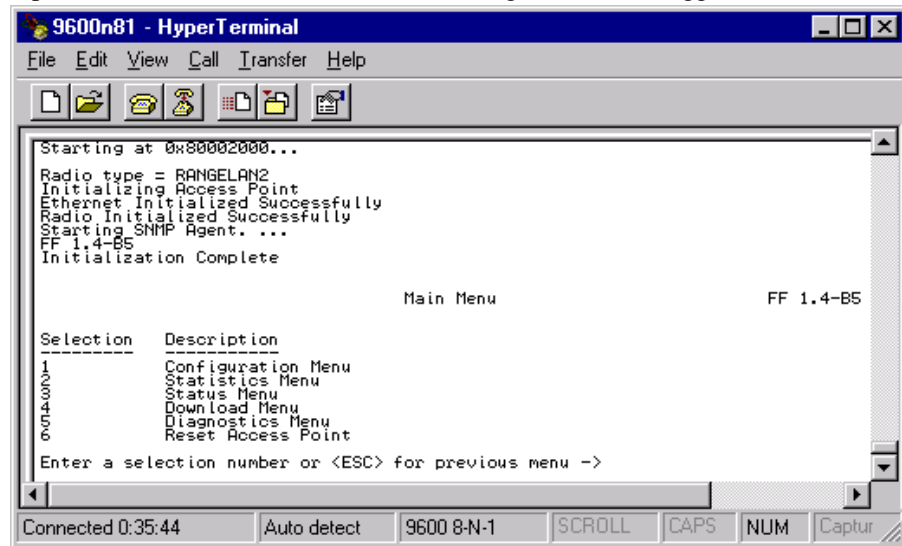


Figure 5-58 Access Point Main Menu

Step 6. Type **4** (Down load Menu) after Enter a selection number and **Enter** to display the Down Load Menu shown in Figure 5-59.

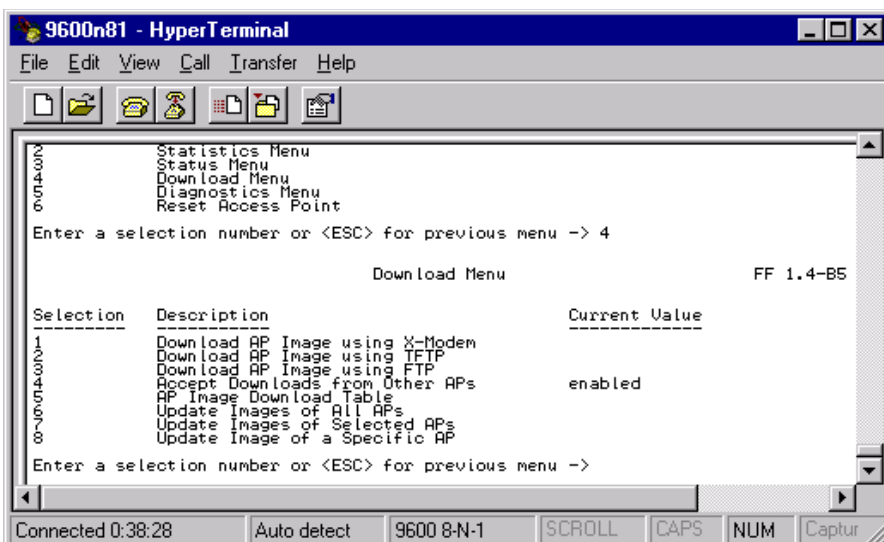


Figure 5-59 Down Load Menu

Step 7. Type **1** (Down load AP Image using X-Modem) after Enter a selection number and **Enter** to Start Binary File Transfer. See Figure 5-60.

