NTPM99CA 02

Nortel Networks

WLAN Cable Access Point 6220

User Guide

Standard Release 2.0 Issue 1 Dec 2005

What's inside?

Copyright © 2004 Nortel Networks

Multi-Region Product Documentation

This document may describe features that are not available in your region due to local regulations.

Compliances

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

. • Reorient the receiving antenna
. • Increase the separation between the equipment and receiver
. • Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
. • Consult the dealer or an experienced radio/TV technician for help

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

The transmitted power of the APU and CSU does not exceed 36 dBm.

Publication history

December 2005

Issue 1. Issued for WLAN Cable Access Point 6220 APU & CSU

Contents

About this document

This document describes the system features used in the WLAN Cable Access Point 6220 Release 2.0 Product.

Topics covered include the following:

- Overview
  - Introduction
  - Product Description
  - APU (Access Point Unit)
  - CSU (Corporate Service Unit)
- System Planning
  - Site Survey & Planning
  - Wireless Network Designing
- Installation
  - APU Hardware Installation
  - CSU Hardware Installation
- Configuration
  - APU in Secure Data Mode (P2P, P2M)
  - CSU in Secure Data Mode (P2P, P2M)
  - Testing Connection between APU and CSU
- Advanced Configuration
  - System Administration Tasks
  - Save configuration
  - Edit configuration
  - Load new configuration
  - Upload new license
- Troubleshooting

Audience

The intended audience for this document includes:

- Installers
- Technicians
- Nnetwork planners
- Network & system engineers
- Network administrators

List of Abbreviations

AP	Access Point
APU	Access Point Unit
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
BPSK	Binary Phase-Shift Keying
CATV	Community Antenna Television
CM	Cable Modem
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CSU	Corporate Service Unit
DBPSK	Differential Binary Phase-Shift Keying
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data Over Cable Service Interface Specifications
DQPSK	Differential Quadrature Phase Shift Keying
DVM	Digital Volt Ohm Meter
EAP	Extensible Authentication Protocol
EIRP	Equivalent Isotropic Radiated Power
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FTP	File Transfer Protocol
HFC	Hybrid Fiber Coax
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial Scientific and Medical equipment
ISP	Internet Service Provider
ITU	International Telecommunication Union
LOS	Line of Sight
MAC	Media Access Control
MIB	Management Information Base
NAS	Network Access Server
NAT	Network Address Translation

NLOS	Non Line of Sight
NMS	Network Management System
NWID	Network ID
OLOS	Optical Line of Sight
ONU	Optical Network Unit
PCMCIA	Personal Computer Memory Card International Association
PI	Power Inserter
POE	Power over Ethernet
PSU	Power Supply Unit
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Services
RF	Radio Frequency
RIP	Routing Information Protocol
SEC	Super Ethernet Converter
SMTP	Simple Mail Transfer Protocol
SNMP	Single Network Management Protocol
SNR	Signal to Noise Ratio
SSID	Service Set Identification
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VSWR	Voltage Standing Wave Ratio
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

Technical Support and Information

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support as indicated in the following table.

Internet	**http://www.nortelnetworks.com/cgi-bin/comments/comments.cgi**	• Click on Technical Support • Select Online Support • Open a Customer Service Request online
Telephone	**1-800-4NORTEL (1-800-466-7835)**	• Call 1-800-4NORTEL • Find the nearest Technical Solutions Center • Enter ERC (Express Routing Code) if it is available

FCC Conformance

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference. And (2) this device must accept any interference received, including interference that may cause understand operation.

This Class B digital apparatus complies with Canadian ICES-003.

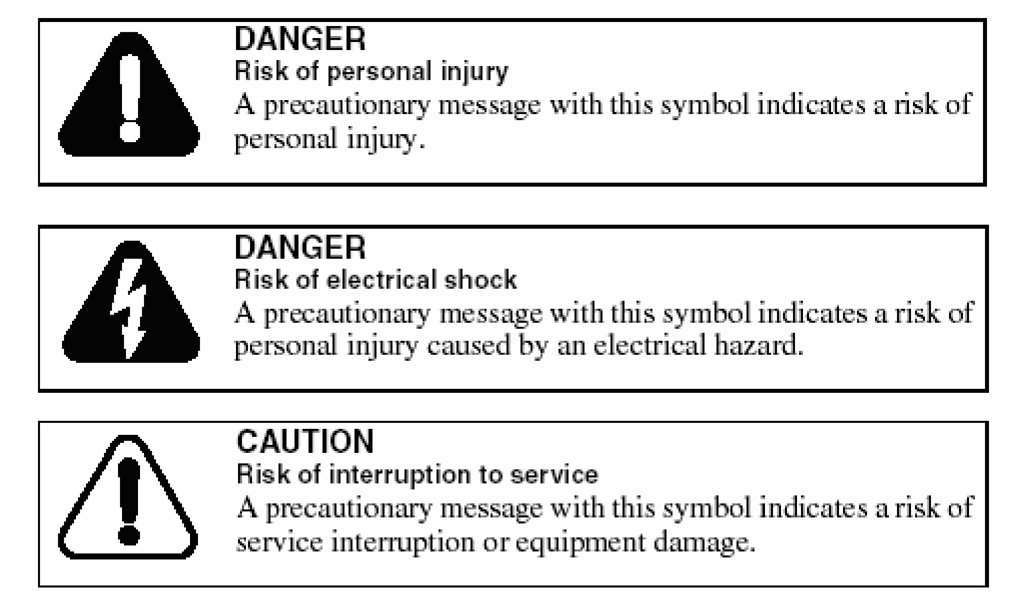
Safety guidelines

This chapter contains safety guidelines that you must follow for personal safety and for the correct handling and operation of equipment.

Warning and safety precautions

To prevent personal injury, equipment damage, or service interruption, follow all precautionary messages found in WLAN Cable Access Point 6220 documentation and the safety procedures established by your company.

The following precautionary messages appear in WLAN Cable Access Point 6220 documentation:



DANGER
Risk of personal injury
A precautionary message with this symbol indicates a risk of personal injury.

DANGER
Risk of electrical shock
A precautionary message with this symbol indicates a risk of personal injury caused by an electrical hazard.

CAUTION
Risk of interruption to service
A precautionary message with this symbol indicates a risk of service interruption or equipment damage.

The graphic symbol of an exclamation point within an equilateral triangle warns the user of the device that it is necessary to refer to the instruction manual and its warnings for proper operation of the unit.

Summary of Warning and Safety Precautions

MAKE SURE THAT POWER SUPPLIER IN HFC NETWORK IS TURNED OFF PRIOR TO CONNECTING THE COAXIAL CABLE TO THE CABLE ENTRY CONNECTOR ON APU ENCLOSURE.

DO NOT FASTEN OR UNFASTEN THE COAXIAL CABLE CONNECTOR ON THE APU WITH UNDER THE UNIT POWERED.

DO NOT CONNECT OR INJECT ANY AC POWER EXCEPT CATV UPS/POWER SUPPLY. SUCH A MISTAKE WILL CAUSE APU TO BE SERIOUSLY DAMAGED.

REFER SERVICING TO A QUALIFIED TECHNICIAN TO REDUCE THE RISK OF ELECTRIC SHOCK WHEN THE UNIT DOES NOT APPEAR TO OPERATE NORMALLY OR EXHIBITS A MARKED CHANGE IN PERFORMANCE.

WHEN INSTALLING THE UNIT, CHOOSE A LOCATION THAT PROVIDES A MINIMUM SEPARATION OF 20 cm FROM ALL PERSONS DURING NORMAL OPERATION.

AN APPROPRIATE DISCONNECT DEVICE SHALL BE PROVIDED AS PART OF THE INSTALLATION.IN THE END SYSTEM.

THE APU AND CSU SHALL BE INSTALLED BY A PROFESSIONAL FIELD TECHNICIAN

BOTH TYPES OF UNITS SHOULD BE INSTALLED BY A PROFESSIONAL FIELD TECHNICIAN TO REMOVE THE POSSIBILITY OF INCORRECT INSTALLATION FOR APU AND CSU.

DO NOT EXPOSE THIS UNIT TO RAIN, MOISTURE OR DUST UNCOVERED.

BE SURE NOT TO BE SITUATED NEAR HIGH VOLTAGE POWER SOURCES.

MAKE SURE THAT ALL BOLTS ON THE ENCLOSURE ARE TIGHTENED FIRMLY SO THAT WATER DOES NOT ENTER THE UNIT.

BE SURE THAT ALL CONNECTORS ARE CONNECTED TO THE UNIT AND THE RF CABLE HAS BEEN PROTECTED BY THE WATER-PROOF CAP.

BE SURE THAT THE POWER SUPPLY UNIT THAT PROVIDES AC POWER TO THE APU OPERATES WITHIN THE GUIDELINES IN THIS MANUAL.

IF YOU ARE NOT SURE OF THE TYPE OF POWER SUPPLIED TO YOUR UNIT, CONSULT YOUR LOCAL NORTEL NETWORKS REPRESENTATIVE OR NETWORK SERVICE COMPANY.

BE SURE THAT THE RADIO ANTENNA IS LOCATED AWAY FROM ALL POWER FACILITIES SUCH AS CABLE OR POWER SUPPLIERS.

NEVER PUSH OBJECTS OF ANY KIND INTO THE UNIT. IT MAY TOUCH DANGEROUS VOLTAGE POINTS OR SHORT-OUT PARTS THAT COULD CAUSE AN ELECTRIC SHOCK.

DO NOT ATTEMPT TO HANDLE THE UNIT YOURSELF. WITHOUT FULL KNOWLEDGE OF THE OPERATIONS AND CHARACTERISTICS OF THE APU PRODUCT AS OPENING OR REMOVING COVERS MAY EXPOSE YOU TO DANGEROUS VOLTAGE OR OTHER HAZARDS.

Overview

Introduction

This document describes the system features used in the WLAN Cable Access Point 6220 Release 2.0 Product.

The Wireless LAN Cable Access Point 6220 is an outdoor hardened, strand-mountable access point solution designed to extend the reach of the cable operators' hybrid fiber coax network utilizing wireless technologies from existing rights of ways. This solution from Nortel Networks provides cable operators a fast, low-cost alternative for delivering service to new customers by eliminating the time, permits, and construction costs associated with extending aerial or buried drops.

The WLAN Cable Access Point 6220 solution provides:

Flexible service platform

The WLAN Cable Access Point 6220 is a flexible service platform giving cable operators the ability to offer many different wireless services such as Public Hot Spots and Commercial High Speed Data services.

Standard Compliance and Interoperability

The WLAN Cable Access Point 6220 utilizes standard-compliant DOCSIS^{TM} cable modems, thus ensuring interoperability with the existing cable network. Wireless access is accomplished using industry-standard IEEE 802.11 radios approved by government regulatory agencies for use in “unlicensed” ISM and U-NII band frequencies.

Security

Security is of the highest importance when delivering wireless services. The WLAN Cable Access Point 6220 adheres to industry standards for 802.11 devices and augments those standards with additional security features designed to provide both the cable operator and the end-user maximum protection.

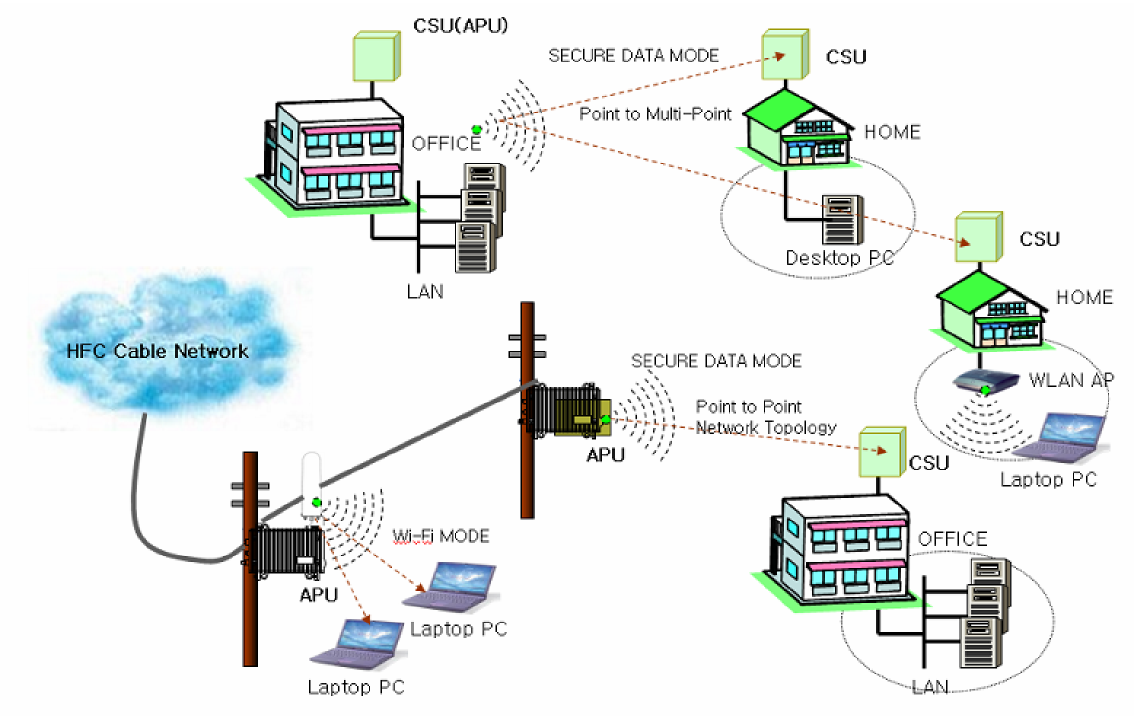
Performance optimization via multiple antenna options

Nortel Networks provides antenna options specifically engineered to enable the WLAN Cable Access Point 6220 to achieve peak link performance in Line of Sight (LOS) and Near LOS applications.

Ease of installation

Designed for simple, fast installation by professional technicians, the WLAN Cable Access Point 6220 is installed in a simple three-step procedure: lock down strand clamps, connect power via coax drop, and attach and align antenna for service optimization

Figure 1-1
WLAN Cable Access Point 6220 Service Concept Diagram



Product Description

Figure 1-2
WLAN Cable Access Point 6220 APU Package Components

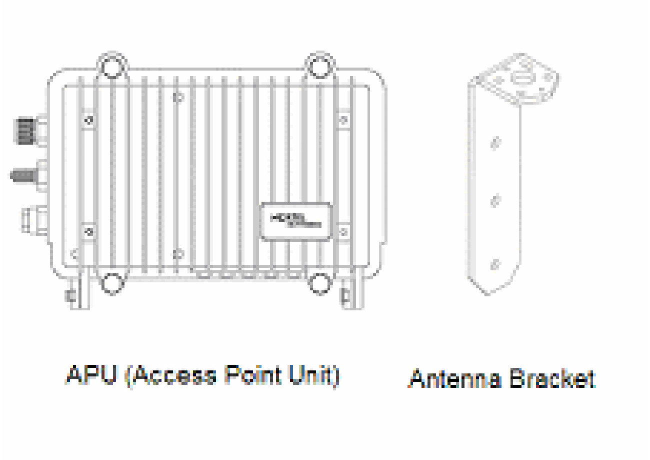
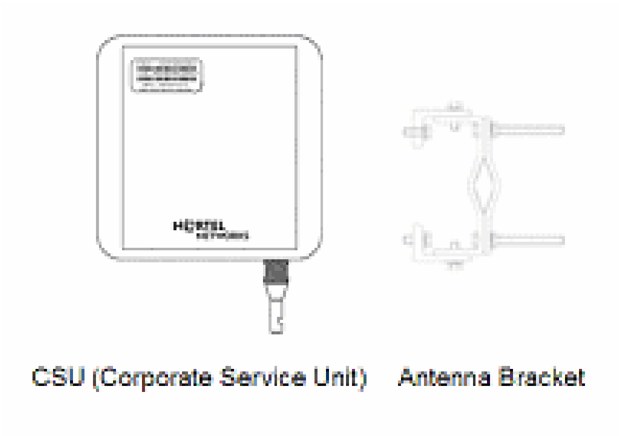


Figure 1-3
WLAN Cable Access Point 6220 CSU Package Components



APU (Access Point Unit)

The following is a list of WLAN Cable Access Point 6220 APU features:

- Enclosure has three sorts of connectors which support the connection to CATV Cable Network, Antenna and Monitoring Equipment.

- Coaxial Port has the standard type of connector that can be efficiently adapted to every connector regardless of the termination type of coaxial cable such as “Trunk or Drop Cable”

- Operation Power and Data Traffic are mixed at a signal amplifier as TBA (Trunk Bridge Amplifier), PI (Power Inserter) and supplied to the coaxial port on the APU through coaxial cable.

- Monitoring Port can provide the safe testing method for measuring CATV signal to an installation engineer by attenuating RF power and protect AC power signal.

- Basically, two kinds of mounting types are available for the APU, such as a steel wire strand mounting and wall mounting, but in case of wall mounting, another optional bracket kit will be needed for installation.

- The three available antennas are ‘Directional Type’, ’Bi-directional Type’ and ‘Omni-directional Type’, which can be mounted on the front or rear cover of the APU with a Universal Bracket.

- Cable Modem Module is compliant to DOCSIS 2.0(Cablelabs) as well as DOCSIS 1.1 and WLAN AP support the secure mode connection which means that wireless traffic from APU and CSU is not scanned and detected by a conventional sniffing program like ‘Netstumbler’.

Figure 1-4
APU (Top head)

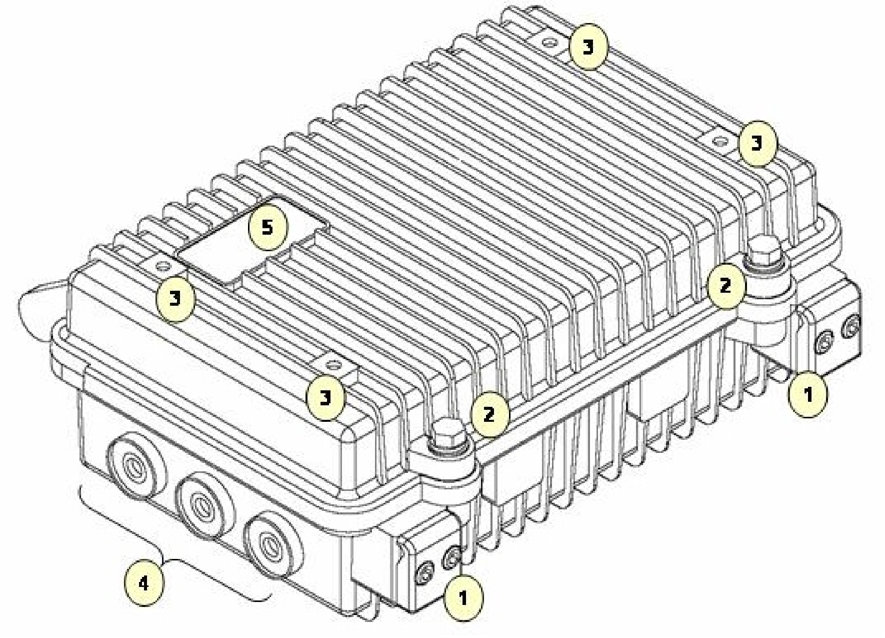


Figure 1-5
APU (Bottom)

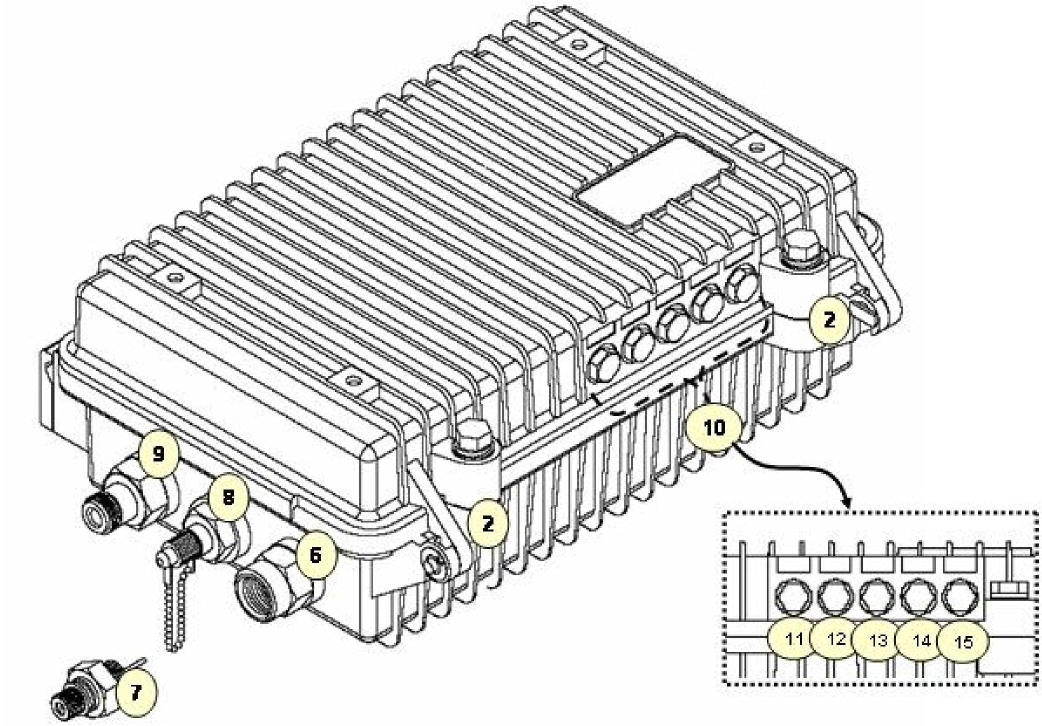


Figure 1-6
Inner Panel (APU)