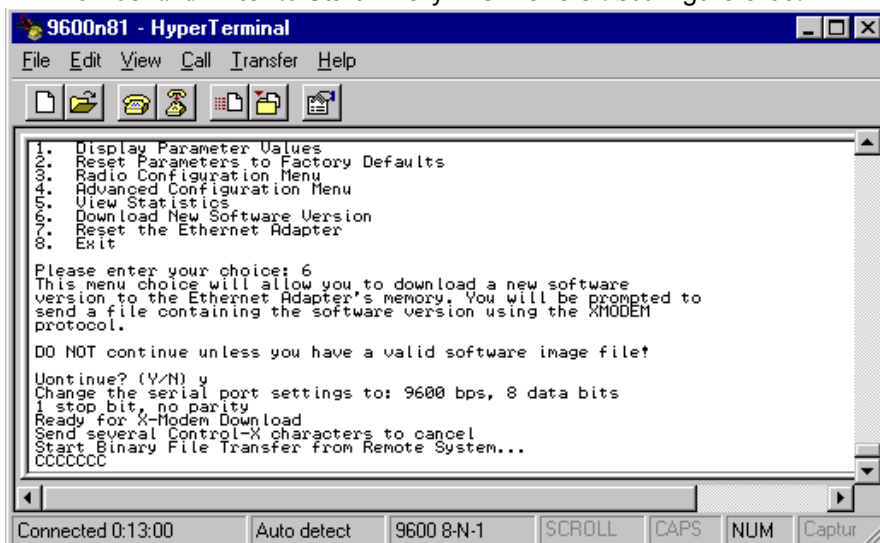


Figure 5-60 Start Binary File Transfer Information

The Access Point will send the ASCII character **C** as a prompt to initiate the transfer. When the **Cs** appear:

For computers running Windows NT:

Step 8. Click **Transfer** in the upper row menu of the HyperTerminal window to display the **Send File** window of Figure 5-61.

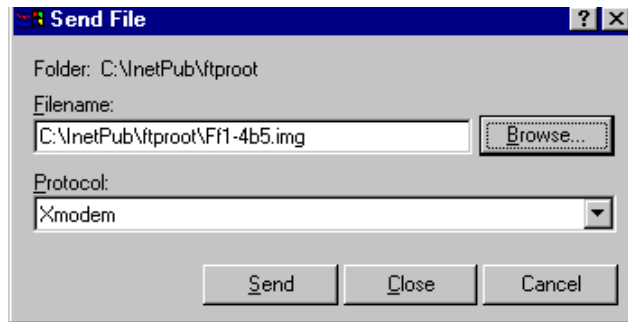


Figure 5-61 HyperTerminal Send File Window

Step 9. Find the file *.img in the directory it was copied to and click on it to display it in the **Filename:** field.

Note The **Browse** button can be used to display the file directories on the computer's drives and locate this file.

Step 10. Select **Xmodem** in the **Protocol:** field. Use the arrow to the right of the field to display the Protocol: options.

Step 11. Click **Send** to transfer the *.img firmware file to the Access Point. The **Xmodem file send** window of Figure 5-62 will appear displaying the progress of the firmware transfer.

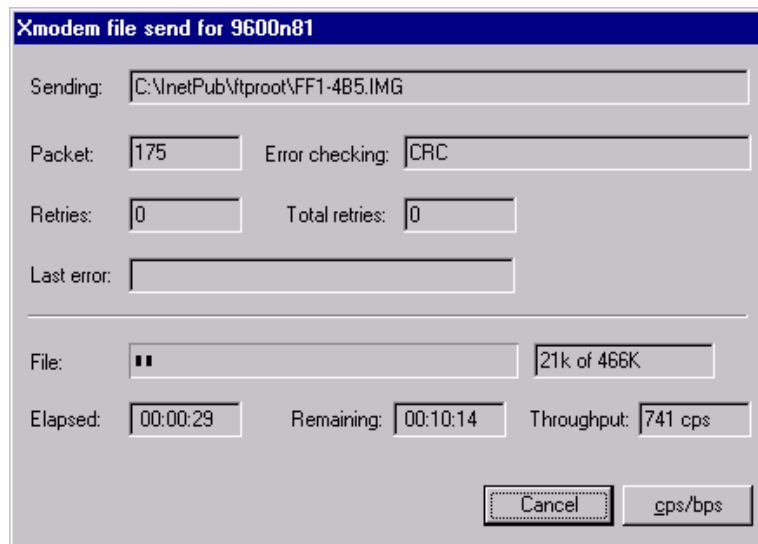


Figure 5-62 Xmodem file send Window

Note The file transfer process takes about 10 minutes.

When the progress window closes, the **HyperTerminal** window reappears with **Done** following the **C** sequence, and **Down load Successful -- Resetting AP**, as shown in Figure 5-63.

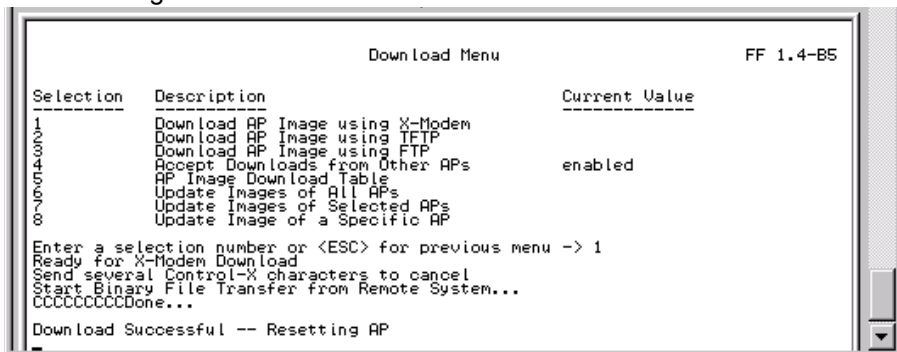


Figure 5-63 HyperTerminal Done Window

The Access Point will load the flash memory with the new firmware and then reboot. This takes a couple of minutes. After reboot, the Access Point will uncompress the Flash Image file. This takes a few minutes during which the **Access Point Boot ROM** information shown in Figure 5-64 is displayed.

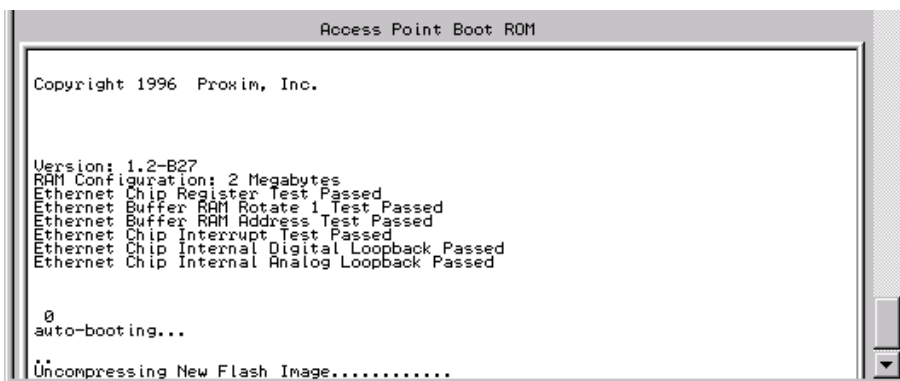


Figure 5-64 Access Point Boot ROM Information

When the uncompression of the New Flash Image is complete, the HyperTerminal window of Figure 5-65 displays the message **Initialization Complete**.

```
Version: 1.2-B27
RAM Configuration: 2 Megabytes
Ethernet Chip Register Test Passed

Ethernet Buffer RAM Rotate 1 Test Passed
Ethernet Buffer RAM Address Test Passed
Ethernet Chip Interrupt Test Passed
Ethernet Chip Internal Digital Loopback Passed
Ethernet Chip Internal Analog Loopback Passed

0
auto-booting...

Uncompressing New Flash Image..... done
1067286 + 348320
Starting at 0x00002000...

Radio type = RANGELAN2
Initializing Access Point
Ethernet Initialized Successfully
Radio Initialized Successfully
Starting SNMP Agent. ...
FF 1.4-B5
Initialization Complete
```

Figure 5-65 HyperTerminal Initialization Complete Window

- Step 12.** Press **Enter** to return to the Main Menu, where the firmware revision should appear on the right.
- Step 13.** Turn **OFF** the Access Point and remove the cable.
- Step 14.** Click the **X** in the upper right of the **HyperTerminal** window to close it.

Note

After access point firmware has been restored, its configuration settings should be verified to make certain that they have not changed. If they have changed, it must be reconfigured. See the **Device Configuration** in **Chapter 4**.

Replaceable Parts

Replaceable Parts for the Application Server, Information Center, Client, and Database Servers can be ordered from the **Philips Support Materials Organization**. A complete list of orderable replaceable parts is given in the **Replaceable Parts List**. Also provided is the address and telephone number of Sales and Support Offices.

The components, options and accessories for Philips systems are given in **Chapter 1, Components and Options**. These can also be ordered from the **Support Materials Organization**.

Troubleshooting

Testing Product Assurance

Testing Product Assurance

Before using the Information Center system clinically with patients, proper performance of the system should be verified. This section includes a series of **Product Assurance Tests** that should be performed after system installation and any system repair or upgrade to verify system functionality.

Notes

These validation tests do not check all system specifications but are intended to verify performance of the primary features of Information Center functionality. However, successful completion of the performance tests should yield a fully functioning system.

When performing product assurance tests, Information Centers must be connected to the SDN or Clinical Network.

Visual Tests

Prior to using the Philips system with patients, all system components, cables, and connectors should be thoroughly visually inspected.

System Components

Step 1. Check all components of the Information Center system for signs of mechanical damage.