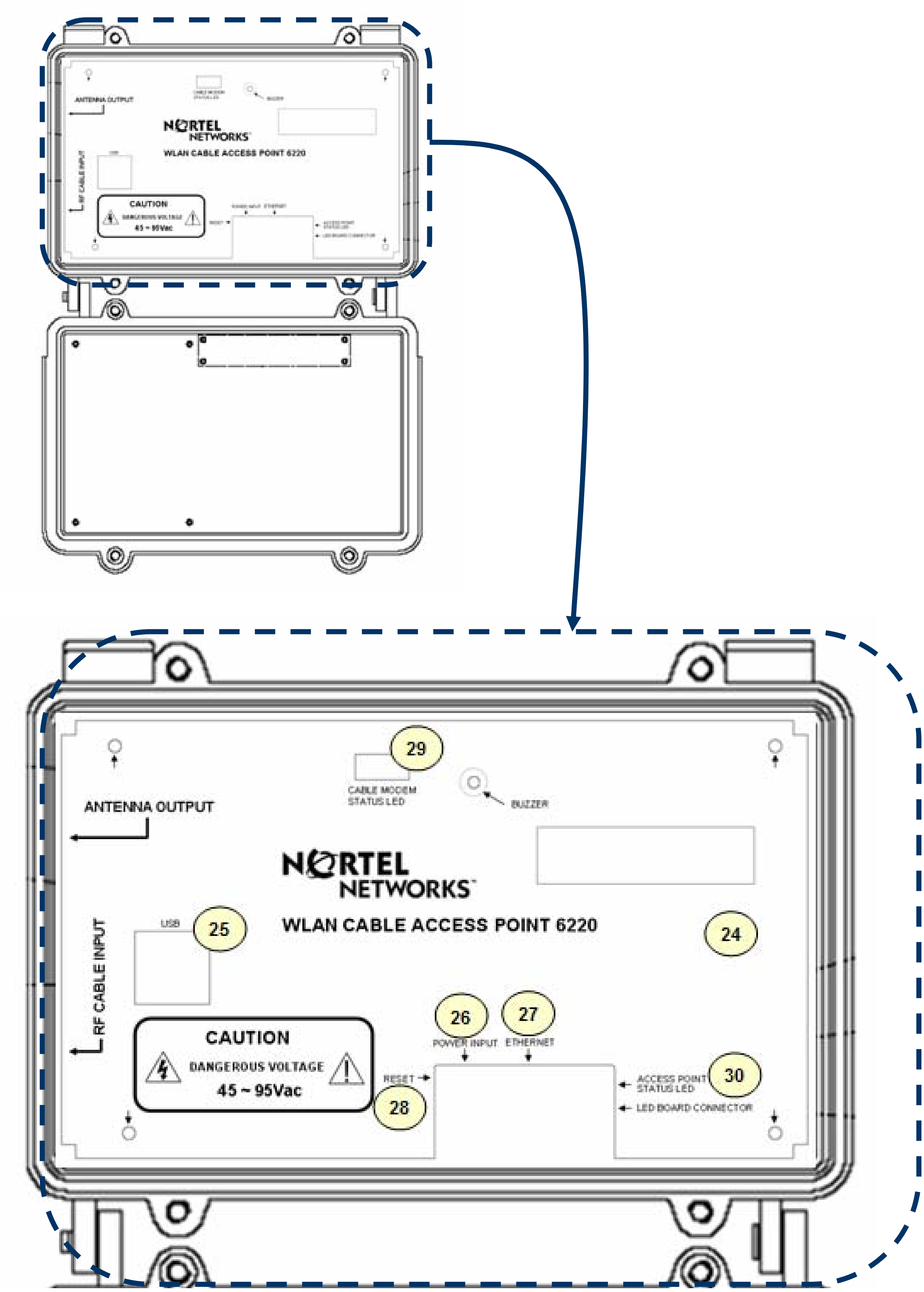


Figure 1-7
APU (Back)

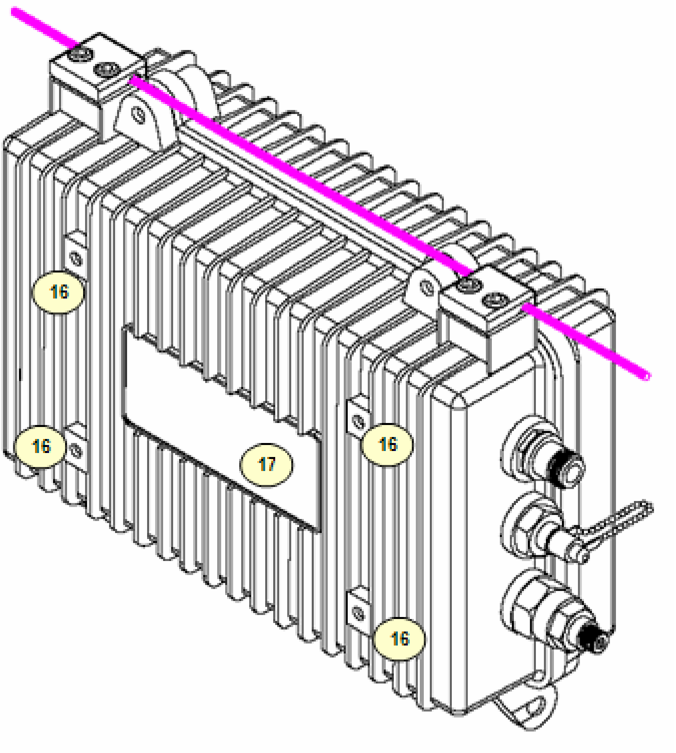


Figure 1-8
APU System Structure and Signal Flow

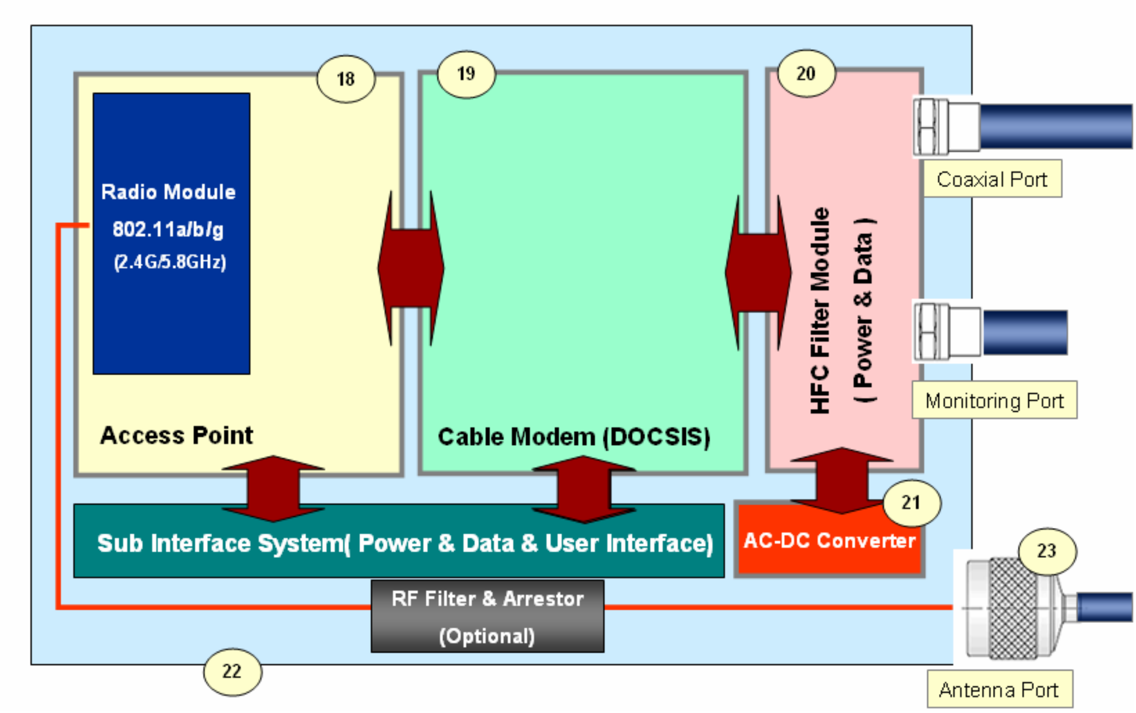


Table 1-1. Modules and Connectors (APU)

Item	Label	Description & Function	
1	Clamp Module	Provide strand mounting function to APU, Strand Clamp and Mount Bosses	
2	Lid Bolt	Lid Bolt for closing a case of APU enclosure	
3	Antenna Mount Hole	Screw Holes for mounting a APU antenna with a universal bracket	
4	Reserved Port	Reserved Location for a future upgrade and revision	
5	Logo Panel	Location for Nortel networks Logo	
6	Cable Entry Port	Port for coaxial cable connection. Trunk and Drop termination types are supported	
7	Cable Adaptor	Coaxial Adaptor Port to connect F-type Drop cable to APU Cable Entry Port	
8	Monitoring Port	Port reserved for safe testing of Cable RF signal. The signal on this port is attenuated by 20 dB	
9	Antenna Port	Port for antenna connection	
10	LED Panel	Provide the information for system operation status through LED Display	
11	LED1(Power)	Indicate Power is turned on	
12	LED2(Link #1)	ON	Indicate a valid cable modem operation
		Flash	Indicate that cable modem is linked up on the HFC network
13	LED3(Link #2)	ON	Indicates a Ethernet link between access point and cable modem
		Flash	Indicates that the access point is transmitting or receiving data
14	LED4(Radio #1)	ON	Indicates the 802.11 radio is enabled and operating
		Flash	Indicate that a frame is transmitted or received on the radio port
15	Reserved		Reserved location for a future upgrade
16	Antenna Mount Hole Grounding Hole	Screw Holes for mounting a APU antenna with a universal bracket and grounding the APU enclosure	
17	Label	Location for attaching a product label which include S/N,PEC,MAC address and so on	
18	Access Point	Mini-PCI type III Radio Card, System Board(Wi-Fi & Secure Data Mode ^{TM})	
19	Cable Modem	DOCSIS 2.0 compliant cable modem	
20	HFC Filter	Split a HFC Signal and AC power from the combined signal	
21	PSU	AC to DC Power converter	
22	Case	Housing case which can be mounted on strand and antenna mounting bracket	
23	Antenna	2.4GHz and 5.8GHz Radio Frequency Antenna (Flat Panel, Omni-directional and Bi-directional). APU antenna can be mounted on the front or rear cover of APU with universal bracket.	
24	Inner Panel	Cover Panel to secure the main system boards(WLAN AP, Cable Modem)	
25	USB Port	USB type port for testing the Cable Modem Module	
26	DC Connector	3-pin connector to supply DC power to system board from Power Converter	
27	Ethernet Port	Port to connect APU to laptop/PC for testing purpose	
28	Reset S/W	Switch to reset the system to default settings	
29	Cable Modem LED	Indicate the full status of Cable Modem	
30	Access Point LED	Indicate the full status of Access Point	

CSU (Corporate Service Unit)

The following is a list of WLAN Cable Access Point 6220 CSU features:

- Enclosure has a POE connection interface and a DC Power Adapter Jack at the bottom of the CSU.
- Operation Power & Data Traffic are mixed at POE Injector and supplied to the Ethernet Port on the CSU through CAT5 Cable.
- Two types of mounting alternatives are available, pole mount and wall mount. If wall mount is used a mounting kit will be required.
- The antenna is basically a Flat Panel type which is a built-in CSU body protected by a plastic material RADOME.
- WLAN AP supports the secure mode connection which means that wireless traffic from APU and CSU is not scanned and detected by a conventional sniffing program like ‘Netstumbler’.

Figure 1-9
WLAN Cable Access Point 6220 CSU (Bottom)

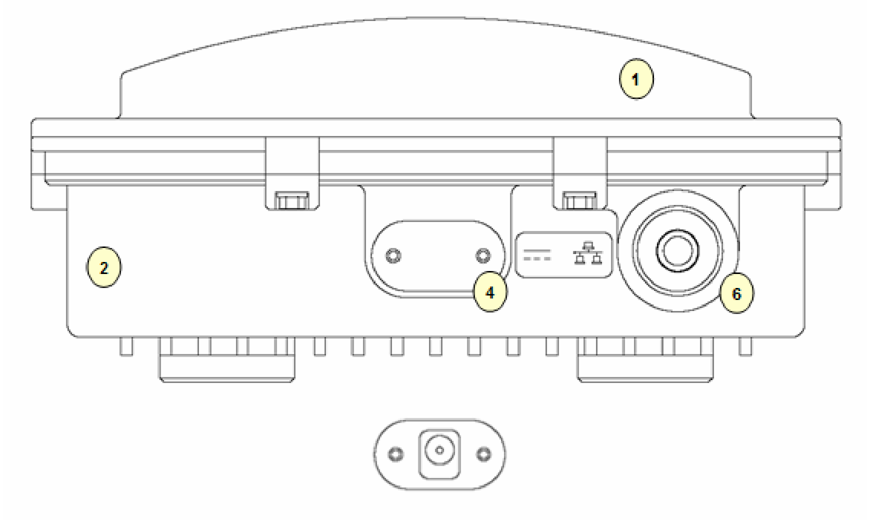


Figure 1-10
WLAN Cable Access Point 6220 CSU (Front)

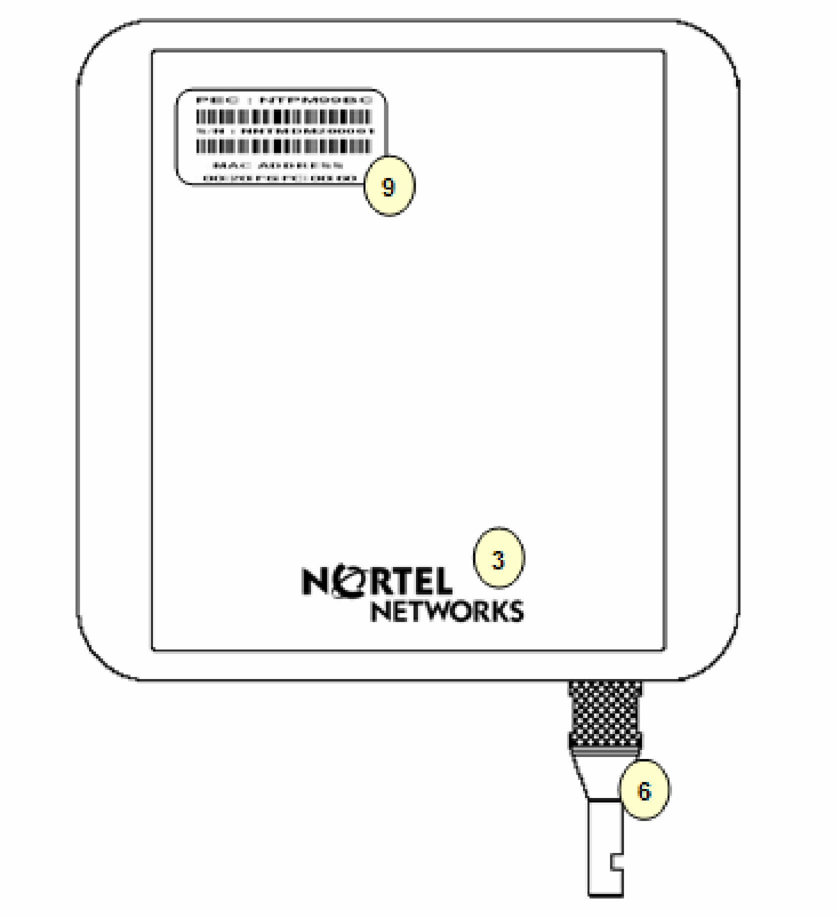


Figure 1-11
WLAN Cable Access Point 6220 CSU (Back)

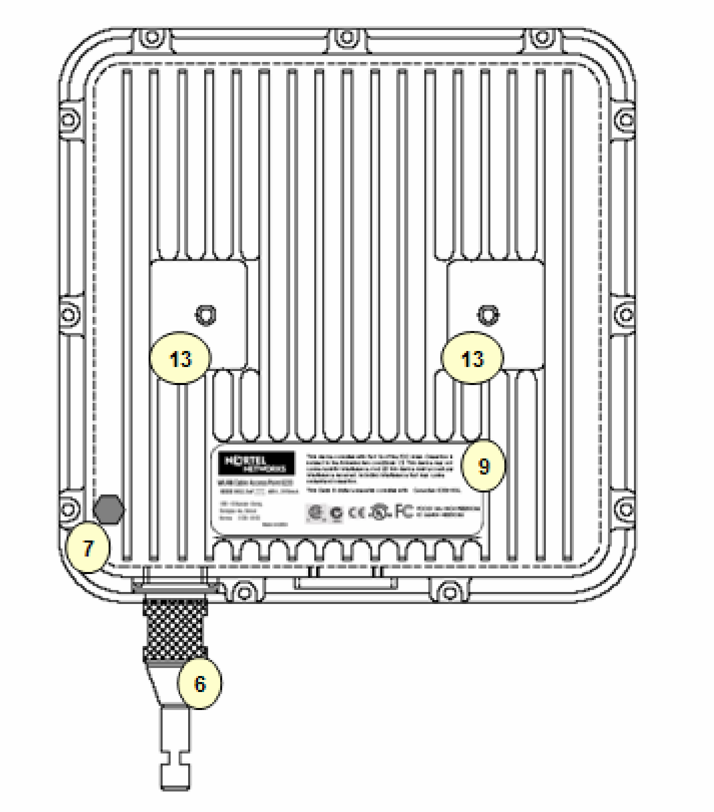


Figure 1-12
WLAN Cable Access Point 6220 CSU

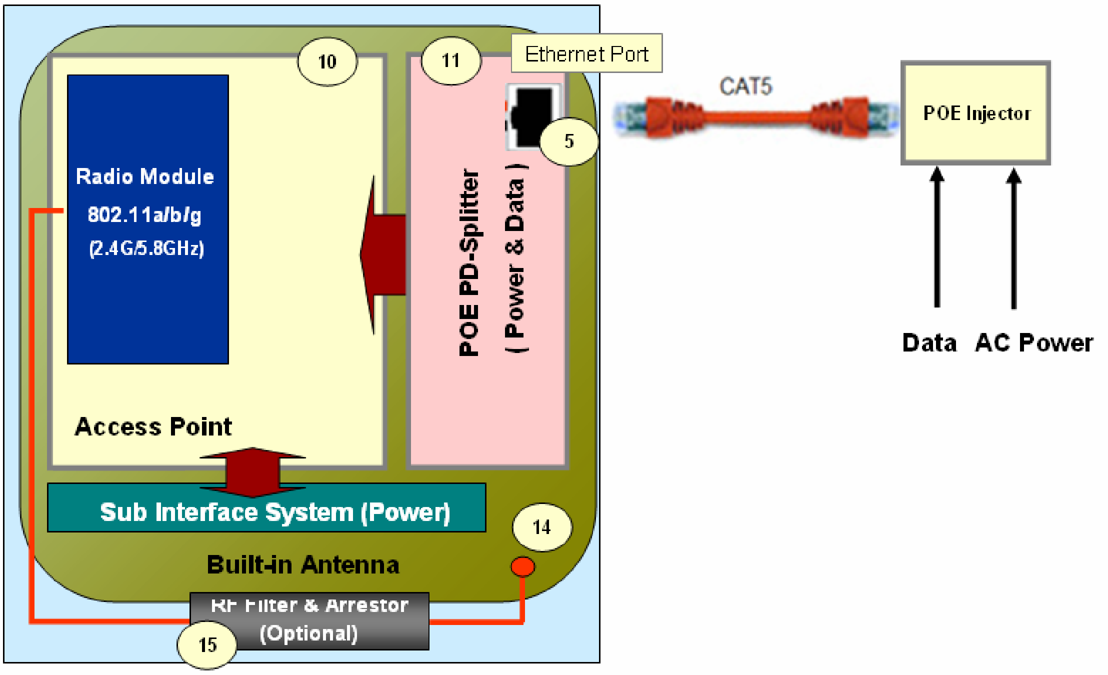


Table 1-3. Modules and Connectors (CSU)

Item	Label	Description & Function
1	Antenna Radome	Protective Cover designed to contain a built-in antenna
2	Enclosure(Body)	Housing Integrated with an Antenna Case Assembly
3	Logo Panel	Location for Nortel networks Logo
4	DC Power Socket	Provide DC power(12V) from AC-DC Adaptor to CSU
5	Ethernet Port(POE)	Provide data connection between CSU and POE Injector or LAN Switch
6	EMI Cap	EMI Cap designed to prevent CSU from interfering to or from other devices Additionally, provide water proof feature accompanied by sealing tape
7	Ground Point	Location for grounding the enclosure to earth for protecting the product from damage
8	Label(Front)	Location for attaching a product label which include S/N,PEC,MAC address and so on
9	Label(Back)	Location for attaching a product label which include S/N,PEC,MAC address and so on
10	Access Point	Mini-PCI type III Radio Card, System Board(Wi-Fi & Secure Mode ^{TM})
11	POE Splitter	Power Module to divide Ethernet Signal and DC power combined signal from POE Injector
12	POE Injector	Provide 802.3af based signal to CSU through Ethernet Port on CSU
13	Bracket Hole	Bolt Hole for assembly of mounting bracket
14	Built-in Antenna	2.4GHz or 5GHz Radio Frequency Antenna (Flat Panel)
15	RF Filter & Arrestor	RF module protecting from out-high voltage surge and ESD damage

⚠ **THE 12V POWER CONNECTOR IS NOT INTENDED FOR FIELD USE. THIS SOCKET IS ONLY APPLICABLE FOR A SPECIAL USE AT FACTORY OR REPAIR FACILITY.**

Planning your WLAN Network

The wireless network is much different than a wired network. The Installation of a wireless network requires some additional planning. This planning includes RF Link Engineering like RF Path planning, site selection, and back-bone network preparation.

The radio links between all end sites are specified as three types of environmental connection as listed below:

LOS (Line Of Sight)
OLOS (Optical LOS)
NLOS (Non LOS)

Because High Frequency Radio travels in a straight forward line, a clear LOS (line-of-sight) between antennas is efficient and ideal. Frequently, locations of the desired links are fixed.

When you cannot achieve a clear line-of-sight, you must plan according to basic consideration:

The Basic considerations for sites include:

- Installation Facility must be constructed (Electric Pole, Tower)
- Possibility of future obstructions
  - Trees that may obstruct the path
  - Buildings between the sites that may obstruct the path
- Lightening
- Distance between sites and Network Structure
- Strong RF interference

Site Survey & Planning

Definition

A site survey is a task-by-task process by which the surveyor discovers the RF behavior, coverage, interference, and determines proper hardware placement in a facility. The site survey's primary objective is to ensure that mobile workers and the wireless LAN's clients experience continuously strong RF signal as they move around the facility.

Items

- *Facilities Analysis*
- *Existing Networks*
- *Area Usage & Towers*
- *Purpose & Business Requirements*
- *Bandwidth & Roaming Requirements*
- *Available Resources*
- *Security Requirements*
- *Preparation Exercises*
- *Preparation Checklist*

Site Survey Equipment

- *Corporate service unit(CSU) with POE Injector*
- *Laptop and/or PDA*
- *Wireless PC card with driver & utility software*
- *Battery pack charger & DC-to AC converter*
- *Site survey utility software (loaded on laptop or PDA)*
- *Clipboard, pen, pencils, notebook paper, grid paper, & highlighter*
- *Blueprints & network diagrams*
- *Outdoor antennas(Omni-directional, Patch, Bi-directional)*
- *Cables & connectors*
- *Specialized software or hardware such as a spectrum analyzer*
- *Digital camera for taking pictures of particular locations within a facility*
- *Variable attenuator*

Wireless Network Planning

Procedure 1 (Location)

1. Select and identify enough location candidates to determine freely as the install point regardless of some design change to some extent.
2. The most crucial parameter is the range at which APU and CSU or other Wi-Fi Client is required to operate. The range can be determined by a conventional formula which consider a various kinds of environmental and radio equipment.
3. Another consideration in installing APU and CSU is the network connection like a CATV Coaxial Cable and CAT5 Ethernet Cable. Even though some locations are the best location in terms of RF performance, the actual installed location is restricted by limited cable reach.

Procedure 2 (Radio Link Path)

1. Choose the proper antenna type with a site survey result.
2. For best performance, mount the APU and CSU in a location where there is LOS (Line Of Sight) to each antenna.
3. Perform the field survey to summarize every obstacle like tree and earth bulge in consideration of OLOS (Optical LOS).
4. With the site survey result, adjust the tilt and angle of antenna so that there is maximum clearance within the FRESNEL ZONE of the direct path.

   Note: The best means of achieving FRESNEL ZONE clearance is to raise the height of APU or CSU mounting point as high as possible
5. In order to get the more exact information on RF radio link path, calculate the Link Budget for Radio Link between APU and CSU which is referred in the end of this section.