If damage to a component is found, assess the damage to determine if repair or replacement is required. Repair or replace the component as required before continuing the Product Assurance Tests.

Cables

Step 2. Check all cables of the Information Center system for signs of abrasion, wear, or other damage.

If any cable shows evidence of damage, repair or replace the cable prior to using the Information Center system for patient monitoring.

Connectors

Step 3. Check all cable connectors for signs of mechanical damage and each cable connection for connection integrity.

If any cable connector shows signs of damage, replace the cable prior to using the Information Center system for patient monitoring.

Step 4. Check that all cable connectors are securely fastened to the rear of each device.

Test and Inspection Procedures

This section is intended for **Philips Cardiac and Monitoring Systems Service Providers**. It documents requirements for test, inspection, and reporting of results for Information Center systems to help assure safe and reliable operation.

Note The tests and inspections in these tables *must be followed by Philips Service Providers* when the Philips system is installed and after any service event.

Table 6-29 describes which tests should be performed for Philips system components -- Information Centers, Clients, Database Servers, Clinical Network components -- for each type of service event.

Table 6-29. M3185 Test and Inspection Requirements

Service Event When performing....	Test Block(s) RequiredComplete these tests
Installation	Visual, Power On, Performance
Preventive Maintenance	Power On
Any component repair or replacement	Power On, Performance
Hardware Upgrade	Power On, Performance
Software Upgrade	Power On, Performance
All other Service Events	Visual, Power On, Performance

Clinical Network Table 6-30 describes the test or inspection to perform for active M3185 Clinical Network components for each type of test specified in Table 6-29.

Table 6-30. M3185 Clinical Network Components - Test and Inspection Matrix

Test Block Name	Test or Inspection to Perform	Expected Results	What to Record on Service Record
Visual	Inspect all system components for obvious damage.	No visible damage	V:P or V:F where P = Pass F = Fail
Power On:	<p>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. Following are normal conditions for each type of device:</p> <p>862084/J4813A HP2524 24 Port Switches: After self test, the Power LED and Fan LED are solid green The LINK LED for each port that has a cable connected is green.</p> <p>Cisco 24 Port Switches: After self test, the System Status LED is solid green and all of the Port Status LEDs are Off (nothing is connected to the front panel.)</p> <p>J3300A Repeater Hubs: After self test, the Power LED is solid green and the Port and Fault LEDs are Off (nothing is connected to the front panel). If a J2606A Transceiver is installed, the Xcvt LED is On. If it is not installed, it is Off.</p> <p>M3188A (862089/M3185A-#C11) 100 Mbit/s UTP/Fiber Media Translator: With power on, the Power LED is solid green. The SDF, SDC, RXC, and RXF LEDs may flash if data activity is present.</p> <p>J4097A HP408 Extension Switch: After self test, the Power LED is solid green</p> <p>862085/AT-FS708 Allied Telesyn Extension Switch: After self test, the Power LED is solid green</p> <p>862105/M3171 Access Point Controller The Power LED is solid green</p> <p>862093/M3173 Remote Power System The AC LED is solid green</p> <p>M3189A (M3185A-#C21) Wireless Access Point: After self test (~ 30 s), system Status LED (uppermost LED on the top panel) is solid green. Other LEDs may be on or off depending on whether data activity is present</p>	Devices power up into expected status; no error indications are shown.	PO:P or PO:F where P = Pass F = Fail

Table 6-30. M3185 Clinical Network Components - Test and Inspection Matrix

Test Block Name	Test or Inspection to Perform	Expected Results	What to Record on Service Record
Performance:	<p>Perform an operational test of the Clinical Network by executing a data passing operation from each connected Information Center to every other Information Center, Client, or Printer on the Network</p> <p>For each M3155 Information Center: Verify that a review application (e.g. Wave Review) can be executed. This verifies connection to the Database Server.</p> <p>For each M3151 Client: Verify that waveforms from every M3155 Information Center on the Network having a connection to an SDN can be viewed on the Client.</p> <p>Verify that a review application (e.g. Wave Review) can be executed. This verifies connection to the Database Server</p> <p>For each wireless Patient Monitor: Verify that waveforms from each wireless patient monitor on the network are displayed on an Information Center and that the waveforms are continuous.</p>	<p>Expected answers are “Yes”. If so, Performance test passed.</p>	<p>P:P or P:F where P = Pass F = Fail</p>
Safety	<p>No safety test is required</p>		<p>S:NA where NA = Not required</p>

A

Worksheets

Overview

This appendix provides a set of worksheets that can assist in the design, installation, and configuration of Clinical Network systems. Included in this section are worksheets for the following:

Network Installation

page A-2

Notes

It is recommend that these worksheets be completed **before** beginning each associated task.