Note: The link budget is a rough calculation of all known elements of the link to determine whether the signal will have the proper strength to the other end of the link.

Procedure 3 (RF Channel Selection)

1. Check all range of channels by RF measurement with Frequency Analyzer in order to see the interference effect with APU and CSU. Actually, RF interference is likely to arise from any other wireless system operating within the same frequency band as ISM/UNII Band Radio Products.

Note: The final selection of operating channel should be done with the testing results of both APU and CSU.

Procedure 4 (Radio Performance Tuning)

Please refer to the Radio Link Test

Installation

General

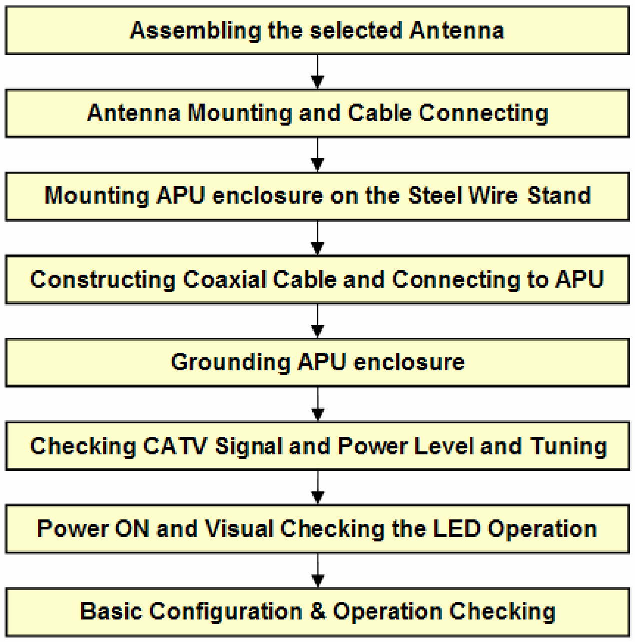
This section provides a complete set of procedures for the installation of WLAN 6220 equipment. It includes cable assembling information as well as required connection information for the WLAN 6220 units, mounting and powering instructions.

It is intended for use by trained installers familiar with CATV or Cable Modem and Wireless installations.

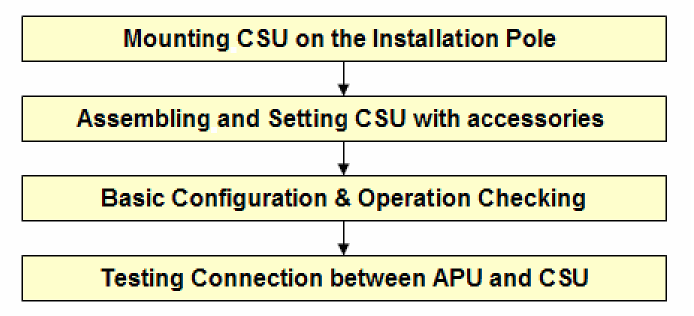
For technical assistance, contact your next level of support or Nortel Networks according to the information available in Technical Support and Information section.

Installation Procedure Summary

APU (Access Point Unit)


Assembling the selected Antenna
Antenna Mounting and Cable Connecting
Mounting APU enclosure on the Steel Wire Stand
Constructing Coaxial Cable and Connecting to APU
Grounding APU enclosure
Checking CATV Signal and Power Level and Tuning
Power ON and Visual Checking the LED Operation
Basic Configuration & Operation Checking

CSU (Corporate Service Unit)


Mounting CSU on the Installation Pole
Assembling and Setting CSU with accessories
Basic Configuration & Operation Checking
Testing Connection between APU and CSU

Required Tools and Materials

Before you install the WLAN Cable Access Point 6220, ensure you have the following:

APU

WLAN Cable Access Point 6220 APU package does not contain an antenna and universal antenna bracket kit. For list of antennas and accessories, see the WLAN Cable AP 6220 manual or contact your local Nortel networks representative.

- One or more antenna cables (N-Male to the connector on the external antenna)
- External antennas selected by yourself
- Flat blade screwdrivers
- Wire cutters
- Phillips screwdriver
- Torque wrench/driver
- Other proper tools for installation
- Heat gun with propane/ Mapp torch
- Trunk & Distribution Cable Connector and Drop Cable F-connector port
- RF cable for connecting between the APU and Testing Unit (if needed)
- Portable CATV Spectrum Analyzer
- DVM(Digital Voltammeter)
- “Document CD” and “Software CD” that contains the APU Configurator, online help for the Configurator, and various documents.
- Advanced Tool: RF Testing Unit: CSU, Laptop computer with radio card

CSU

- IEEE 802.3af-2003-compliant Power over Ethernet (POE) injector

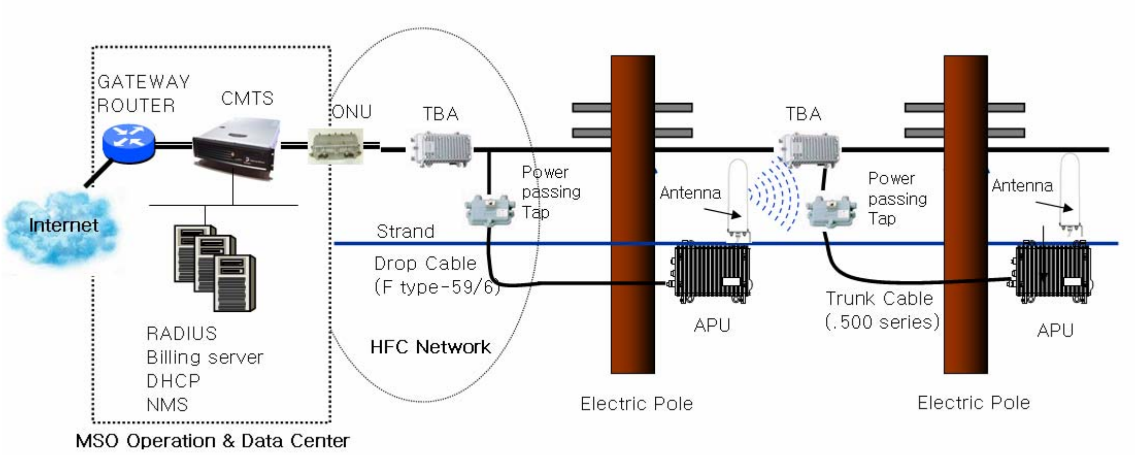
  Note: Ensure that the POE Injector is UL/cUL approved,
  with LPS (limited power source) output.

- Heat gun with propane/ Mapp torch
- 1 CAT5 Ethernet Extender Coupler
- “Document CD” and “Software CD” that contains the APU Configurator, online help for the System Configuration, and various documents.
- PC or workstation with a Web browser for configuration

APU Installation & Configuration

Mounting and Installation Concept

Figure 3-1
APU Installation Concept on CATV Network Facility



By default, APU is strand mountable. Each unit is shipped with a strand clamp module.

Both Drop and Trunk cable termination types are applicable to the APU. The recommended method is Drop cable.

The APU supports a variety of antenna types: omni-directional, flat panel and bi-directional. The antenna type should be selected according to the coverage needed and type of application - please refer to Appendix H for more detailed information.

Procedure 1-1
Assembling and Mounting the selected Antenna

Common Procedure

1. Unpack the antenna box and check the contents listed in the manual in the box.
2. Prepare the recommended tools for assembly and installation of the antenna.
3. Assemble the antenna and bracket kit following the assembly procedure for the selected antenna type.
4. Perform assembly of antenna and bracket as below.

Action

NTA 2407 (Flat Panel Antenna)

Step Action

1. Ensure that each part number is the same as the actual part in the box and the auxiliary mounting bracket (#2311) is securely mounted on the antenna body.
2. Attach the universal mounting bracket (#43) to the auxiliary mounting bracket using the 1/4" flat washers, lock washers, hex nuts, and hex bolts as shown in the diagram. Ensure that the brackets are attached through the oblong hole in mounting bracket.
3. With the antenna connector oriented upward, fasten mounting bracket #43 to the radio using the M6 flat washers, lock washers, and hex bolts as shown in the mounting diagram.
4. To adjust the pan of the antenna, loosen the 1/4" hex bolts that attach the auxiliary mounting bracket with universal mounting bracket, adjust the pan, and re-tighten the bolts.

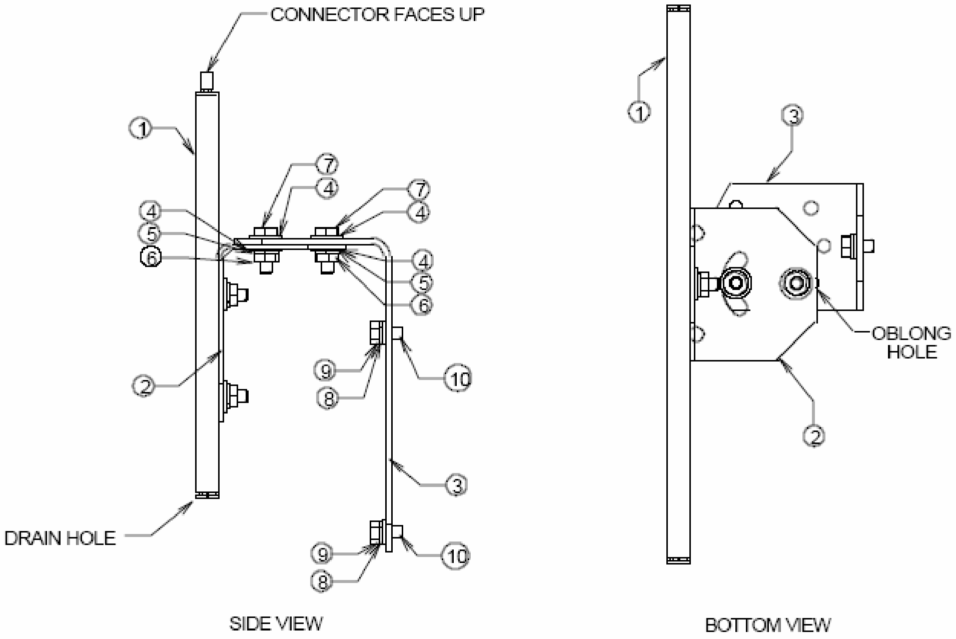
Lightning Protection
The antenna is at DC ground for lightning protection. If the antenna is mounted to a non-conductive structure it should in turn be grounded using practices supplied/approved by the customer.

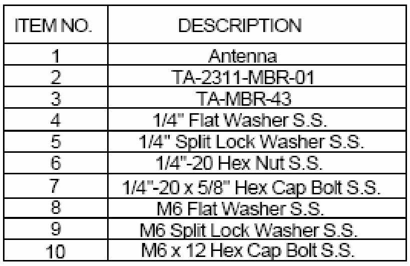
Weatherproofing
All connections between the antenna connector and the transmission line must be weatherproofed according to standard industry practices.

Drainage

Since the RADOME is not pressurized, there is a drain hole in the connector base plate. The antenna must be installed so that the drain hole remains on the bottom. This drain hole must be kept open so that any moisture accumulating inside the RADOME will be able to drain properly.

Figure 3-2
NTA-2407 Antenna Assembly





ITEM NO.	DESCRIPTION
1	Antenna
2	TA-2311-MBR-01
3	TA-MBR-43
4	1/4" Flat Washer S.S.
5	1/4" Split Lock Washer S.S.
6	1/4"-20 Hex Nut S.S.
7	1/4"-20 x 5/8" Hex Cap Bolt S.S.
8	M6 Flat Washer S.S.
9	M6 Split Lock Washer S.S.
10	M6 x 12 Hex Cap Bolt S.S.

NTA 2400 (Omni directional Antenna)

Step Action

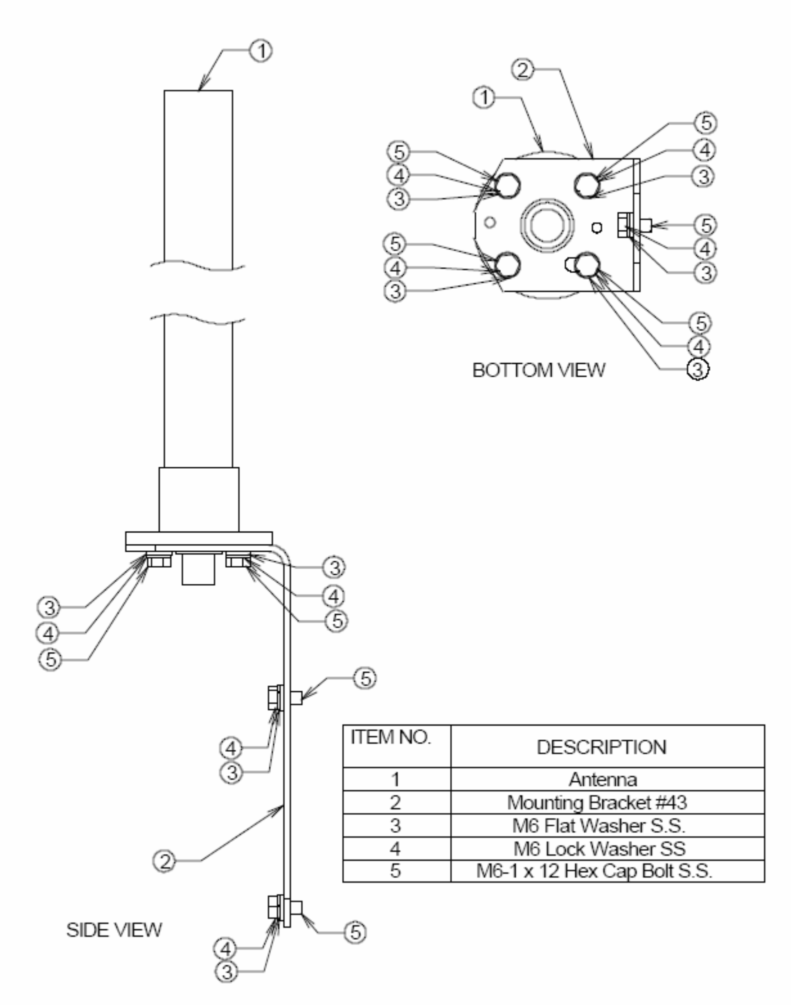
1. Ensure that each part number matches the actual part in the box.
2. Attach the mounting bracket to the antenna using the M6 flat washers, lock washers and hex cap bolts as shown in the mounting drawing.

3. With the antenna oriented upward, fasten the mounting bracket to the radio using the M6 flat washers, lock washers, and hex cap bolts as shown in the mounting diagram.

Lightning Protection
The antenna is at DC ground for lightning protection. If the antenna is mounted to a non-conductive structure (e.g. building wall, wooden pole etc.) it should in turn be grounded using practices supplied/approved by the customer.

Weatherproofing
All connections between the antenna connector and the transmission line must be weatherproofed according to standard industry practices.

Figure 3-3
NTA-2400 Antenna Assembly



ITEM NO.	DESCRIPTION
1	Antenna
2	Mounting Bracket #43
3	M6 Flat Washer S.S.
4	M6 Lock Washer SS
5	M6-1 x 12 Hex Cap Bolt S.S.

NTA 2412 (Bi-directional Antenna)

Step Action

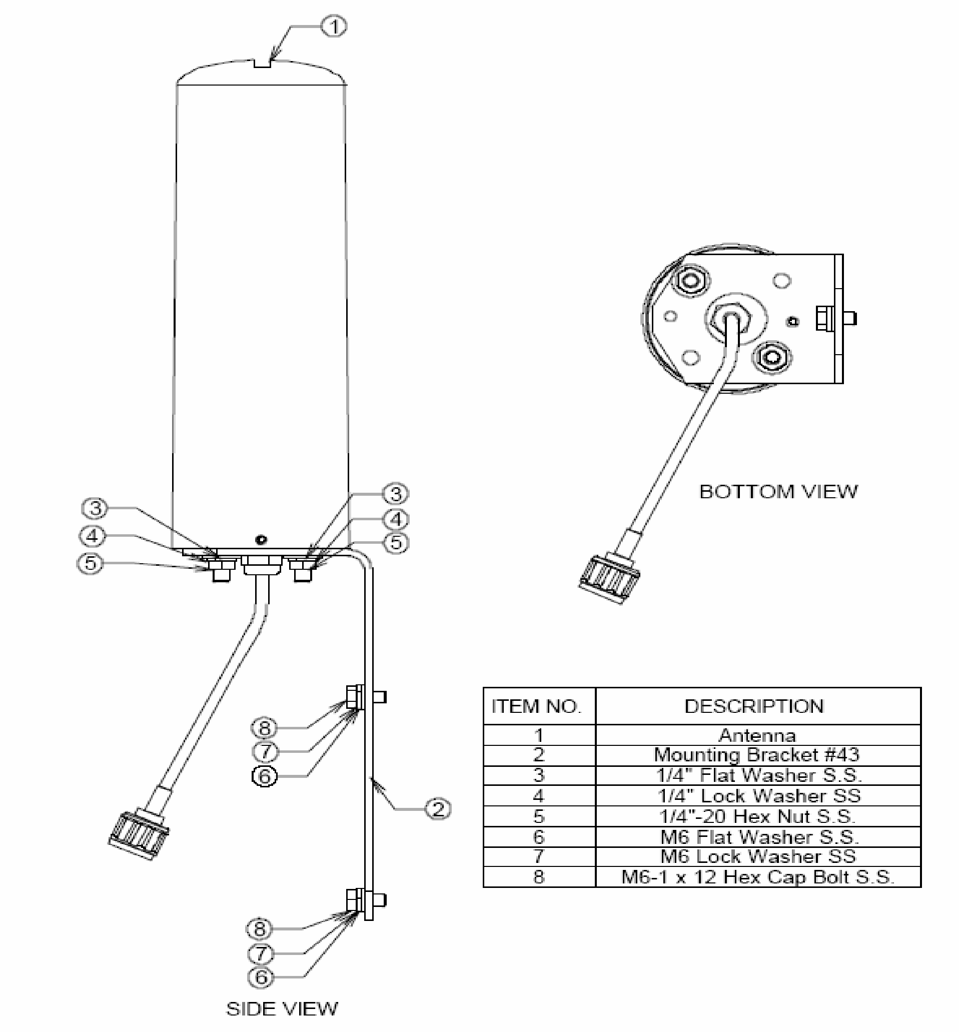
1. Ensure that each part number matches the actual part in the box.
2. Attach the mounting bracket to the antenna using the 1/4" flat washers, lock washers and hex nuts as shown in the mounting drawing.
3. With the antenna oriented upward, fasten the mounting bracket to the radio using the M6 flat washers, lock washers, and hex bolts as shown in the mounting diagram.

Lightning Protection
The antenna is at DC ground for lightning protection. If the antenna is mounted to a non-conductive structure (e.g. building wall, wooden pole etc.) it should in turn be grounded using practices supplied/approved by the customer.

Weatherproofing
All connections between the antenna connector and the transmission line must be weatherproofed according to standard industry practices.

Drainage
Since the RADOME is not pressurized, there is a drain hole in the connector base plate. The antenna must be installed so that the drain hole remains on the bottom. This drain hole must be kept open so that any moisture accumulating inside the RADOME will be able to drain properly.

Figure 3-4
NTA-2412 Antenna Assembly



ITEM NO.	DESCRIPTION
1	Antenna
2	Mounting Bracket #43
3	1/4" Flat Washer S.S.
4	1/4" Lock Washer SS
5	1/4"-20 Hex Nut S.S.
6	M6 Flat Washer S.S.
7	M6 Lock Washer SS
8	M6-1 x 12 Hex Cap Bolt S.S.

Procedure 1-2
Antenna Mounting and Cable Connecting

Action

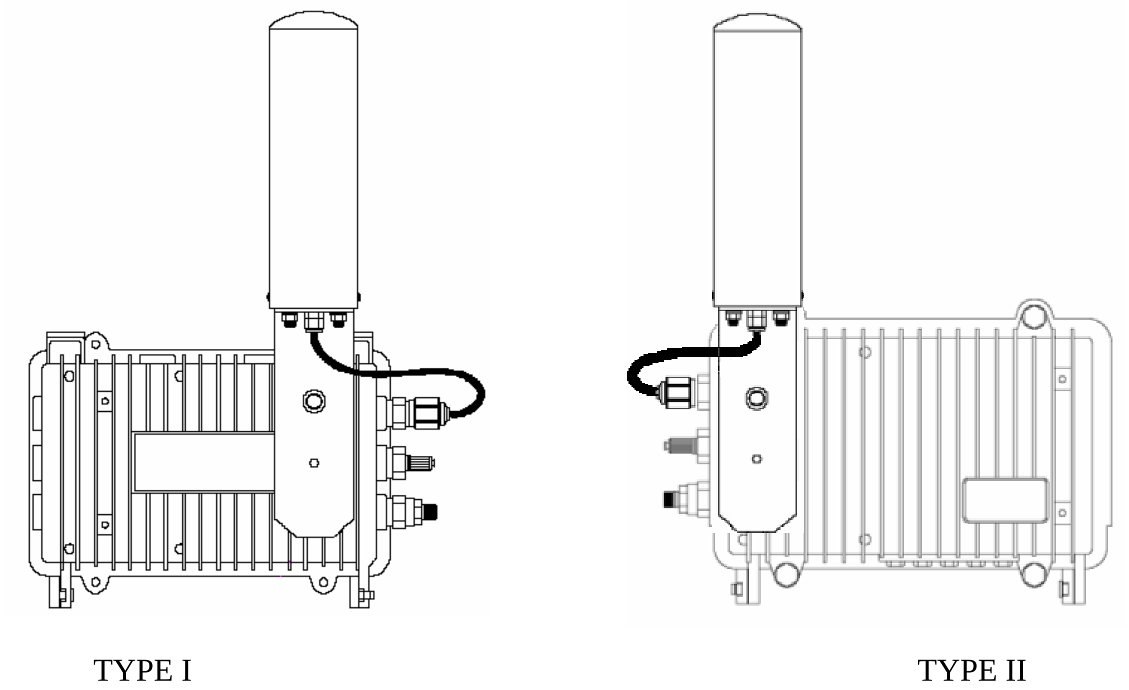
Step Action

1. Attach the bracket on the back surface of the APU and thread one flat washer onto each hex bolt. Screw each bolt with the washer into the two mounting holes.

Note: Even if the APU enclosure has universal mounting holes on the front and rear cover, we recommend that you do not mount two kinds of antenna such as omni-directional and bi-directional type on the front cover. If inevitable, the left side of the front cover is the preferred location in consideration of antenna cable length.

2. Tighten each bolt until the washer is pressed firmly into the APU Enclosure.

Figure 3-5
Antenna mounting with a bracket



TYPE I

TYPE II

BE SURE THAT THE RADIO ANTENNA IS LOCATED AWAY FROM ALL OTHER POWER FACILITIES LIKE CABLE OR POWER SUPPLIERS.