These worksheets can serve as templates that can be photo copied so that a blank copy remains available for future use.

Copies of completed worksheets should be retained as a record of the information that was used.

Network Installation

The following worksheet can be used to record names, IP Addresses, and locations of devices on the Clinical Network.

Table A-1. Network Device Names and Addresses

Device Model	Host Name	Device Name	Location	Tier	IP Address	Subnet Mask
Core Switch					172.31.252.0	255.255.0.0
Edge					172.31.252.1	255.255.0.0
Edge Switch					172.31.252.2	255.255.0.0
Edge Switch					172.31.252.3	255.255.0.0
Edge Switch					172.31.252.4	255.255.0.0
Edge Switch					172.31.252.5	255.255.0.0
Edge Switch					172.31.252.6	255.255.0.0
Edge Switch					172.31.252.7	255.255.0.0
Edge Switch					172.31.252.8	255.255.0.0
Edge Switch					172.31.252.9	255.255.0.0
Edge Switch					172.31.252.10	255.255.0.0
Edge Switch					172.31.252.11	255.255.0.0
Edge Switch					172.31.252.12	255.255.0.0

Table A-2. Network Printer Addresses and Assignments

Printer Name	Location	Info Center Device Names (using this Printer)	Client Device Names (using this Printer)	Hardware Address (from Printer Configuration Page)	IP Address
					172.31.254.1
					172.31.254.2
					172.31.254.3
					172.31.254.4
					172.31.254.5
					172.31.254.6
					172.31.254.7
					172.31.254.8

Table A-6. Harmony Access Point Controller Configuration Attributes

Master and Device Name	Location	Security ID	Channel (0 - 15)	Domain (0 - 15)	IP Address
		m3150			172.31.238.0
		m3150			172.31.238.1
		m3150			172.31.238.2
		m3150			172.31.238.3
		m3150			172.31.238.4
		m3150			172.31.238.5
		m3150			172.31.238.6
		m3150			172.31.238.7
		m3150			172.31.238.8
		m3150			172.31.238.9

Table A-7. Harmony Access Point Configuration Attributes

Master and Device Name	Location	Security ID	Channel (0 - 15)	Domain (0 - 15)	IP Address
		m3150			172.31.236.0
		m3150			172.31.236.1
		m3150			172.31.236.2
		m3150			172.31.236.3
		m3150			172.31.236.4
		m3150			172.31.236.5
		m3150			172.31.236.6
		m3150			172.31.236.7
		m3150			172.31.236.8
		m3150			172.31.236.9
		m3150			172.31.236.10
		m3150			172.31.236.11
		m3150			172.31.236.12
		m3150			172.31.236.13
		m3150			172.31.236.14
		m3150			172.31.236.15

Network Installation

Remote Clients on T1 Lines

Overview

Release E.01 supports the connection of Information Center Clients for remote monitoring over a T1/E1 line. This appendix provides information regarding this connection.

T1 is defined as a dedicated phone connection that supports data rate of 1.544 Mbits per second. T1 lines consist of 24 individual channels, each of which supports 64Kbits per second. Each 64Kbit channel can be configured to carry voice or data traffic. The E1 line is the European format for digital transmission, similar to the T1 line. E1 carries signals at 2 Mbits (32 channels at 64 Kbps). Each Client requires 512Kbps of bandwidth (8, 64 Kbps channels).

The following rules apply:

- The local router must connect to the Core Switch
- The routers must be configured to run frame relay over the T1/E1 line at a minimum bandwidth of 512k (8 channels) per client
- The routers must be configured with static routes
- The routers must be configured to forward UDP broadcasts using ports 67, 68, 137, 138, and 24006.
- The local router needs to forward UDP broadcasts to the remote Clients¹
- The remote router needs to forward UDP broadcasts to the Database Server and to each Information Center that the remote Client will be displaying data from²
- A maximum of 3 Clients per Clinical Network can be connected in this manner using a single T1/E1 line
- The Default Gateway for all connected Information Centers and Database Servers must be the IP address of the local router (i.e. Monitoring LAN)
- Remote Clients connect directly to the router at the remote site or to a switch that is then connected to the remote router
- A different T1/E1 line must be used for each Clinical Network
- A different remote switch must be used for each Clinical Network
- The Application Server portal is not supported on remote Clients. Disable the Web Access portal selection in the Config Wizard, General Configuration page. (Refer to the IntelliVue Information Center System Installation and Service Manual, Chapter 6 for details.)
- Connect the remote Client to a Core switch and verify proper connectivity and operation. Move the remote Client to the remote site, and make the appropriate connections as defined in “System Diagrams” on page B-2, if there is a connectivity or operational problem at that time, it is the remote connection that is the issue.

1. If using a Cisco or HP router, use the **ip-helper-address** command for this

2. If using a Cisco or HP router, use the **ip-helper-address** command for this

System Diagrams

Note Philips Medical Systems does not sell a router to implement this feature. Routers are the responsibility of the hospital.

The following diagrams illustrate how this feature can be implemented, following the rules given above. IP Addresses (IP), Subnet Masks (SM), and Default Gateways (DG) are shown. To configure the IP Addresses, Subnet Masks, and Default Gateways, see “Changing Network Properties” on page B-4.

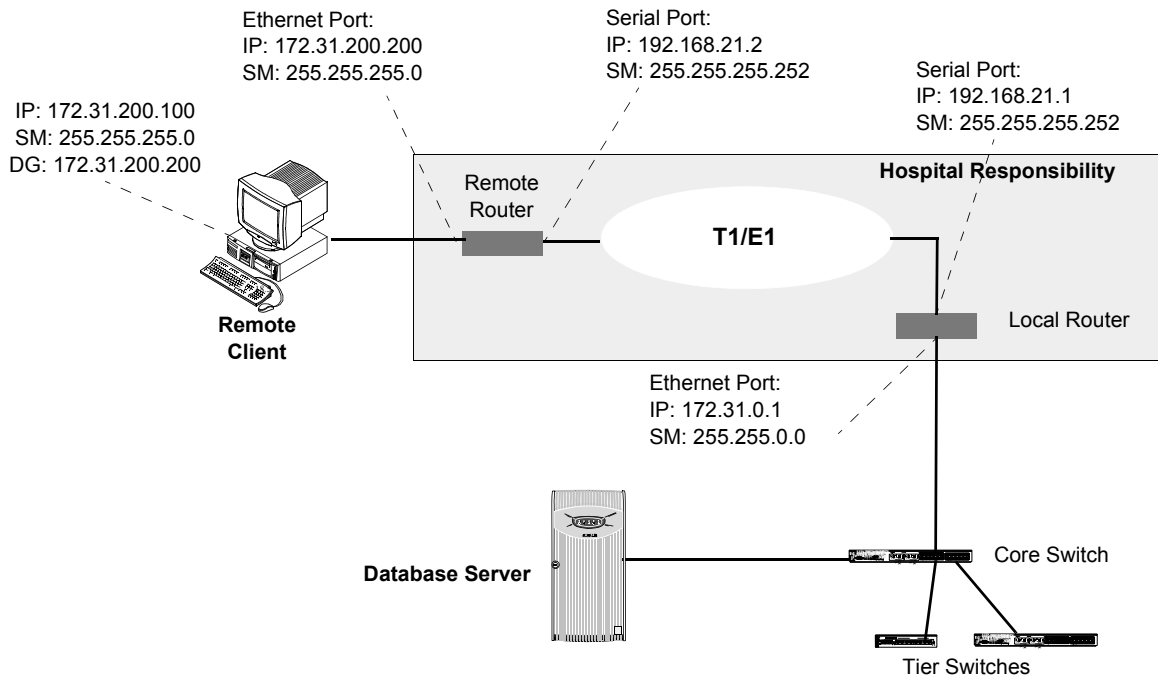


Figure B-1 Single Client Connection on T1/E1 Line

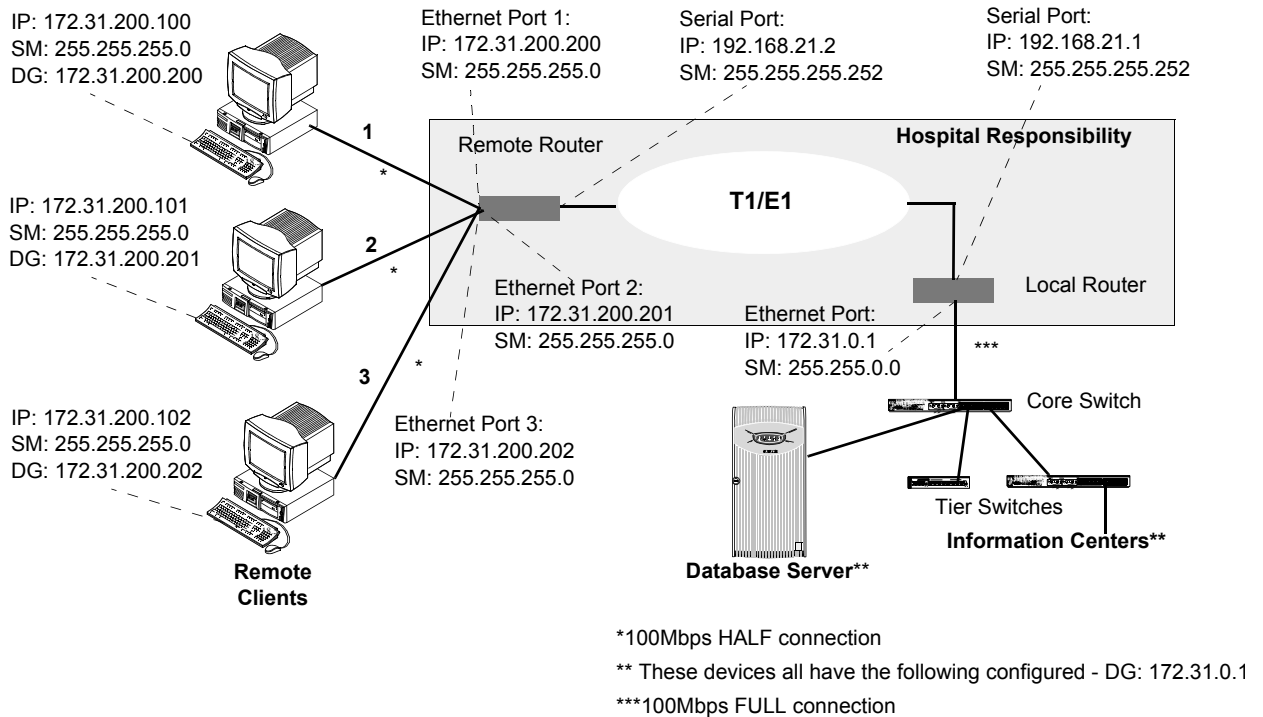


Figure B-2 3 Remote Clients Connected on single T1/E1 Line

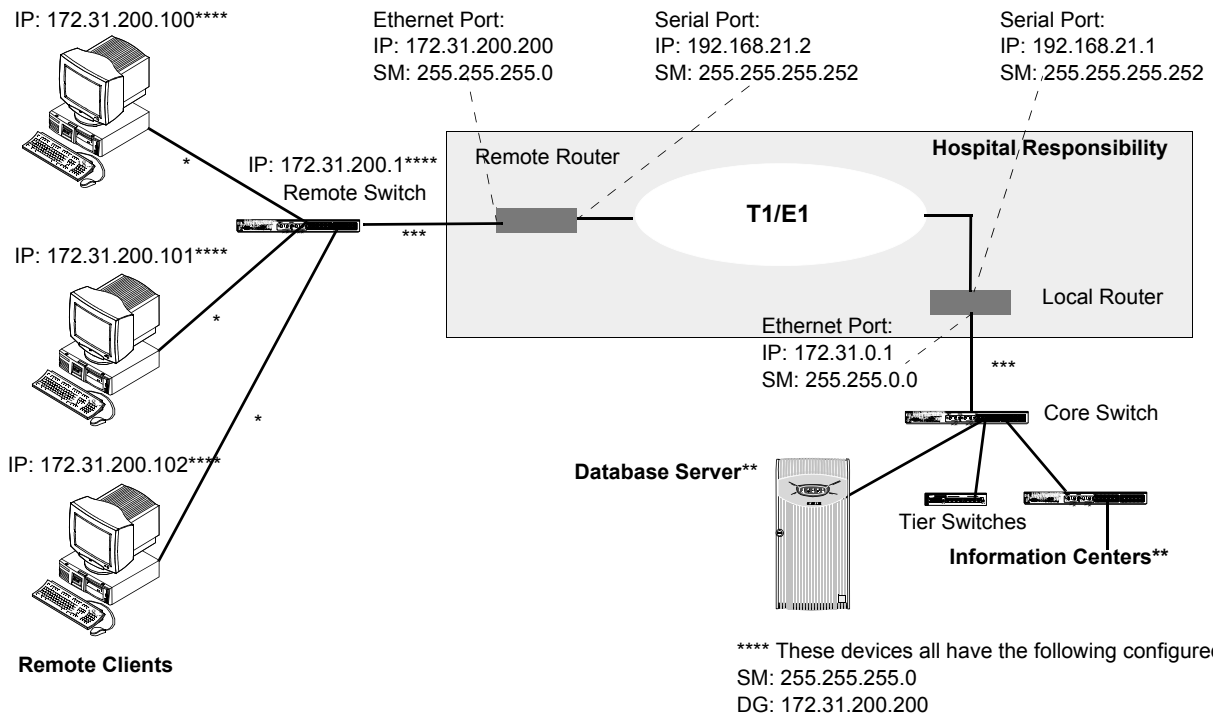


Figure B-3 3 Remote Clients connected to a switch on single T1/E1 Line

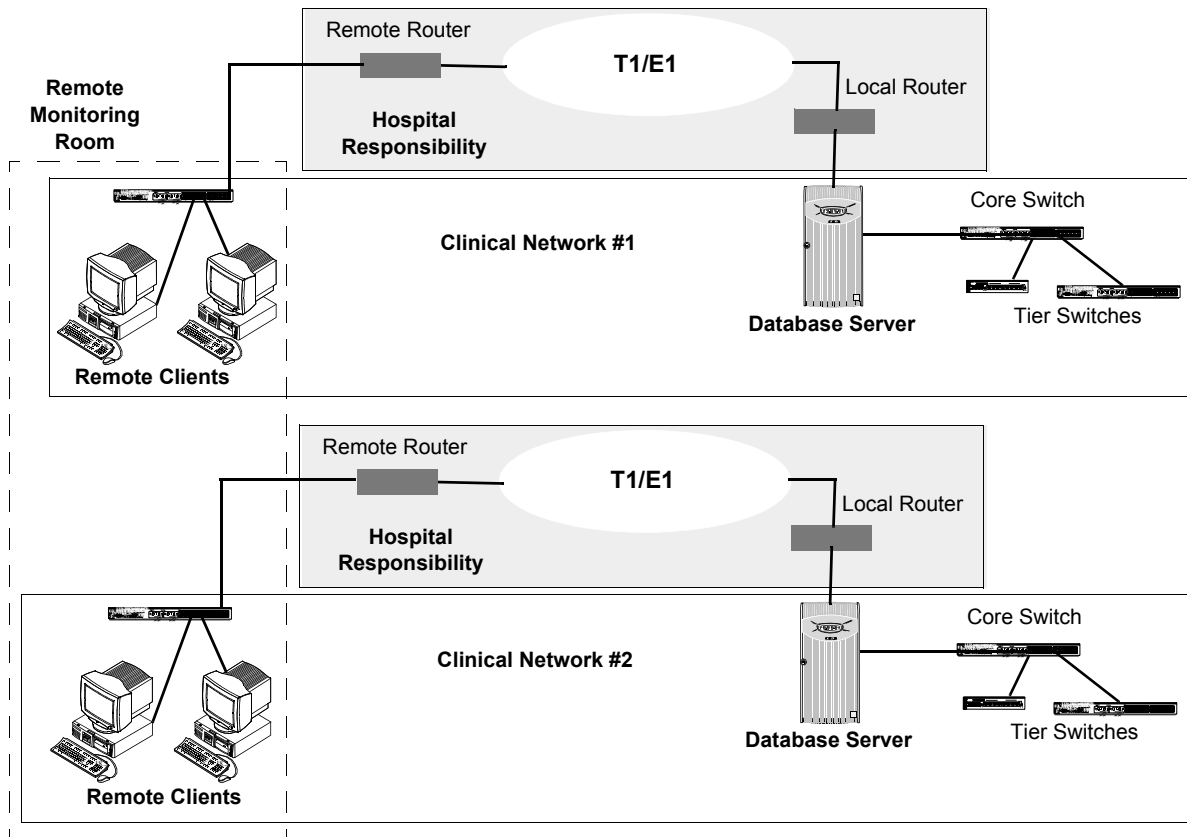


Figure B-4 Remote Clients on different Clinical Networks

Changing Network Properties

To change the Monitoring LAN network properties (IP Address, Default Gateway, Subnet Mask) on the device, go to the **Control Panel** and select the **Network Connections** in Windows XP, or **Network and Dial-up Connections** in Windows 2000. Highlight the **TCP/IP** in the Protocols window and click on **Properties** brings up the **Internet Protocol TCP/IP Properties** window. The IP Address tab shows the **IP Address** of the device. The IP Address can also be changed in this window. The **Subnet Mask** and **Default Gateway** address are also shown, and can be changed here as well.