Procedure 1-3

Mounting the APU on the Steel Wire Strand

Action

Step Action

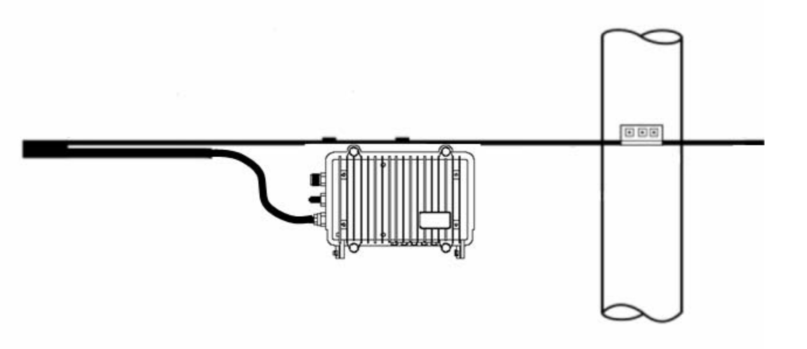
1. Prior to an installation, check if the strand has the strength to sustain the weight of the APU or 10 lbs.

Note: During placing the cable, do not exceed the maximum rated pulling tension of the steel. After the cable has been placed, tension should be applied to the strand only. Refer to the table of guidelines found in the current NESC Rules 250-252.

Table 3-1
Strand Tension and limitation

Strand Diagram inches (mm)	Weight lbs/ft (kg/m)	Max rated Load lbs (kg)
0.109 (2.77)	0.032 (0.048)	1800 (816)
0.134 (3.40)	0.048 (0.075)	2680 (1216)
0.188 (4.77)	0.073 (0.109)	3990 (1810)
0.250 (6.35)	0.121 (0.180)	6650 (3016)

Figure 3-6
APU Installation scheme



2. Attach the strand clamp assemblies to the top strand clamp bosses (mounting surfaces) with a long socket cap screw bolt (Diameter: 5 mm, Length: 15mm) and lock washers.
3. Slide the wire strand into the clamp module.
4. Tighten the bolts with the power tool that has a hex head socket bit so that the enclosure cannot come off the strand, while the location can still be adjusted.
5. Torque the clamp bolts to between 35 and 60 in-lbs (3.9 and 6.8 Nm).

⚠ ENSURE THAT ALL BOLTS IN THE ENCLOSURE ARE FIRMLY TIGHTENED.

⚡ WHEN INSTALLING THE UNIT, CHOOSE A LOCATION THAT PROVIDES A MINIMUM SEPARATION OF 20 cm FROM ALL PERSONS DURING NORMAL OPERATION.

Figure 3-7
Unfastening the Strand Mounting Clamps on the APU

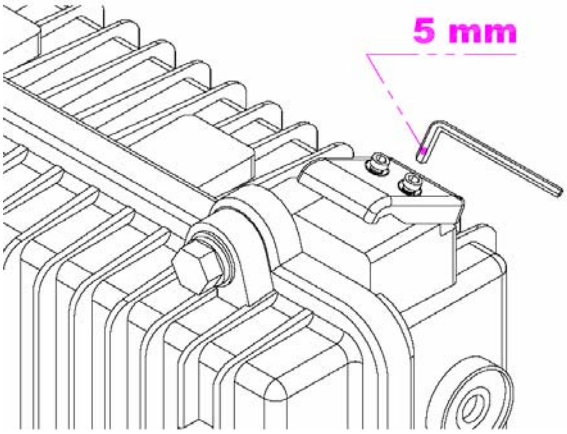
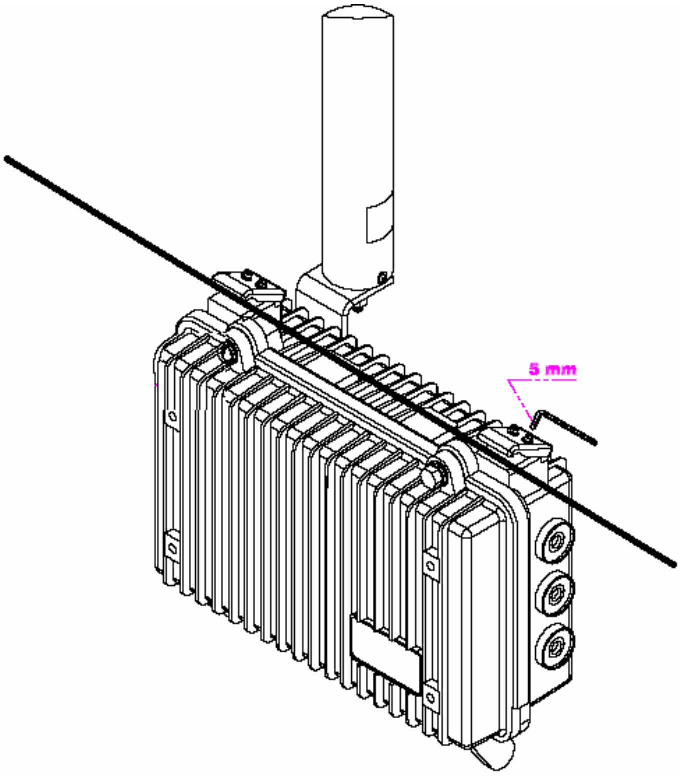


Figure 3-8
Mounting the APU on the Strand by tightening the socket cap screw bolt



Procedure 1-4

Constructing Coaxial Cable and Connecting to the APU

Common Procedure

1. Prior to installation, choose a coaxial cable type:
   - Trunk & Distribution Cable and Connectors : “.500 series”
   - Drop Cable and Connector : “F-type RG-59/6”

Note: The APU standard cable modem operates within the range of +15 dBmV to -15 dBmV. Trunk Cable connection (Hard-line) which may introduce RF power levels higher than 15 dBmV must have external device to attenuate the power being inserted into APU.

A. Perform installation of the coaxial cable as below.

Action

Trunk Cable Connection

Step Action

1. Prepare “.500 series Coaxial Cable”, GRS Type connector and all required Tools for Terminator, Coring, Jacket stripper and Compression.

Figure 3-9
Trunk and Distribution Cable

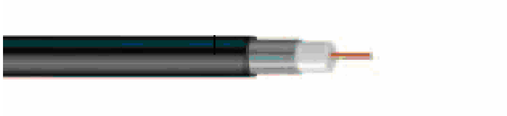
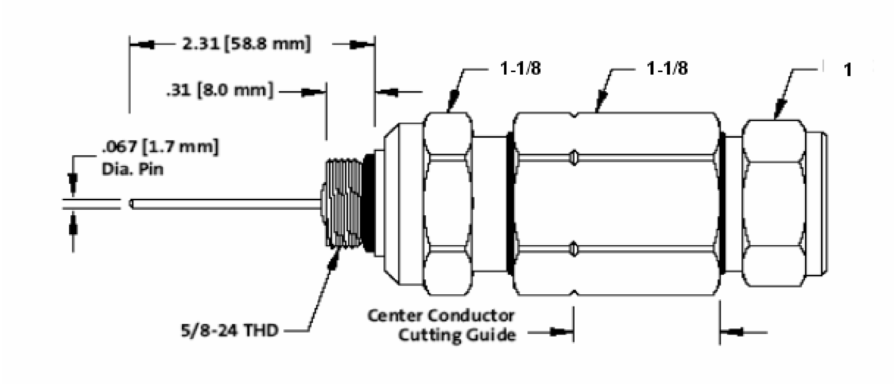


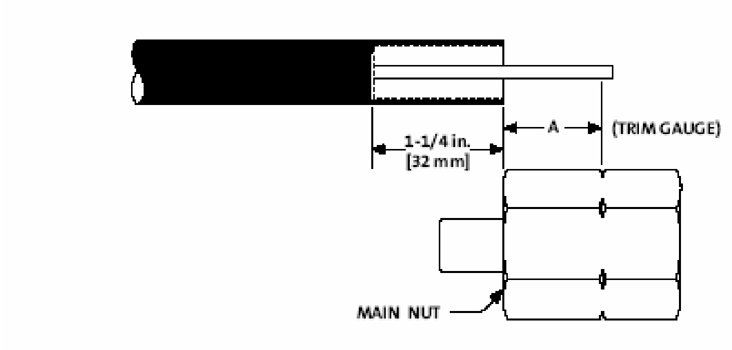
Figure 3-10
Trunk Cable Design



2. Remove the outer jacket/armor to expose the inner jacket, noting that the removal of the outer jacket must be completed without scoring the inner jacket.

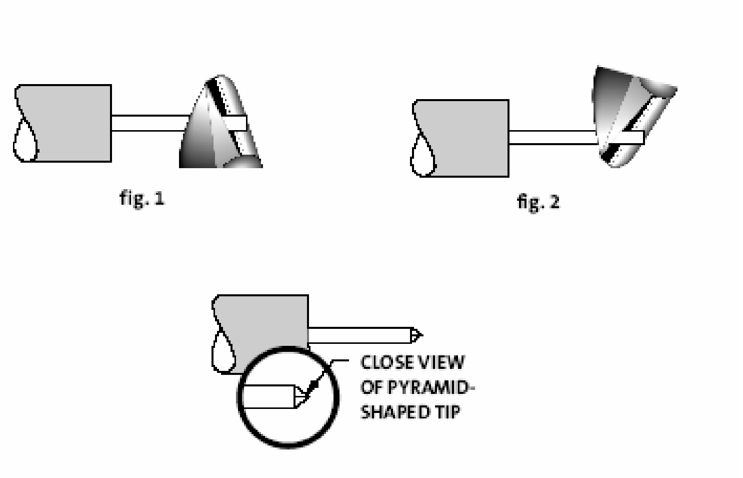
3. Using the built-in trim gauge, verify the center conductor, trim length(15/16 inch: 24mm) and remove the dielectric to a depth of 1 1/4 inch(32mm) from the end of the outer conductor.

Figure 3-11
Constructing Trunk and Distribution Coaxial Cable



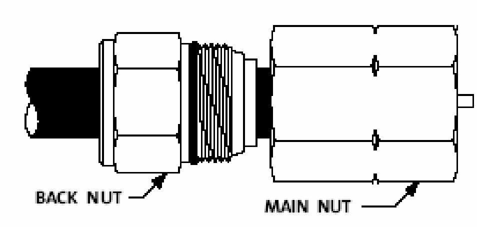
4. After all dielectric and pre-coats have been removed from the center conductor, re-check the center conductor length and trim accordingly.

Figure 3-12
Shading the tip of the center conductor



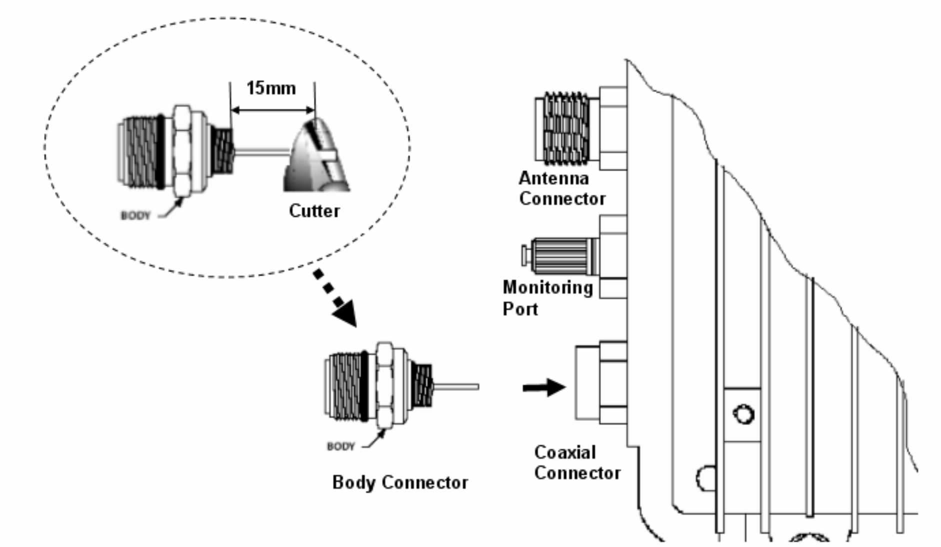
5. Make a cut halfway though and rotate the cutters 90° and complete the cut.
6. Slide the heat shrink tubing over the cable.
7. Remove the outer jacket to a length of ½” (12.7mm).
8. Install the back nut into the cable.
9. Remove and clean flooding material.
10. Install the main nut onto the cable, as a final check on both coring depth and center conductor length. The center conductor will protrude 1/16” to 1/8” past the end of the main nut.
11. Ensure that the cable is fully inserted into the connector so that the jacket butts up against the outer conductor seizing mechanism.

Figure 3-13
Combining Back Nut with Main Nut



12. In order to prevent damage to the connector on the APU enclosure, cut the pin of the Body connector to the length of 0.59” (15mm) with a cutting tool.
13. Install the Body connector to the enclosure and tighten firmly.

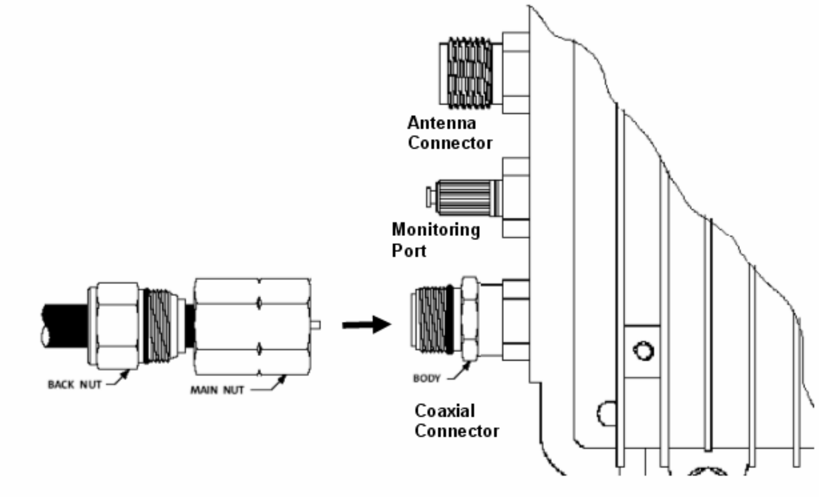
Figure 3-14
Adjusting the length of the center conductor



ENSURE THAT THE PIN LENGTH OF THE BODY CONNECTOR DOES NOT EXCEED 15mm (0.59055 inch) TO PREVENT DAMAGE TO THE JOINT PORTION OF THE HFC FILTER IN THE ENCLOSURE

14. Bring the main nut and cable to the body connector. Hand-tighten the main nut to the body continually keeping pressure on cable towards the body so that the center conductor will be properly seized.
15. Using two wrenches, use one wrench to hold the BODY from rotation and the other to continue tightening the main nut to the body until a firm stop is reached.
16. Tighten the back nut by hand, and by using two wrenches, one on the main nut, complete the installation by tightening the back nut firmly to secure the cable (approximately 35 lbs, ft).
17. Secure the center conductor into the equipment enclosure with the seizing screw.

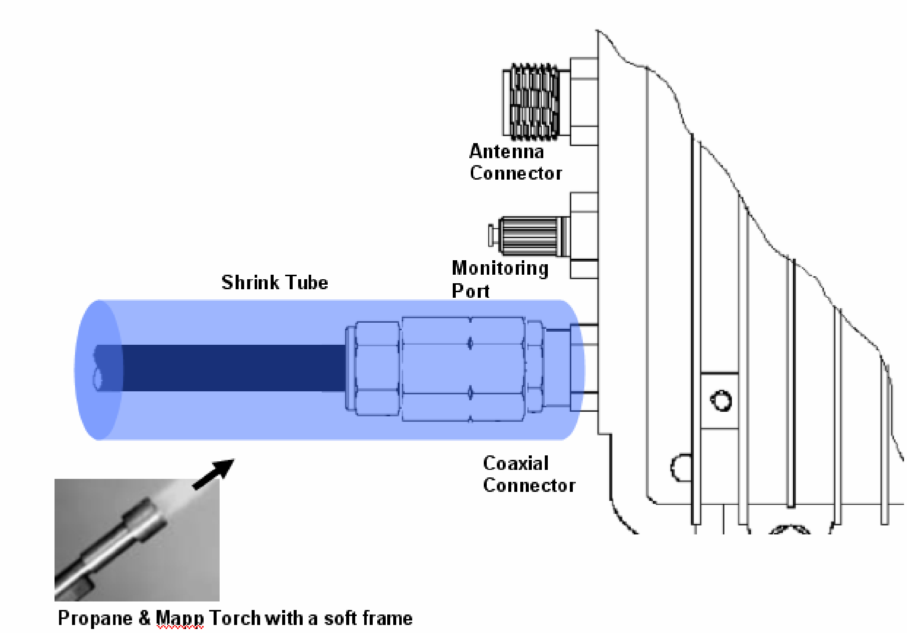
Figure 3-15
Connecting the main connector module to the connector port



ENSURE THAT THE POWER SOURCE IS TURNED OFF PRIOR TO CONNECTING COAXIAL CABLE (75 ohm) TO PROTECT FROM ELECTRICAL SHOCK

18. Slide the heat shrink tubing over the connector against the APU.
19. Shrink the tubing with a painting motion not concentrating on any one area using a propane torch with a broad "soft" frame.

Figure 3-16
Shrinking the tubing to Water Proof

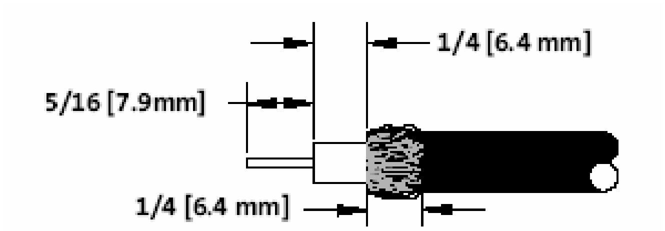


Drop Cable Connection

Step Action

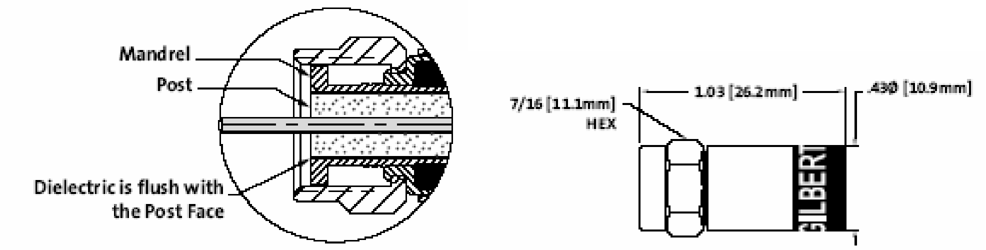
1. Prepare “F series Coaxial Cable”, connector and all required Tools for Terminator, Coring, Jacket stripper and Compression
2. Remove the outer jacket/armor to expose the inner cable. Fold exposed braid back over jacket. Leave foil attached to dielectric.

Figure 3-17
Drop Cable

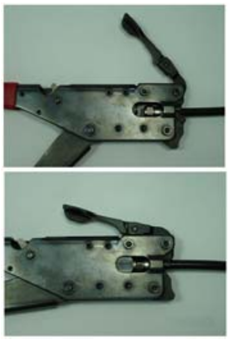


3. Push connector onto the cable until the cable dielectric is flush with the connector post face. Approximately 1/4 inch (6.4mm) of center conductor will protrude beyond the end of the connector nut.

Figure 3-18
Drop Connector Design

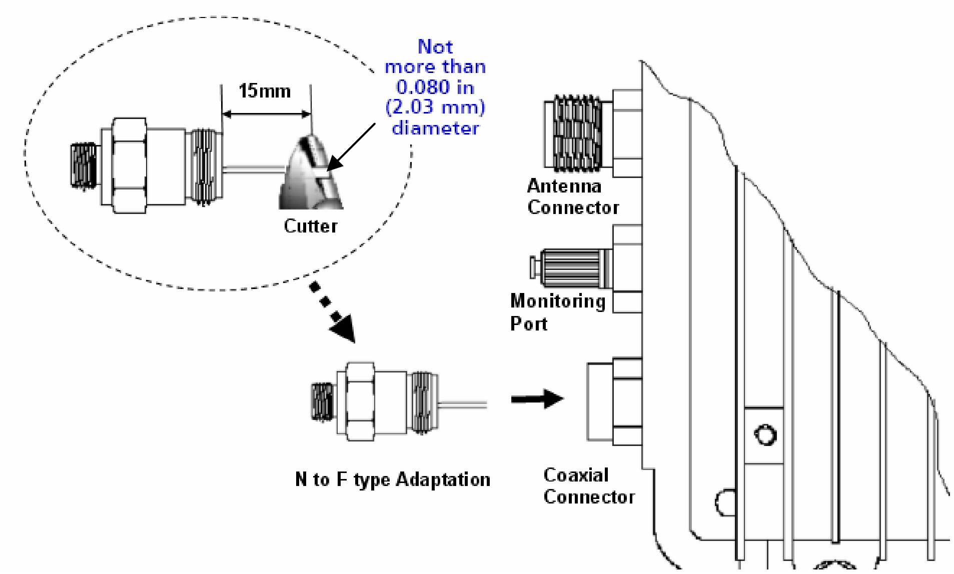


4. Slightly angle the connector/cable and insert into the compression tool area between the plunger tip and the cable gate allowing the center conductor to enter the center conductor guide. Push the cable into the cable gate. Compress the connector by squeezing the tool handles together until a positive stop is reached.



5. Remove the connector/cable from the tool by opening the cable gate to release the assembly from the tool.
In order to prevent damage to the connector on APU enclosure, cut the pin of N to F type adapter to the length of 0.59inch (15mm) with a cutting tool

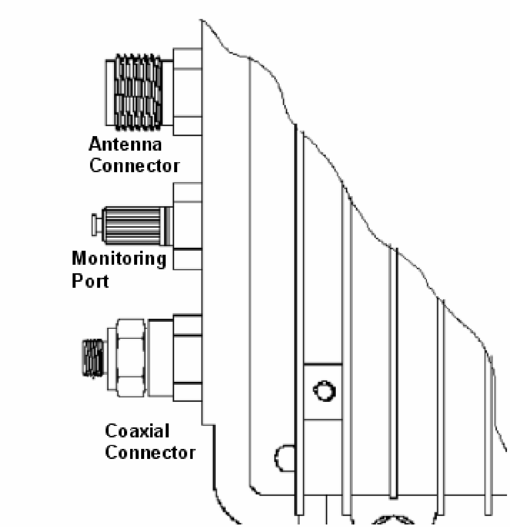
Figure 3-19
Adjusting the length of the center conductor



⚠	**ENSURE THAT THE PIN LENGTH OF THE ADAPTATION CONNECTOR DOES NOT EXCEED 15mm (0.59055 inch) TO PREVENT DAMAGE TO THE HFC FILTER JOINT PORTION IN THE UNIT.**

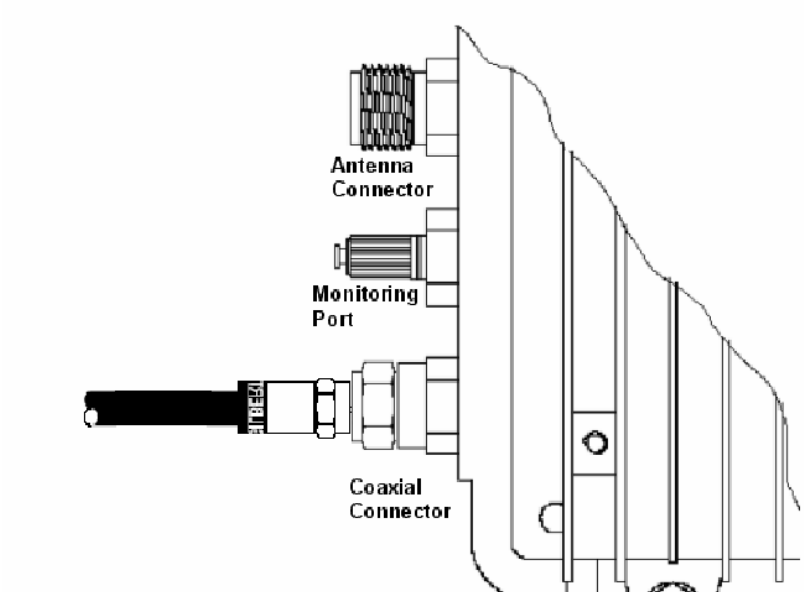
6. Install the N to F type Adapter to the enclosure and tighten firmly

Figure 3-20
Connecting the N to F type Adapter to the enclosure



7. Connect a coaxial cable to the F-connector port and fasten enough to prevent a water intrusion into the gap between connectors.

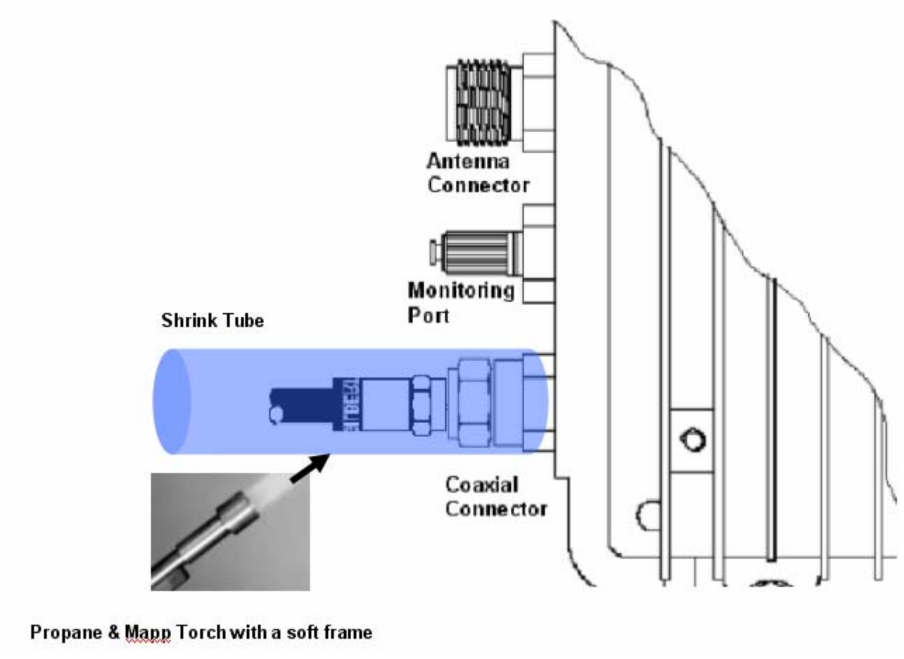
Figure 3-21
Connecting the coaxial cable to the connector port



ENSURE THAT THE POWER SOURCE IS TURNED OFF PRIOR TO CONNECTING COAXIAL CABLE (75 ohm) TO PROTECT AN INSTALLER FROM ELECTRICAL SHOCK

8. Slide the heat shrink tubing over the connector against the APU.
9. Shrink the tubing with a painting motion not concentrating on any one area using a propane/Mapp torch with a broad “soft” frame.

Figure 3-22
Shrink the tubing to Water Proof



Procedure 1-5
Grounding APU enclosure

Action

Step	Action

1. Loosen the grounding bolt and wind the end of the ground wire around the bolt.
2. Fasten the bolt and the ground wire to the earth by connecting them to the earth facility.

Figure 3-23
Assembling the grounding bolt and wire

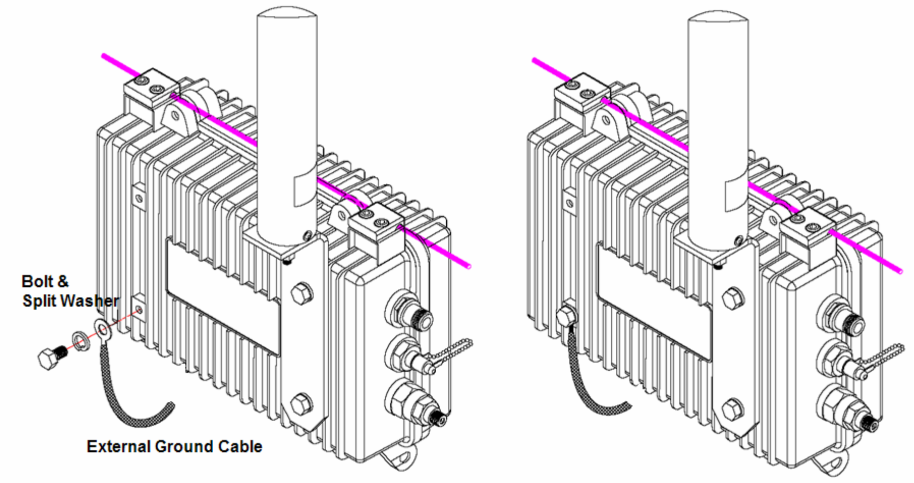
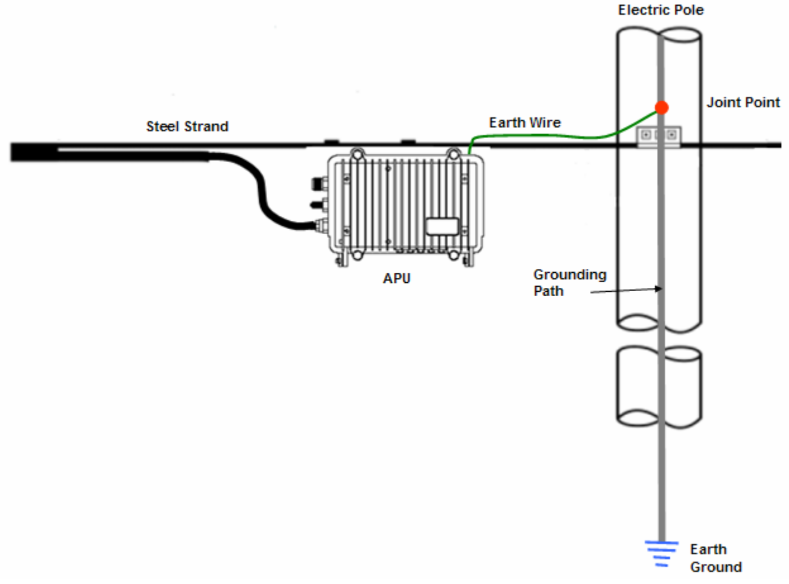


Figure 3-24
Concept diagram of APU enclosure grounding



Procedure 1-6
Checking CATV Signal and Power Level and Tuning

Action

Step Action

1. Connect an actual coaxial cable to the coaxial port on the APU.
2. Connect a measurement coaxial cable to the monitoring port on the APU.
3. Measure the Signal Power level at monitoring port.

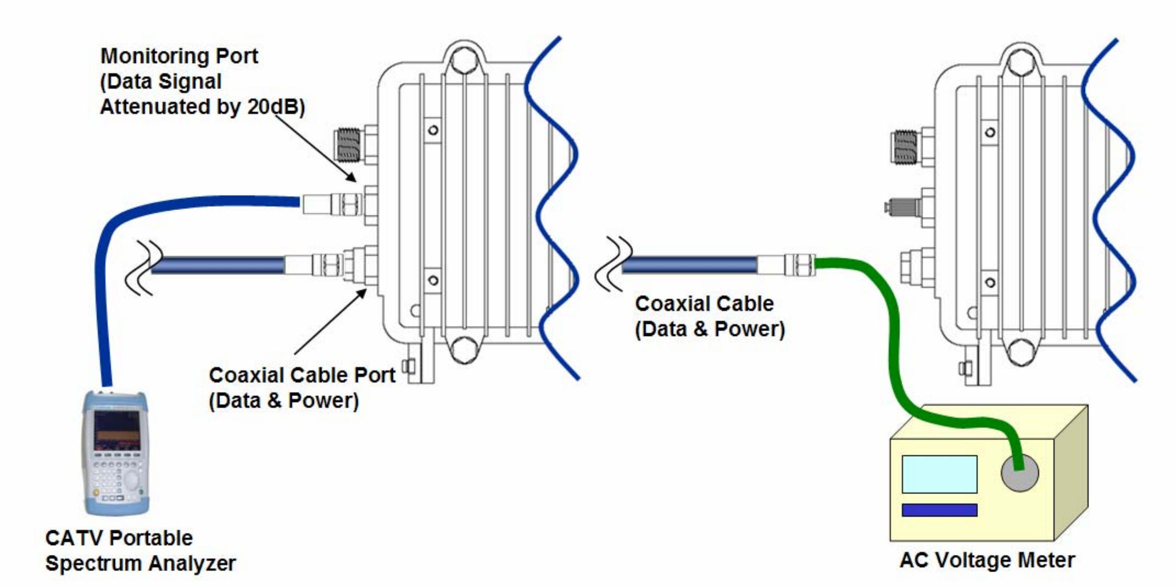
Note: In case of installation using a Trunk or Distribution Cable & Connector, it is crucially recommended to measure the RF Signal level directly at the termination of the coaxial cable from CATV AMP(TBA) or Splitter before connecting to APU in order to ensure a perfect operation of Cable Modem inside APU.

If the measured Signal level is outside from the allowed range referred in DOCSIS, you should adjust the AMP Power level or perform another proper tuning method to meet the requirement of RF signal level.
It is also recommended to measure AC voltage from CATV UPS Power Supply to ensure a perfect operation.

Note: In case of installation using a Drop Cable, it is recommended to measure the AC voltage from Local CATV Power Supply to ensure a perfect operation. But if you can confirm that a power supply facility is compliant to the power requirement of APU, this step can be skipped

4. Check if the acquired power level converted by adding 20dBmV to monitored value satisfy the range (-15dBmV ~ +15dBmV) referred in DOCSIS standard. But, some level margin should be added to the measured power level by 1 ~ 3 dB.

Figure 3-25
Measuring the Power Level at the Monitoring Port



Acceptable Signal Levels

HFC Signal level (DOCSIS 1.1 ~ 2.0 Standard)
+ Standard Signal level (Actual Value): - 15dBmV ~ 15dBmV
+ Calculated Signal level at Monitoring Port (Downstream): - 35dBmV ~ -5dBmV
+ Effective Signal level at Monitoring Port (Downstream): - 37dBmV ~ -7dBmV
HFC AC Power level (Square wave): 45 VAC ~ 95VAC (Recommended level: 63Vac)

Procedure 1-7
Power ON and Visual Checking the LED Operation

Action

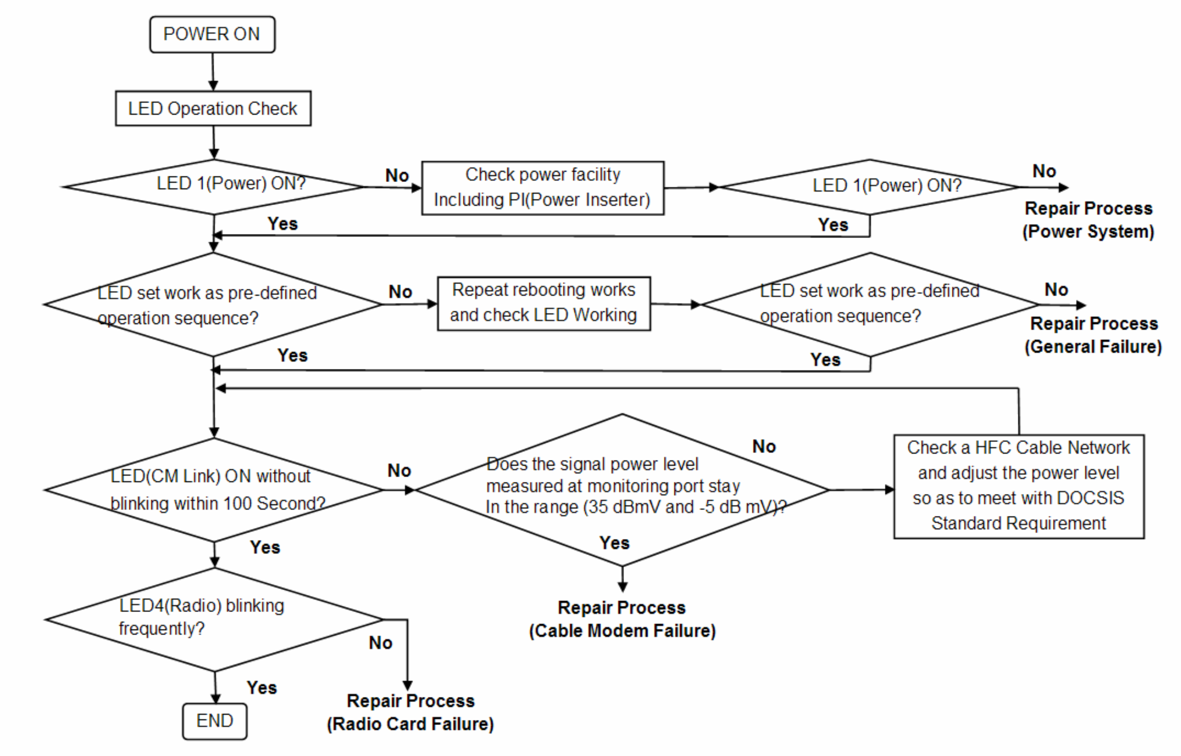
Step Action

1. Ensure that you know what each one of LED Lights means for the unit. Please refer to the LED indicators page.
2. Turn ON the HFC Power Supply.
3. Check if the LED operation follows the pre-defined steps during and after booting.
4. Refer to the System Failure Analysis Procedure on the next page
5. Check if the LED 1(Power) is ON.

Note: If there is no LED light, check if the power supply which provides the CATV (HFC) network with AC power (45 ~ 95VAC) signal is working properly and that the CATV power is detected at the end of the coaxial cable. (If any problem has been found in the power system, the unit has to be entered into a Repair Process)

6. Check if LED 2 (CM Link) flashes for over 100 seconds from when power is first supplied.
   If the LED flashes for more than 100 seconds, check if the data signal level at the monitoring port on the APU meets the recommended range of the signal level.

Figure 3-26
LED Visual Checking Procedure


POWER ON
LED Operation Check
LED 1(Power) ON?
No
Check power facility Including PI(Power Inserter)
LED 1(Power) ON?
No
Repair Process (Power System)
Yes
Yes
LED set work as pre-defined operation sequence?
No
Repeat rebooting works and check LED Working
LED set work as pre-defined operation sequence?
No
Repair Process (General Failure)
Yes
Yes
LED(CM Link) ON without blinking within 100 Second?
No
Does the signal power level measured at monitoring port stay In the range (35 dBmV and -5 dB mV)?
No
Check a HFC Cable Network and adjust the power level so as to meet with DOCSIS Standard Requirement
Yes
Yes
Repair Process (Cable Modem Failure)
LED4(Radio) blinking frequently?
No
Yes
END
Repair Process (Radio Card Failure)

CSU Installation & Configuration

Mounting and Installation Concept

Figure 3-1
CSU Installation Concept #1 on User's facility

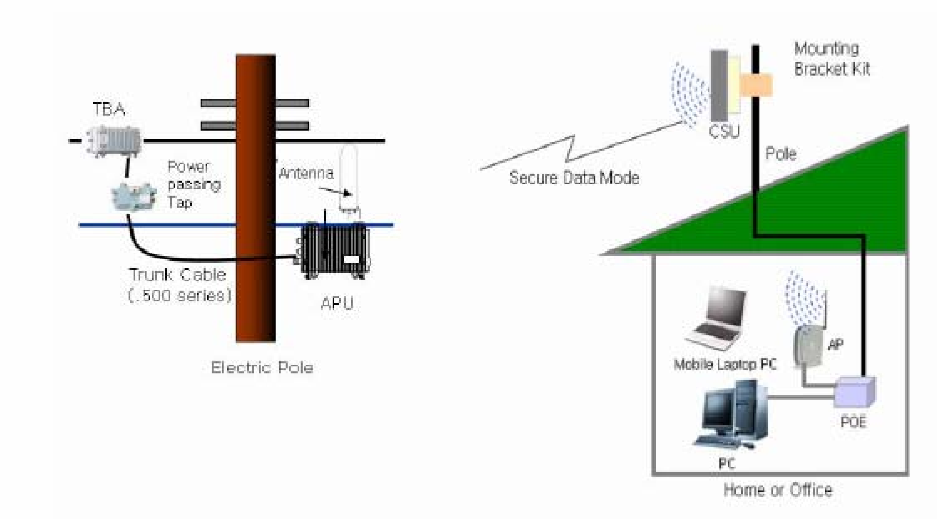
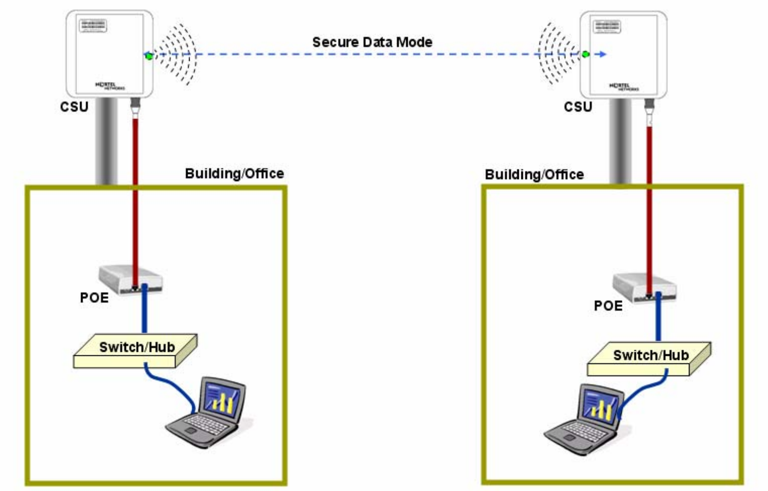


Figure 3-2
CSU Installation Concept #2 on User's facility



By default, CSU is pole mounted. Each unit is shipped with a pole mounting module.

ENSURE THE CSU HAS BEEN POSITIONED NO LESS THAN 3 FEET ABOVE THE GROUND, OR FROM A ROUGHLY HORIZONTAL SURFACE.

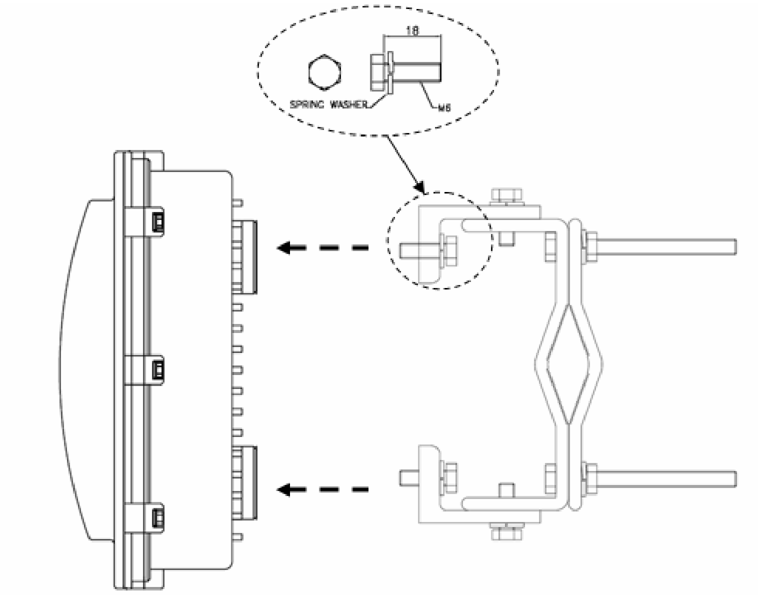
Procedure 2-1
Mounting the CSU on the Steel Wire Strand

Action

Step Action

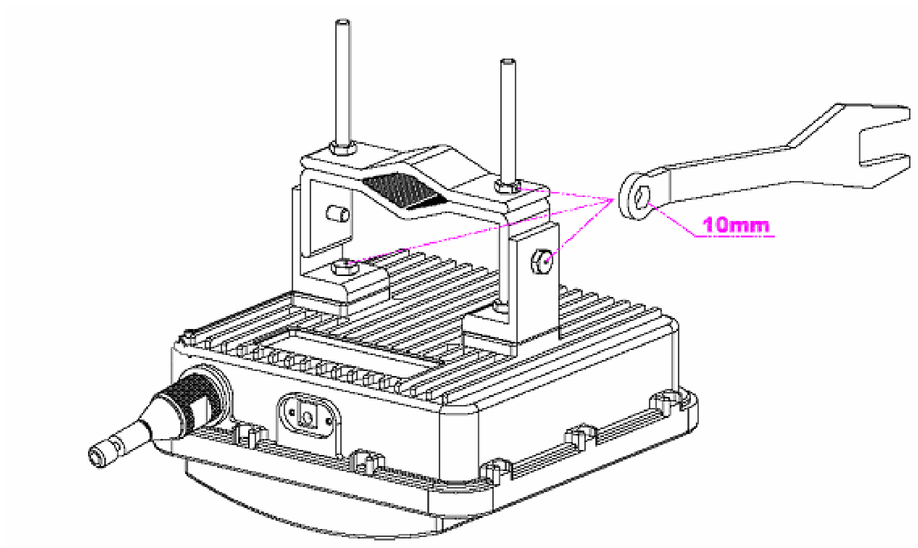
1. Prior to an installation, check if the Pole has the strength and stability to sustain the weight of CSU in a strong wind
2. Please find a mounting tool for installing CSU illustrated in Figure 3-30
3. Place the CSU face (RADOME side) down on a flat surface.
4. Using the mounting tool, attach the Mounting Tilt Brackets to the back of CSU and insert the two stainless steel M6 hex head screws and M6 split lock washers into the hole.

Figure 3-3
Assembling the mounting bracket on the CSU



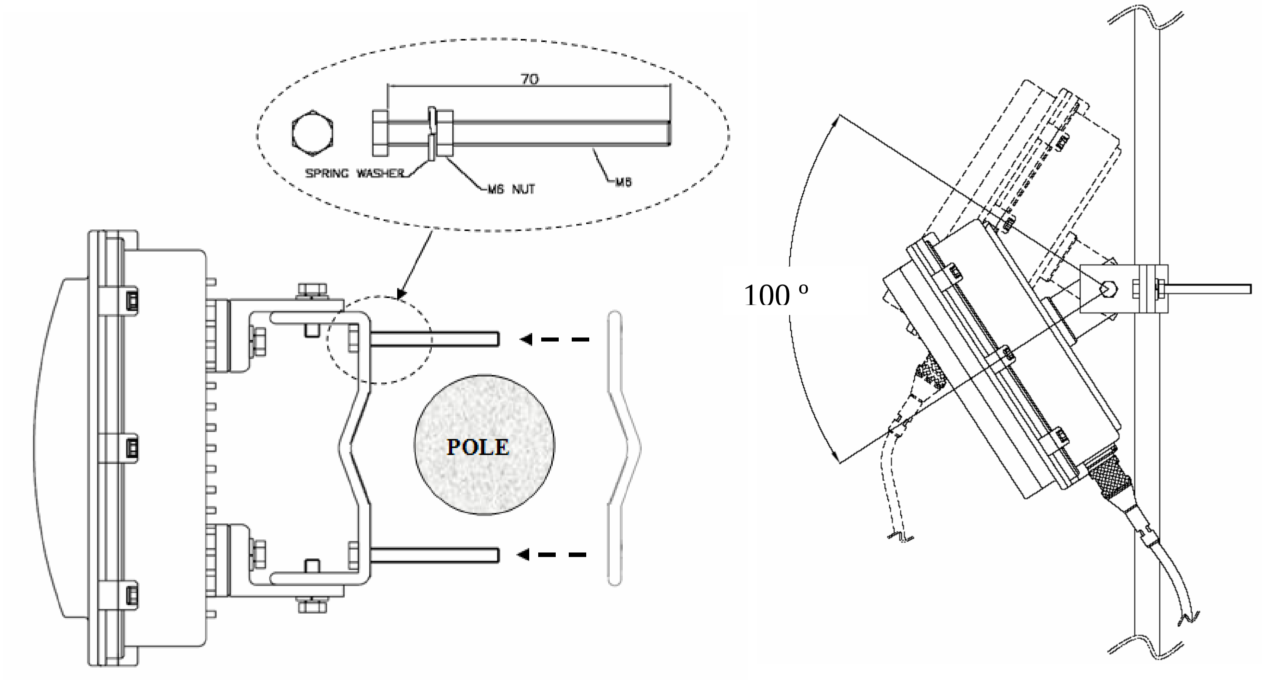
5. Lift the CSU to a selected installation point on the pole and then attach the clamp to the original location while lashing the CSU to the pole or using a hoisting rope to keep the unit in place during mounting work.
6. Slide two mounting nuts through a washer to each bracket hole as illustrated in Figure 3-3
7. Adjust the azimuth of CSU Antenna RADOME toward the remote unit and fasten sufficiently to secure the CSU on the pole.

Figure 3-4
Assembling the mounting bracket with a installation tool



8. Adjust the up/down tilt (- 50 º to 50 º) and move the top or bottom of the CSU until the unit is roughly positioned at the correct angle and height.

Figure 3-5
CSU Pole Mounting and Antenna Tilting



Procedure 2-2

Mounting the CSU on the Steel Wire Strand

Action

Step Action

1. Loosen the EMI cap and slide the CAT5 or 6 cables without the RJ45 connector into the hole of the EMI hood shaped cap.

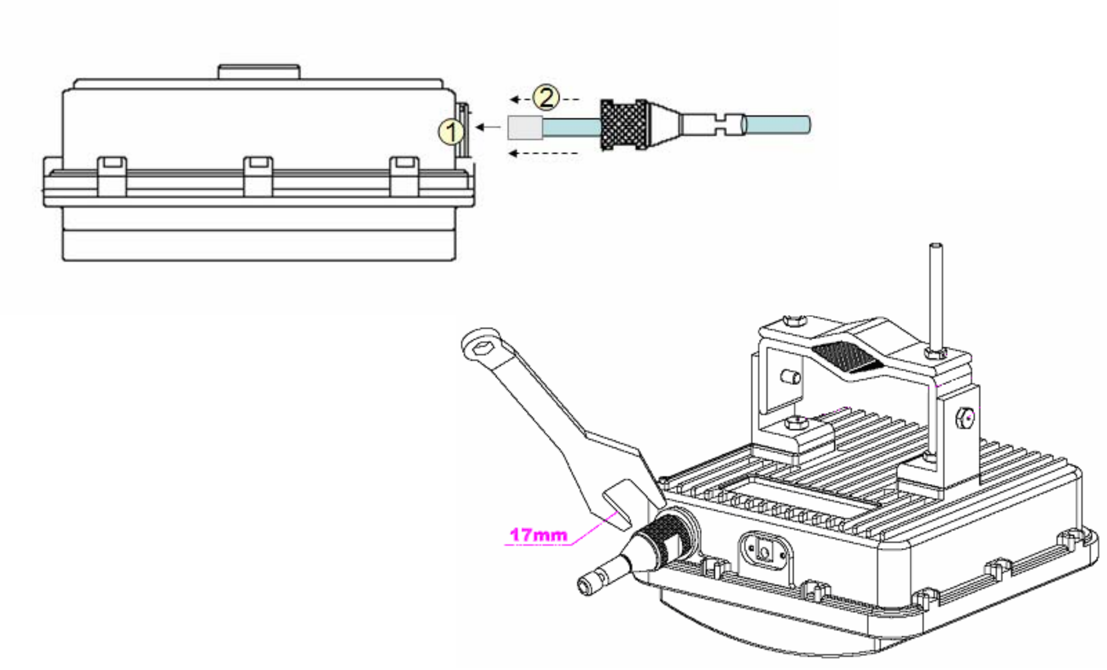
Follow the conventional procedure of creating a CAT5 or 6 Ethernet cable.

Note: It is recommended to use a shielded cable like S-FTP(Foiled Twisted Pair) or STP (Shielded Twisted Pair) in which wire pairs are covered with overall shield material to prevent EMI effects to or from the near electronic devices or facilities.

Note: The cable from CSU to POE Injector and from POE Injector to CPE (PC) should be a straight-through cable.

2. Connect a cable to the POE port on the front panel of CSU through the hole of EMI cap and tighten it firmly.

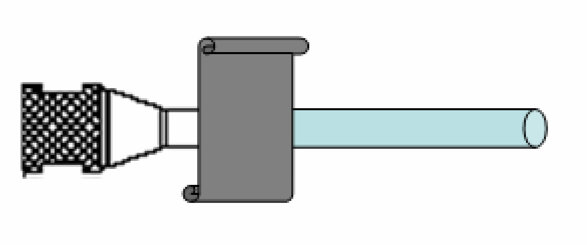
Figure 3-6
Connecting Ethernet Cable to CSU and Securing the EMI Cap



3. Secure the cable in the EMI cap by tightening it with a cable tie. Cover the connectors with black self amalgamating tape or shrink wrap tubing to ensure a waterproof seal. This is the most crucial step in the installation. If this procedure is disregarded or done insufficiently an unexpected system fault could occur in a normal operation and affect on the system performance factor relevant to the long term reliability.
4. Tighten the EMI cap securely with the special tool packaged in the product box.

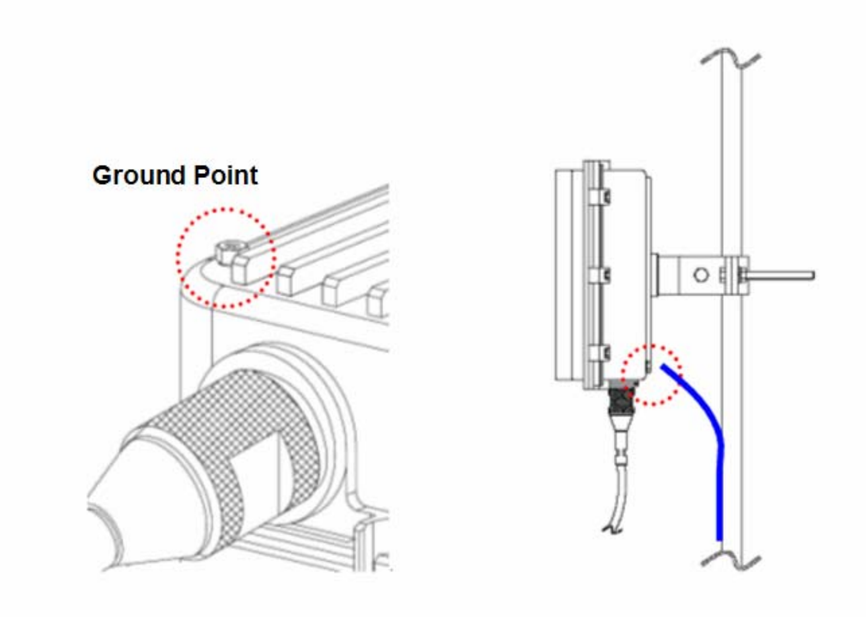
WHEN INSTALLING THE UNIT, CHOOSE A LOCATION THAT PROVIDES A MINIMUM SEPARATION OF 20 cm FROM ALL PERSONS DURING NORMAL OPERATION.

Figure 3-7
Covering the entry of EMI Cap and Shielded Cable with Tape or shrink wrap tubing



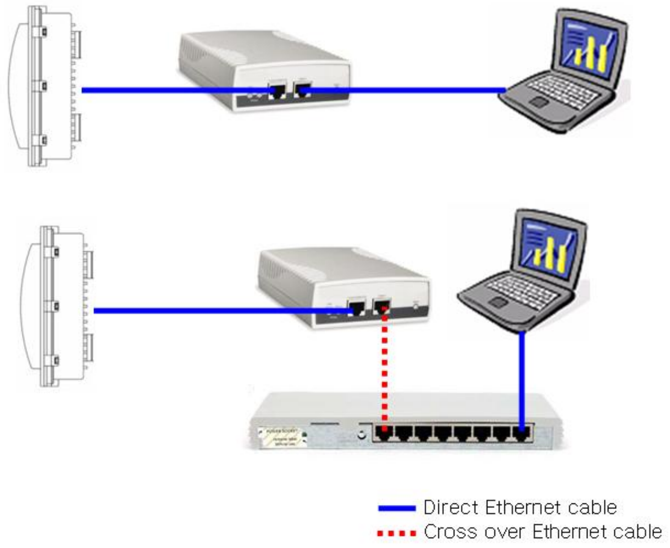
5. Connect the ground wire to the ground point at the lower right end of CSU back panel.

Figure 3-8
Connecting the ground wire to the ground point



6. Connect the other end of the data cable to the POE Injector indoor.
7. Plug the power cord of the POE Injector into an electrical outlet

Figure 3-9
Connecting CSU and User PC by an Ethernet Cable though POE Injector



Mounting Tips

- Verify the Line-of-Sight -- Before installing CSU, make sure a clear line-of-sight exists. Line of sight (LOS) can be defined as each antenna clearly seeing the other antenna, and seeing the remote locations when viewing from the central base location. Be sure to look level with the center of origin of the transmission (i.e., the middle of the antenna). Repeat this procedure from the remote location. Any disruption of the signal path due to trees, buildings, or any other obstructions may cause the link to function incorrectly. If you see any obstructions between two antennas, move one or both antennas to another location.
- Use mounting hardware provided to secure the unit to the pole.
- Leave the unit mounting loose enough to allow for movement when performing the alignment/testing procedure. The unit should be tightened only after the alignment/testing procedure is completed.
- Install the unit away from microwave ovens and 2.4 GHz cordless phones. Microwave ovens and some cordless phones operate on the same frequency as the unit and can cause signal interference.
- Begin at the lowest point, so the tape overlaps from bottom to top creating a shingled effect. This creates an effective barrier against water runoff. Apply this "shingle effect" to each layer of the sealing process. Apply two layers of electrical tape to the connector, and leave approximately 3 inches of cable exposed on either side of the connector.

Configuration

WLAN Cable Access Point 6220 CSU (APU, CSU) has the following management and operational features listed below:

Software Installation

APU-APU mode Basic Configuration and Operation Test

CSU-APU mode Basic Configuration and Operation Test

CSU-CSU mode Basic Configuration and Operation Test

Testing the connection between APU & CSU (APU mode) and CSU

Testing Wireless Network Performance

Basic Configuration

Advanced and Optional Configuration

Software Installation (AP Configurator)

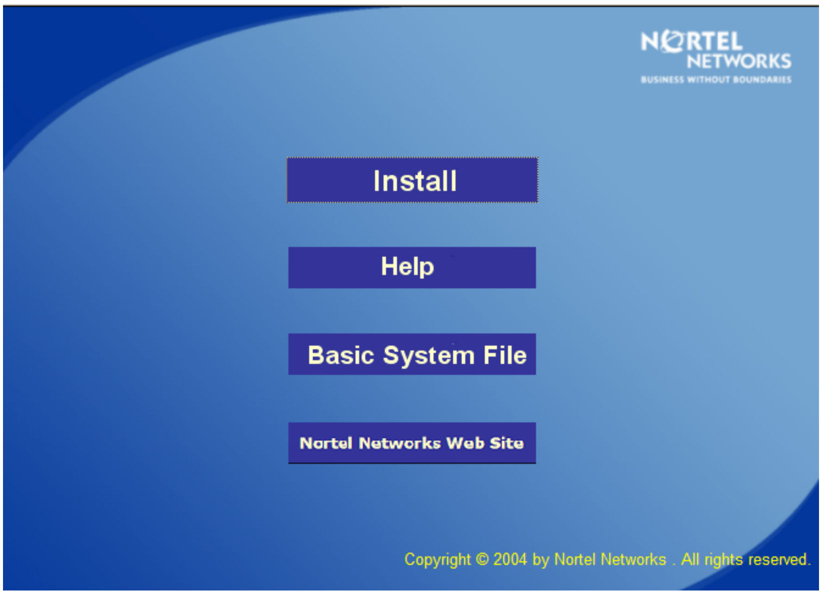
The WLAN Cable AP Configurator is used to configure your wireless networking devices. Both the executable file needed to install the Configurator and the online help for the Configurator (*.chm) are included on the Software CD that you received with your hardware device. Refer to the online help or the WLAN Cable AP Configuration User Guide on the Document CD for detailed instructions on how to configure your device. This section explains the system configuration in detail.

Note: The features available to you in the WLAN Cable AP Configuration vary depending on the version of the software. This section explains all possible features involved in basic configuration. Your actual software may not display all of the features and fields described.

Installing the Configurator Software

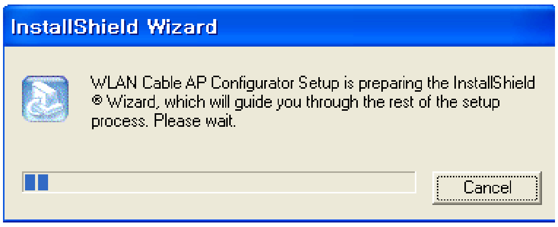
1. Insert the Software CD into your PC's/laptop's CD ROM drive, then you can see the installation web page as below.

Figure 4-1
Software CD Starting Display


NORTEL NETWORKS
BUSINESS WITHOUT BOUNDARIES
Install
Help
Basic System File
Nortel Networks Web Site
Copyright © 2004 by Nortel Networks . All rights reserved.

2. Click the "Install" button and press the "open" button to find the dialog box.
3. Double click the name of the Configurator Installation program (the .exe file on your Software CD).

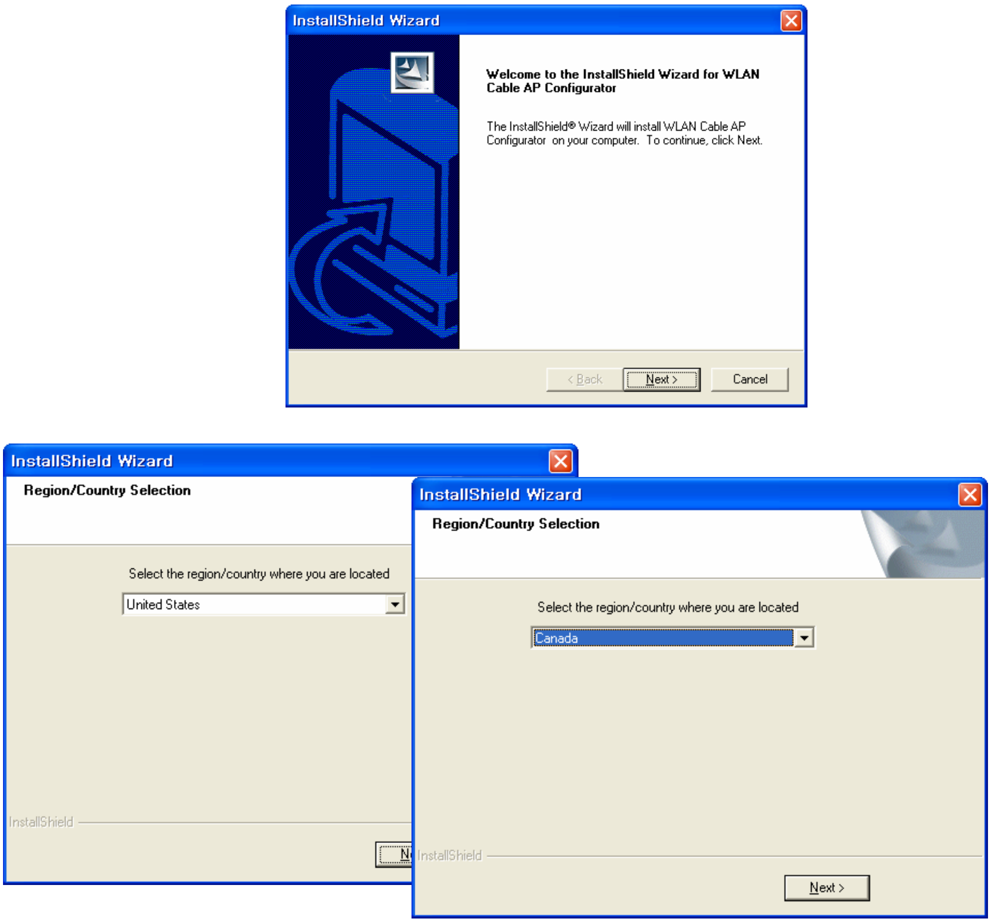
Figure 4-2
Software Installation Launching



WLAN Cable AP Configurator Setup is preparing the InstallShield ® Wizard, which will guide you through the rest of the setup process. Please wait.

3. Follow the onscreen instructions to install the Configurator.

Figure 4-3
Installation Dialog Window



Welcome to the InstallShield Wizard for WLAN Cable AP Configurator

The InstallShield® Wizard will install WLAN Cable AP Configurator on your computer. To continue, click Next.

Region/Country Selection

Select the region/country where you are located

United States

Region/Country Selection

Select the region/country where you are located

Canada

If you are installing the Configurator for the first time, files are stored in the directory Program Files/Nortel/WLAN Cable AP Configurator. If you are upgrading from a previous Configurator installation, your files will be stored in the directory where you last saved the Configurator files. The Install Shield also installs shortcuts to the Configurator on your desktop.

Procedure 3-1
Basic configuration and Operation Test (APU-APU Mode)

Action

Step Action

1. The APU(APU mode) has the following factory default parameters:

Factory Default

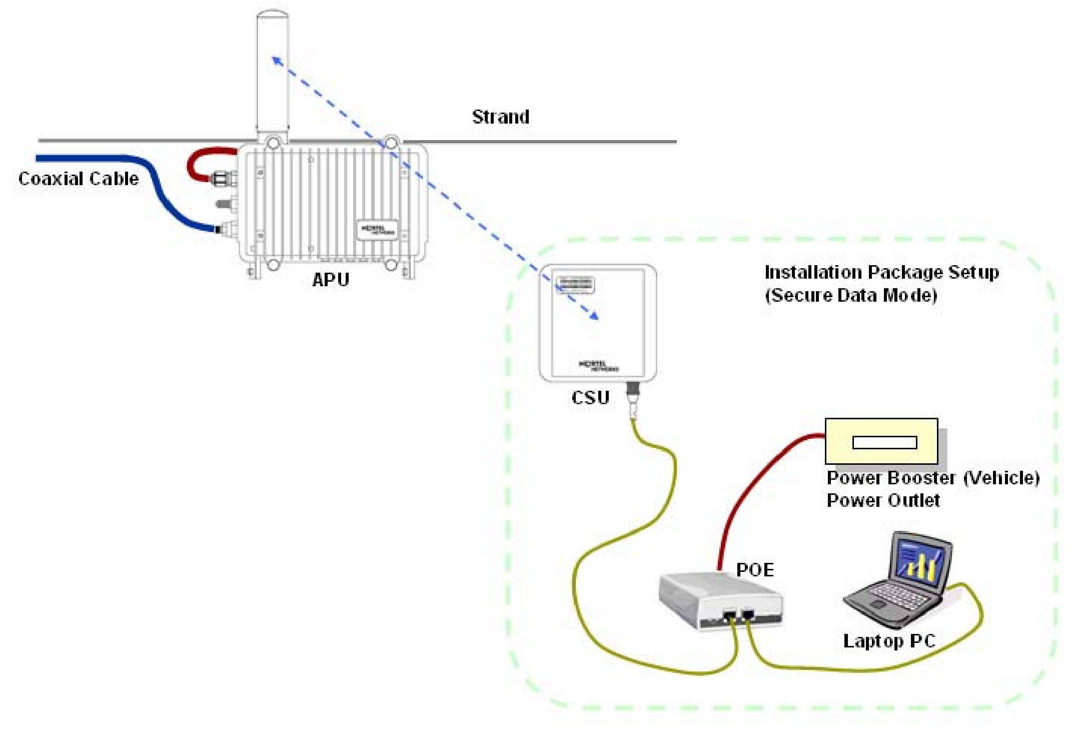
- IP address: DHCP Client (Ethernet 1)
- Read Write Password: public
- SNMP Secure Configuration Password: public
- IEEE 802.11 Interface Setup
  - Mode Selection: APU SDM(Secure Data Mode)
  - Base station mode: Polling (Primary)
  - Frequency
    → 802.11b/g Unit: CH1 (2412 MHz)
    → 802.11a Unit: CH149 (5745 MHz)
  - Network ID: 0
  - Transmit Rate
    → 802.11a/g Unit: 54Mbps
    → 802.11b Unit: 11Mbps
  - WEP Encryption: Disable

2. The CSU (CSU mode) shall have the same system parameters with a factory default parameter of APU to install.

Table 4-1
System Main Parameters

Parameter	APU/CSU(APU mode)	CSU
IP address	DHCP Client	DHCP Client
Read Write Password	Public	Public
SNMP Secure Configuration Password	Public	Public
Mode Selection	APU Secure Data Mode	CSU Secure Data Mode
Base Station Mode	Polling(Primary)	N/A
Frequency	User specific	User specific
Transmit Rate	User specific	User specific
Network ID	0	0
Others	User-specific	User-specific

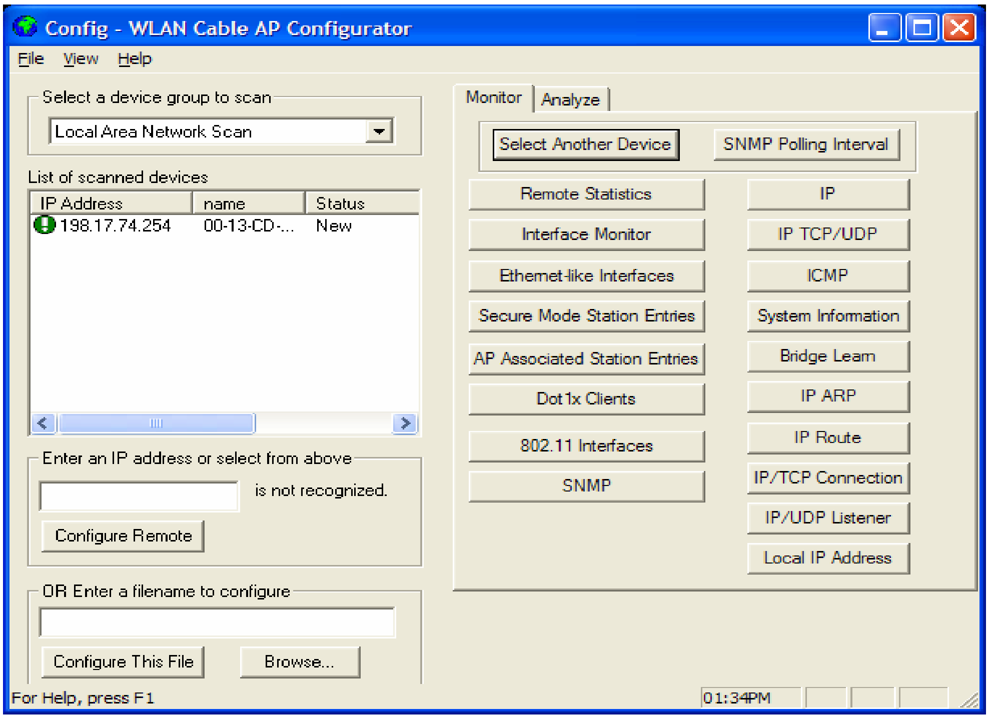
Figure 4-4
Test Network Configuration (Radio Connection)



3. Prepare a Laptop computer and a client unit to test and configure the CSU at the installation location.
4. Connect Laptop PC to CSU Ethernet port with a straight-forward cable to setup.
5. Launch the Configurator by either double clicking the WLAN Cable AP Configurator icon on your desktop or by opening the file config.exe from the directory “C:\Program Files\Nortel\WLAN Cable AP Configurator” where software is installed at.
6. Run the Configurator and the IP Address for your APU (and the IP addresses for any other devices in your network) as appears in the Configurator window below.

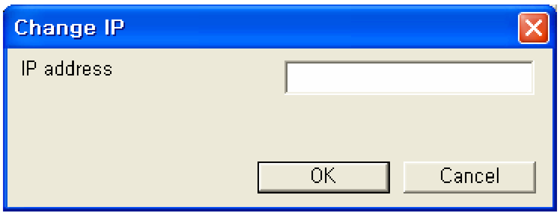
Note: In factory default, APU and CSU have a default IP address as “198.17.74.254” regardless of the software modes (APU, CSU mode), which means that APU and CSU are ready to get it’s IP address from a remote DHCP Server. Therefore, when you launch AP configurator at PC with CSU turned on at first, you can find the default IP address of the CSU showing the green exclamation point “198.17.74.254” in the List of Scanned Devices window. In case that DHCP service is available in the cable network, you can find a new local IP address assigned to the unit from DHCP server in the list box except the default IP address.

Figure 4-5
Configurator Starting Window



7. In case you want to forcibly setup IP address, follow this procedure as below.
8. Right click on the IP address of CSU, and then select ‘Configure This Device’. or click “Configure Remote” button below the list box.
9. The Change IP window is displayed, as shown in the following screenshot.

Figure 4-6
IP setup dialog box

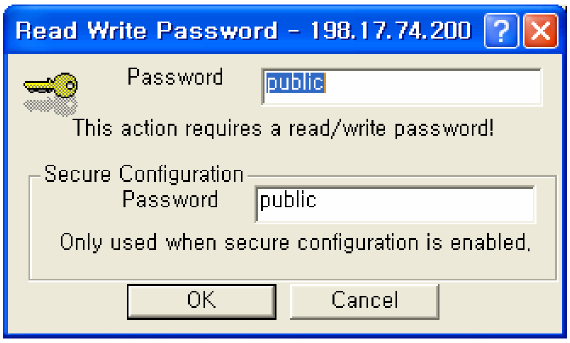


10. Enter an IP address that will be local to the IP of the PC/laptop running the Configurator, and then click the OK button in Read Write Password window.

Note: The IP address to enter should be included in the same subnet area with PC/Laptop computer for access to CSU.
For example, in case the IP address of Laptop computer is 192.168.0.100/24, the CSU will be allowable in 192.168.0.1/24 ~ 192.168.0.254/24 as the IP address subnet group.

11. The SNMP Password dialog box is displayed, as shown below.
12. Press “Enter” key or enter a new password instead of the default password “public” in the basic SNMP password box.

Figure 4-7
SNMP Read Write Password dialog box



Read Write Password - 198.17.74.200

Password: public

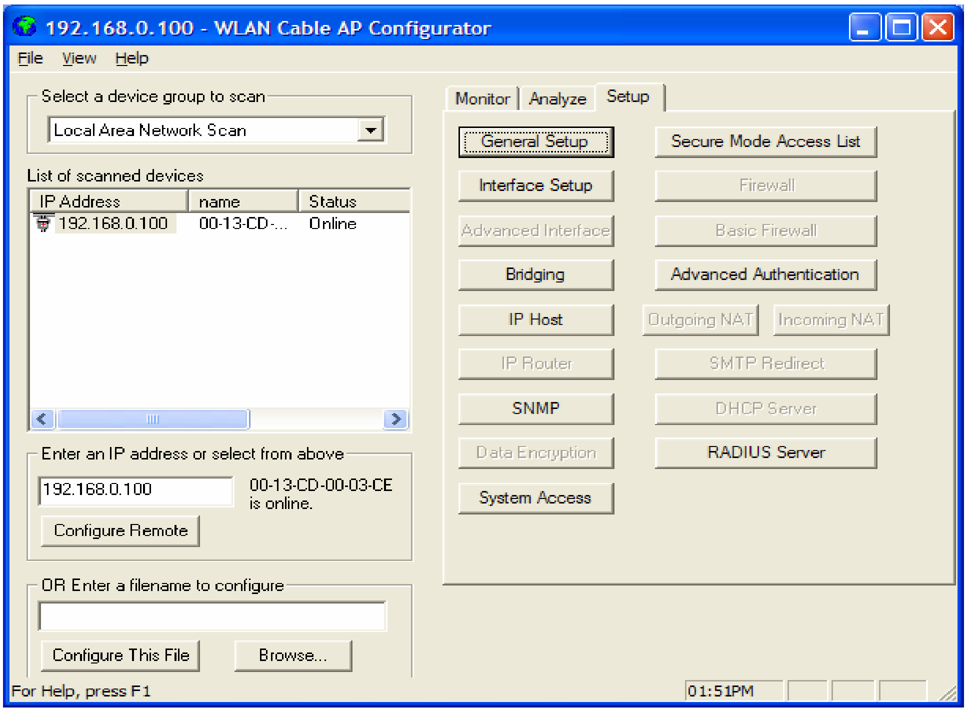
This action requires a read/write password!

Secure Configuration Password: public

Only used when secure configuration is enabled.

13. The main window is redisplayed.
14. To setup the interface, Click on the Interface Setup button.
15. The Interface Setup screen is enabled and displayed, as shown in the Figure 4-9

Figure 4-8
AP Configurator Main window



192.168.0.100 - WLAN Cable AP Configurator

Select a device group to scan: Local Area Network Scan

List of scanned devices

IP Address	name	Status
192.168.0.100	00-13-CD-...	Online

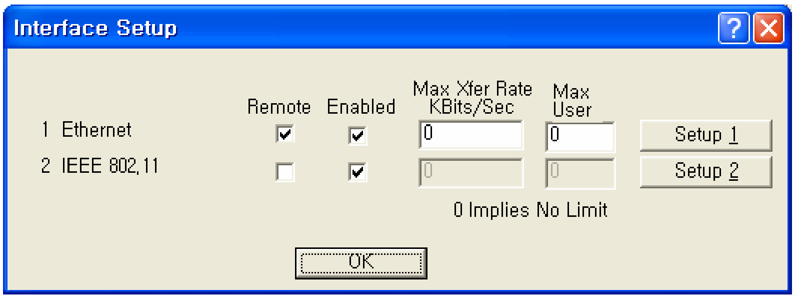
Enter an IP address or select from above: 192.168.0.100

00-13-CD-00-03-CE is online.

For Help, press F1

01:51PM

Figure 4-9
Interface setup dialog box



Interface Setup

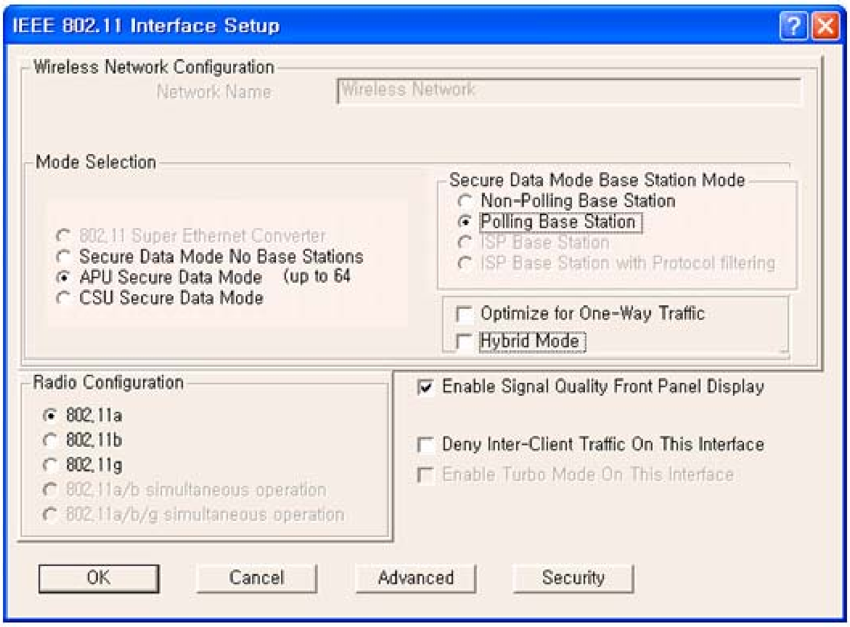
	Remote	Enabled	Max Xfer Rate KBits/Sec	Max User	
1 Ethernet	☑	☑	0	0	Setup 1
2 IEEE 802.11	□	☑	0	0	Setup 2

0 Implies No Limit

OK

16. If you have an 802.11 radio card, click the Setup 2 button to set up the 802.11 interface.
17. Click the Setup 2 button. The IEEE 802.11 Setup screen is displayed, as shown in Figure 4-10.
18. Select a radio standard to use according to the built-in antenna specification like an operating frequency range.
    Ex) 2.4GHz antenna : 802.11b/g, 5.8GHz antenna: 802.11a
19. Make sure the APU Secure Data Mode in the left portion of Mode Selection is selected while “Polling Base station” is clicked in Secure Data Mode Base Station Mode.
20. Select the Enable Signal Quality Front Panel Display checkbox if your unit has a front panel display that is capable of displaying the signal quality.

Figure 4-10
Interface setup dialog box



IEEE 802.11 Interface Setup

Wireless Network Configuration

Network Name: Wireless Network

Mode Selection

○ 802.11 Super Ethernet Converter
○ Secure Data Mode No Base Stations
● APU Secure Data Mode (up to 64
○ CSU Secure Data Mode

Secure Data Mode Base Station Mode

○ Non-Polling Base Station
● Polling Base Station
○ ISP Base Station
○ ISP Base Station with Protocol filtering

□ Optimize for One-Way Traffic
□ Hybrid Mode

Radio Configuration

● 802.11a
○ 802.11b
○ 802.11g
○ 802.11a/b simultaneous operation
○ 802.11a/b/g simultaneous operation

☑ Enable Signal Quality Front Panel Display

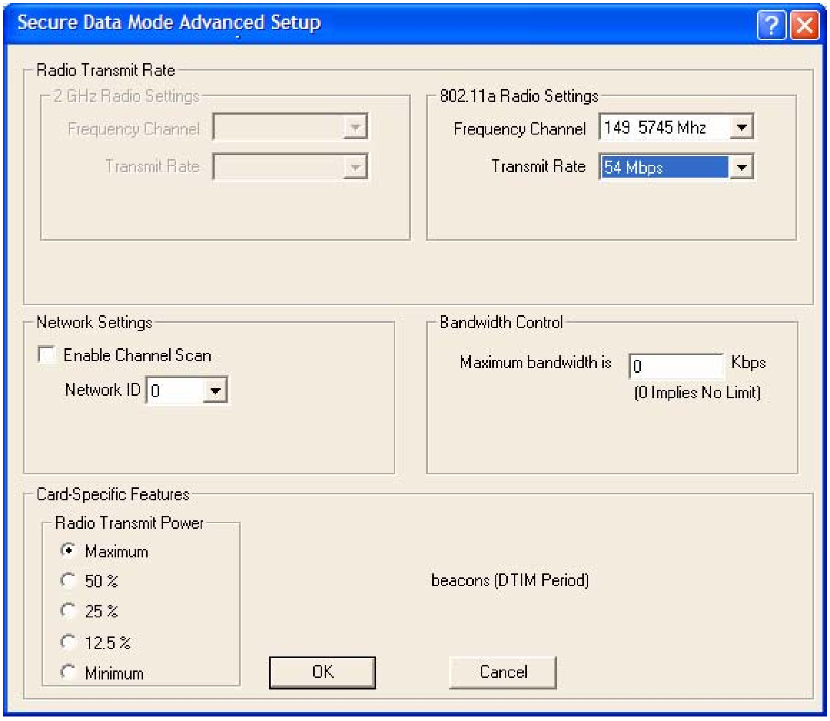
□ Deny Inter-Client Traffic On This Interface
□ Enable Turbo Mode On This Interface

OK Cancel Advanced Security

21. Click on the advanced button to set up crucial parameters such as Radio Frequency, Transmit Rate (Bandwidth) and Network ID.
22. The Advanced Setup screen for a Secure Data Mode is shown below.
23. Setup all radio parameters including a frequency channel and transmit power referring to the permitted setting value specified in the following tables per radio standard.

Figure 4-11
Advanced setup dialog box

[802.11a]



Secure Data Mode Advanced Setup

Radio Transmit Rate

2 GHz Radio Settings
Frequency Channel
Transmit Rate

802.11a Radio Settings
Frequency Channel: 149 5745 Mhz
Transmit Rate: 54 Mbps

Network Settings
□ Enable Channel Scan
Network ID: 0

Bandwidth Control
Maximum bandwidth is 0 Kbps
(0 Implies No Limit)

Card-Specific Features
Radio Transmit Power
● Maximum
○ 50 %
○ 25 %
○ 12.5 %
○ Minimum

beacons (DTIM Period)

Frequency Channel	
149	5745 MHz
153	5765 MHz
157	5785 MHz
161	5805 MHz

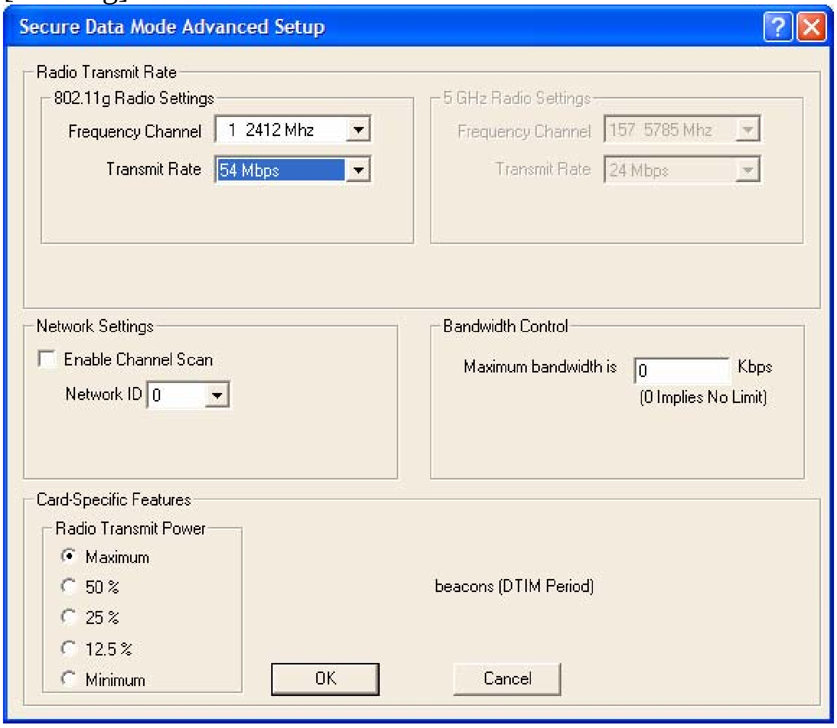
Transmit Rate	
6Mbps	36Mbps
9Mbps	48Mbps
12Mbps	54Mbps
24Mbps	

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(APU/11A): 22dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (22dBi) in case you select 802.11a mode as operation radio standard.

Note: It is recommended that you set the transmit power to “Maximum” as the antennas listed in Appendix C(Antenna) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

[802.11g]



Secure Data Mode Advanced Setup

Radio Transmit Rate

802.11g Radio Settings

Frequency Channel 1 2412 Mhz

Transmit Rate 54 Mbps

5 GHz Radio Settings

Frequency Channel 157 5785 Mhz

Transmit Rate 24 Mbps

Network Settings

□ Enable Channel Scan

Network ID 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

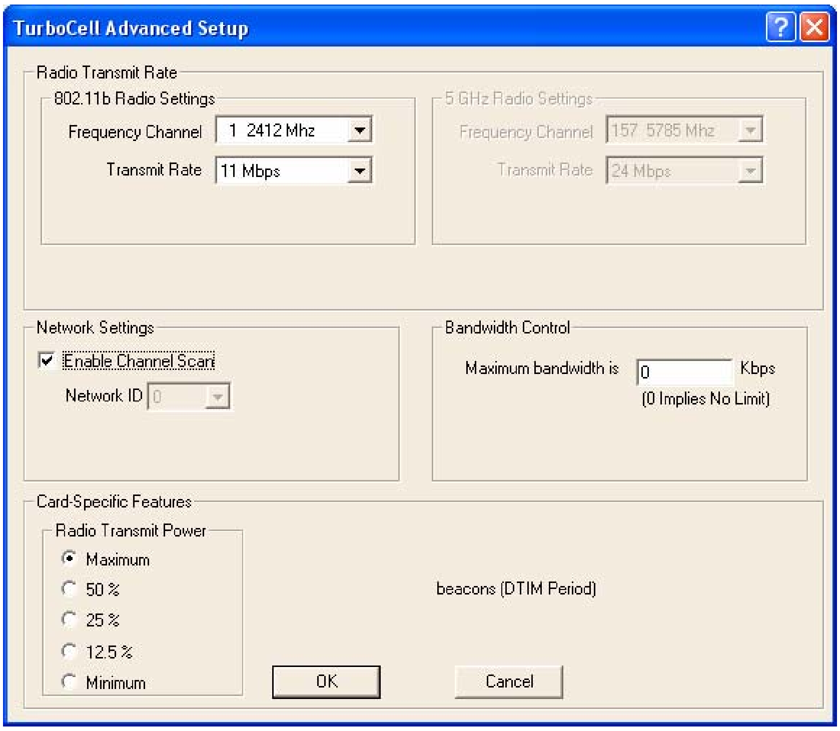
Transmit Rate	
54 Mbps	6 Mbps
48Mbps	11 Mbps
36 Mbps	5.5 Mbps
24 Mbps	2 Mbps
12 Mbps	1 Mbps

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna - Omni-directional: 7dBi - Bi-directional: 9dBi - Flat panel : 14dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum gain per each antenna type in case you select 802.11b/g mode. For example, if you are intended to use omni-directional antenna for APU, it is illegal that you use a similar type of antenna with 14dBi even though the max allowable antenna is up to 14dBi.
Make sure that a gain per antenna type does not exceed the certified value.

Note: It is recommended that you set the transmit power to "Maximum" as the antennas listed in Appendix C(Antenna) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

[802.11b]



TurboCell Advanced Setup

Radio Transmit Rate

802.11b Radio Settings

Frequency Channel: 1 2412 Mhz

Transmit Rate: 11 Mbps

5 GHz Radio Settings

Frequency Channel: 157 5785 Mhz

Transmit Rate: 24 Mbps

Network Settings

☑ Enable Channel Scan

Network ID: 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

Transmit Rate
11 Mbps
5.5 Mbps
2 Mbps
1 Mbps

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna
50%	- Omni-directional: 7dBi
25%	- Bi-directional: 9dBi
12.5%	- Flat panel : 14dBi

Caution: Do not use any other antennas exceeding the allowed maximum gain per each antenna type in case you select 802.11b/g mode. For example, if you are intended to use omni-directional antenna for APU, it is illegal that you use a similar type of antenna with 14dBi even though the max allowable antenna is up to 14dBi.
Make sure that a gain per antenna type does not exceed the certified value.

Note: It is recommended that you set the transmit power to “Maximum” as the antennas listed in Appendix C(Antenna) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

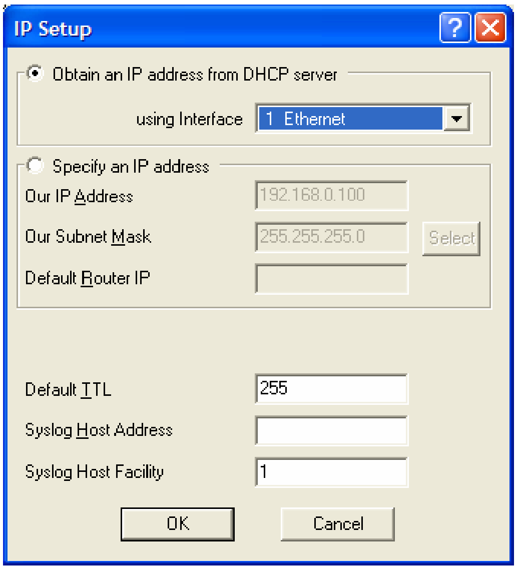
24. Select the Network ID in Network Settings referring to Appendix G “Wireless Network Planning."

Note: the Secure Data Mode network ID number (0-15) is used to differentiate between multiple Secure Data Mode stations using the same System Access Pass Phrase. This is used to allow a Secure Data Mode CSU to specify the APU mode unit that it wants to connect to if two APU mode units can be seen by the same CSU. Generally, this value should be the same as the Channel Number.

Note: The channel/frequency values are usually determined by network administrators. If you set the channel and frequency in 802.11b/g, ensure that there are at least four numerical channel differences between two overlapping cells to avoid interference. For example, channels 1, 6 and 11 don’t overlap, but channels 1 and 3 do.
In the other side, if you are intended to use 802.11a, please keep in mind that all channels (4 channels) with 20MHz bandwidth are not permitted to be overlapped with each channels in the frequency plan.

25. Click “OK” button.
26. Click the Setup → IP Setup button. The IP Setup screen is displayed, as shown below.

Figure 4-12
IP setup dialog box



IP Setup

● Obtain an IP address from DHCP server

using Interface: 1 Ethernet

○ Specify an IP address

Our IP Address: 192.168.0.100

Our Subnet Mask: 255.255.255.0

Default Router IP:

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

Note: The IP Setup screen allows you to set the Secure Data Mode Station's IP Addressing information. The Secure Data Mode Station must have an IP address assigned to it if you wish to connect to it using the Configurator tool, which makes use of SNMP to connect to the Secure Data Mode Station.

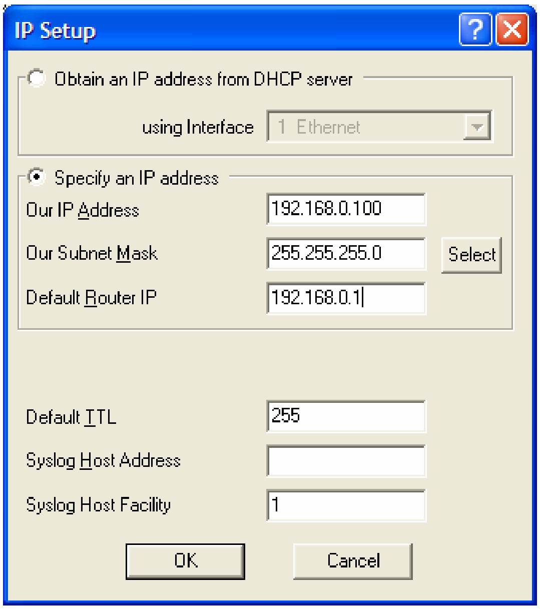
27. Select “Specify an IP address” and type a specific IP address and gateway IP address. Click OK button.

Note: Except for cable modem built-in APU, the CSU to operate as APU mode is required to set a mandatory static IP address for the unit even though it can be set in both static IP and DHCP setup. But, you can set DHCP mode to the CSU (APU mode) so that it can retrieve its IP address from a remote or local DHCP server.

Note: For DHCP client mode, select “1 Ethernet” as the interface which is used to get DHCP IP address from DHCP Server.

Note: If you select the DHCP option, it is recommended (though not required) that you set up your DHCP server to always provide the same IP address to this Secure Data Mode Station system.

Figure 4-13
IP setup dialog box



IP Setup

○ Obtain an IP address from DHCP server

using Interface: 1 Ethernet

● Specify an IP address

Our IP Address: 192.168.0.100

Our Subnet Mask: 255.255.255.0

Default Router IP: 192.168.0.1

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

28. For a more detailed setup, refer to the procedure 3-5(Basic Configuration) and 3-6(Advanced and Optional Configuration).

Procedure 3-2
Basic configuration and Operation Test (CSU-APU Mode)

Action

Step Action

1. The CSU(APU mode) has the following factory default parameters:

Factory Default

- IP address: DHCP Client (Ethernet 1)
- Read Write Password: public
- SNMP Secure Configuration Password: public
- IEEE 802.11 Interface Setup
  - Mode Selection: APU SDM(Secure Data Mode)
  - Base station mode: Polling (Primary)
  - Frequency
    → 802.11b/g Unit: CH1 (2412 MHz)
    → 802.11a Unit: CH149 (5745 MHz)
  - Network ID: 0
  - Transmit Rate
    → 802.11a/g Unit: 54Mbps
    → 802.11b Unit: 11Mbps
  - WEP Encryption: Disable

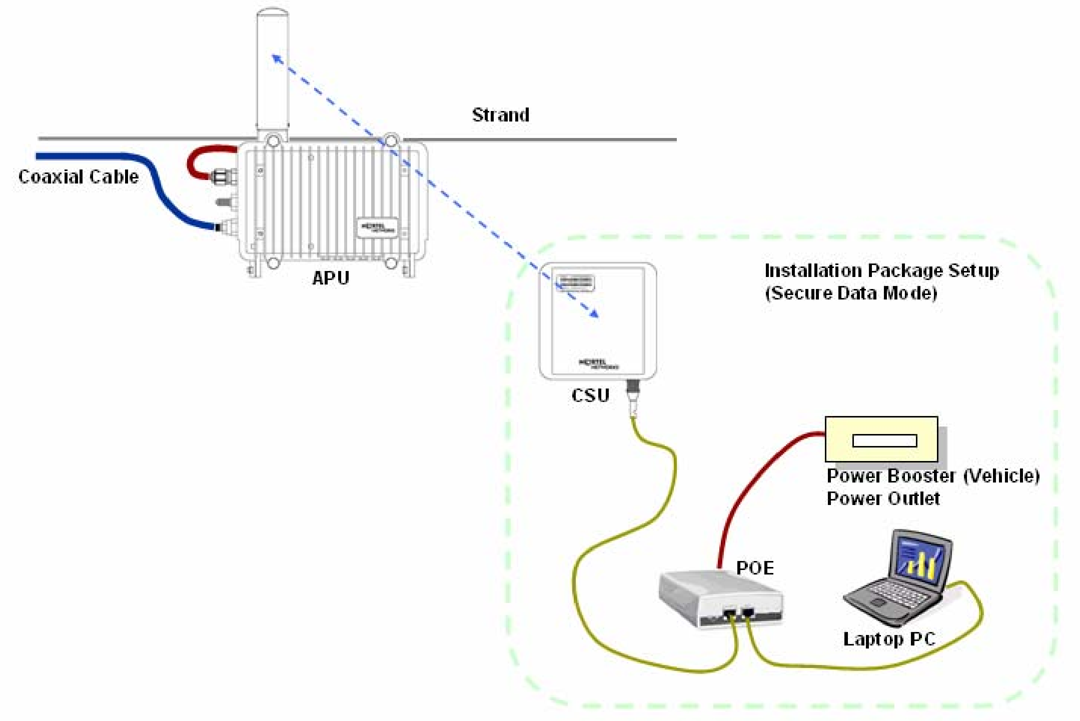
2. The CSU (CSU mode) shall have the same system parameters with a factory default parameter of APU to install.

Table 4-1
System Main Parameters

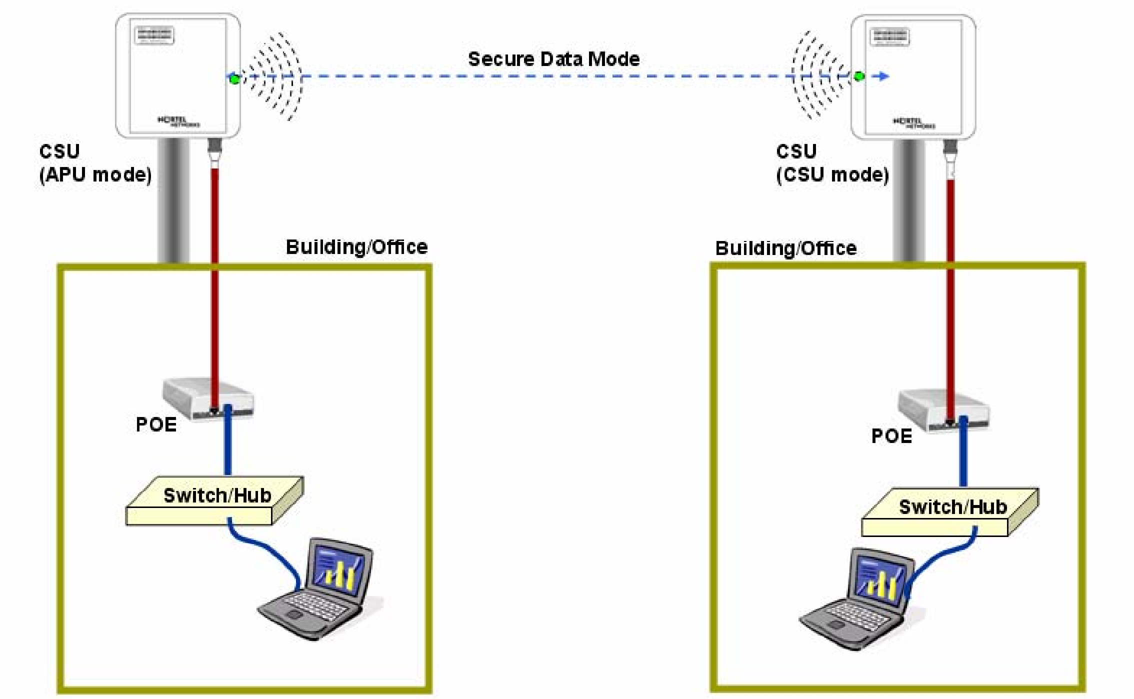
Parameter	APU/CSU(APU mode)	CSU
IP address	DHCP Client	DHCP Client
Read Write Password	Public	Public
SNMP Secure Configuration Password	Public	Public
Mode Selection	APU Secure Data Mode	CSU Secure Data Mode
Base Station Mode	Polling(Primary)	N/A
Frequency	User specific	User specific
Transmit Rate	User specific	User specific
Network ID	0	0
Others	User-specific	User-specific

Figure 4-14
Test Network Configuration (Radio Connection)

[Case I] APU to CSU (PTP or PMP)



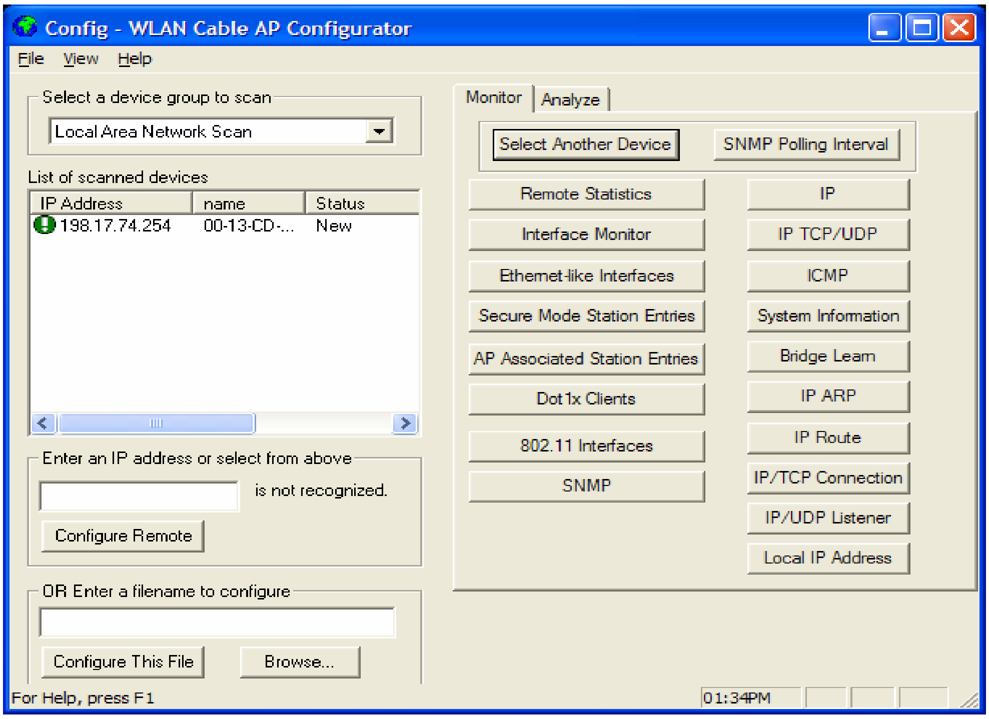
[Case II] CSU to CSU (PTP or PMP)



3. Prepare a Laptop computer and a client unit to test and configure the CSU at the installation location.
4. Connect Laptop PC to CSU Ethernet port with a straight-forward cable to setup.
5. Launch the Configurator by either double clicking the WLAN Cable AP Configurator icon on your desktop or by opening the file config.exe from the directory “C:\Program Files\Nortel\WLAN Cable AP Configurator” where software is installed at.
6. Run the Configurator and the IP Address for your APU (and the IP addresses for any other devices in your network) as appears in the Configurator window below.

Note: In factory default, APU and CSU have a default IP address as “198.17.74.254” regardless of the software modes (APU, CSU mode), which means that APU and CSU are ready to get it’s IP address from a remote DHCP Server. Therefore, when you launch AP configurator at PC with CSU turned on at first, you can find the default IP address of the CSU showing the green exclamation point “198.17.74.254” in the List of Scanned Devices window. In case that DHCP service is available in the cable network, you can find a new local IP address assigned to the unit from DHCP server in the list box except the default IP address.

Figure 4-15
Configurator Starting Window

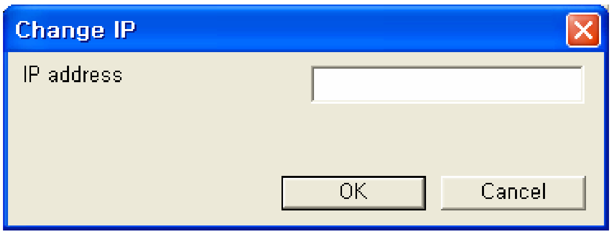


Select a device group to scan: Local Area Network Scan

IP Address	name	Status
198.17.74.254	00-13-CD-...	New

7. Right click on the IP address of CSU, and then select ‘Configure This Device’. or click “Configure Remote” button below the list box.
8. The Change IP window is displayed, as shown in the following screenshot.

Figure 4-16
IP setup dialog box



Change IP

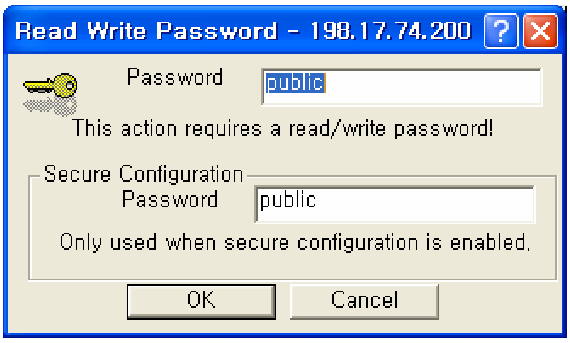
IP address

9. Enter an IP address that will be local to the IP of the PC/laptop running the Configurator, and then click the OK button in Read Write Password window.

Note: The IP address to enter should be included in the same subnet area with PC/Laptop Computer for access to CSU.
For example, in case the IP address of Laptop computer is 192.168.0.100/24, the CSU will be allowable in 192.168.0.1/24 ~ 192.168.0.254/24 as the IP address subnet group.

10. The SNMP Password dialog box is displayed, as shown below.
11. Press “Enter” key or enter a new password instead of the default password “public” in the basic SNMP password box.

Figure 4-17
SNMP Read Write Password dialog box



Read Write Password - 198.17.74.200

Password public

This action requires a read/write password!

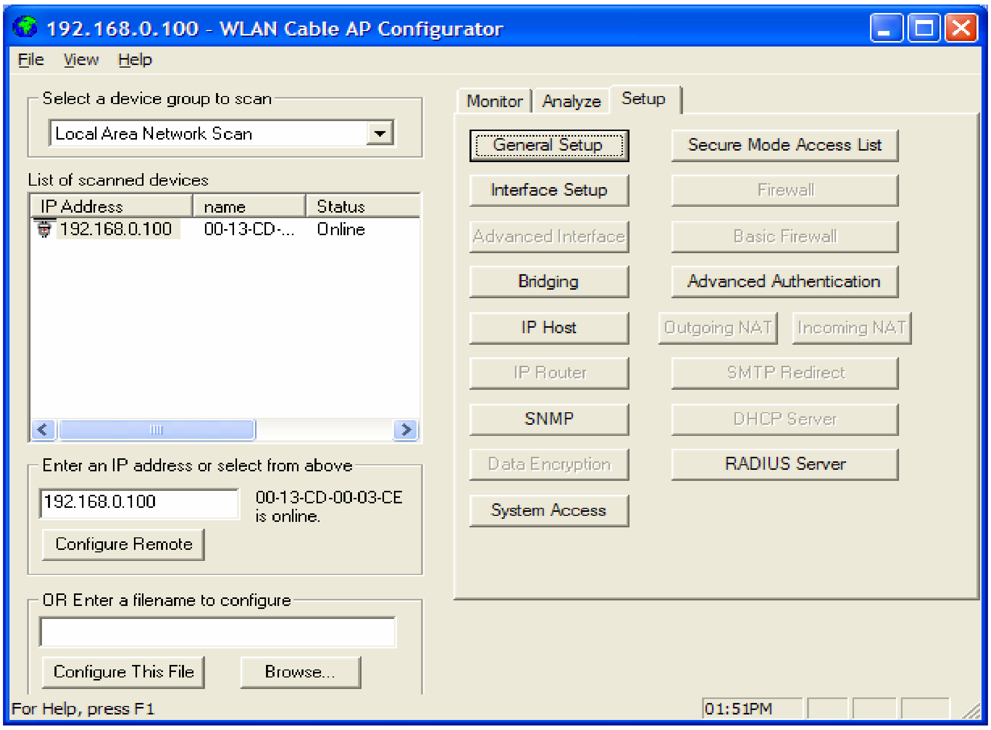
Secure Configuration

Password public

Only used when secure configuration is enabled.

12. The main window is redisplayed.
13. To setup the interface, Click on the Interface Setup button.
14. The Interface Setup screen is enabled and displayed, as shown in the Figure 4-19

Figure 4-18
AP Configurator Main window



Select a device group to scan: Local Area Network Scan

List of scanned devices

IP Address	name	Status
192.168.0.100	00-13-CD-...	Online

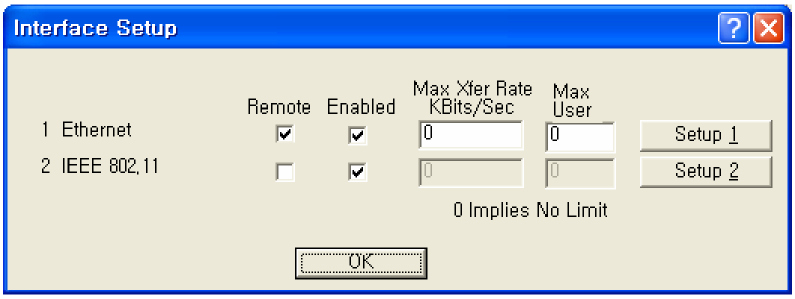
Enter an IP address or select from above: 192.168.0.100

00-13-CD-00-03-CE is online.

OR Enter a filename to configure

For Help, press F1 01:51PM

Figure 4-19
Interface setup dialog box



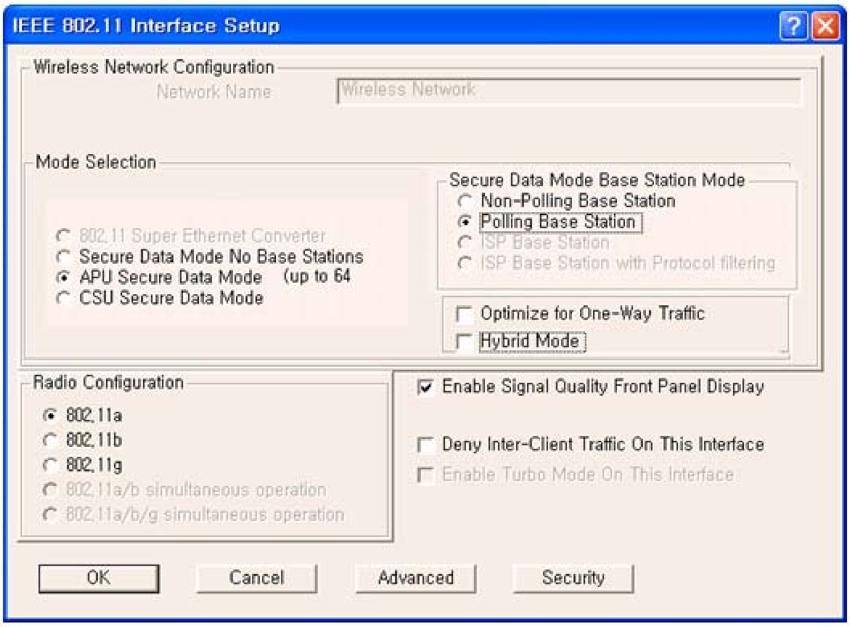
	Remote	Enabled	Max Xfer Rate KBits/Sec	Max User
1 Ethernet	☑	☑	0	0
2 IEEE 802.11	□	☑	0	0

0 Implies No Limit

15. If you have an 802.11 radio card, click the Setup 2 button to set up the 802.11 interface.
16. Click the Setup 2 button. The IEEE 802.11 Setup screen is displayed, as shown in Figure 4-20.
17. Select a radio standard to use according to the built-in antenna specification like an operating frequency range.
    Ex) 2.4GHz antenna : 802.11b/g, 5.8GHz antenna: 802.11a
18. Make sure the APU Secure Data Mode in the left portion of Mode Selection is selected while “Polling Base station” is clicked in Secure Data Mode Base Station Mode.

19. Select the Enable Signal Quality Front Panel Display checkbox if your unit has a front panel display that is capable of displaying the signal quality.

Figure 4-20
Interface setup dialog box



IEEE 802.11 Interface Setup

Wireless Network Configuration

Network Name: Wireless Network

Mode Selection

- ○ 802.11 Super Ethernet Converter
- ○ Secure Data Mode No Base Stations
- ● APU Secure Data Mode (up to 64
- ○ CSU Secure Data Mode

Secure Data Mode Base Station Mode

- ○ Non-Polling Base Station
- ● Polling Base Station
- ○ ISP Base Station
- ○ ISP Base Station with Protocol filtering

- □ Optimize for One-Way Traffic
- □ Hybrid Mode

Radio Configuration

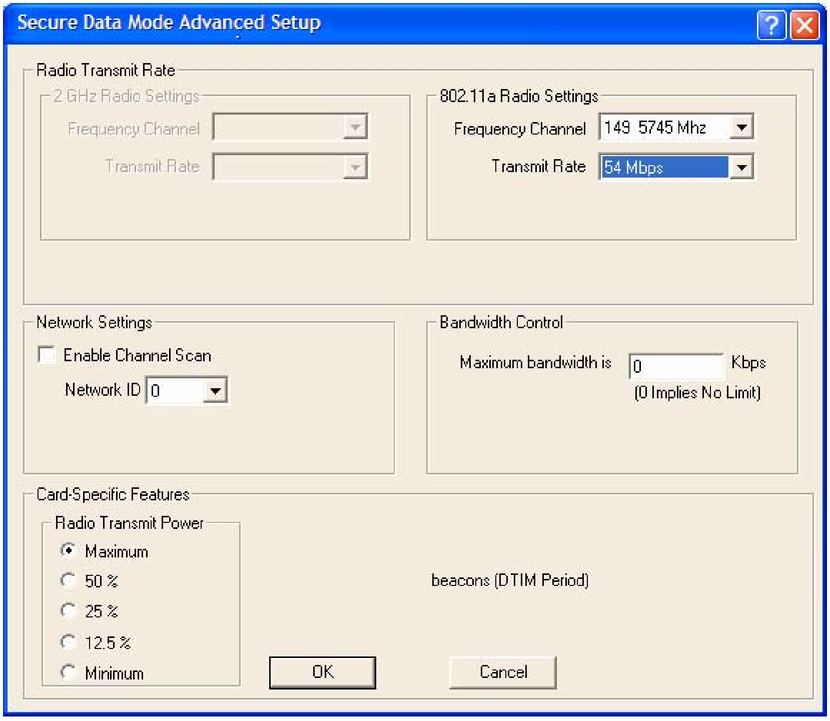
- ● 802.11a
- ○ 802.11b
- ○ 802.11g
- ○ 802.11a/b simultaneous operation
- ○ 802.11a/b/g simultaneous operation

- ☑ Enable Signal Quality Front Panel Display
- □ Deny Inter-Client Traffic On This Interface
- □ Enable Turbo Mode On This Interface

20. Click on the advanced button to set up crucial parameters such as Radio Frequency, Transmit Rate (Bandwidth) and Network ID.
21. The Advanced Setup screen for a Secure Data Mode is shown below.
22. Setup all radio parameters including a frequency channel and transmit power referring to the permitted setting value specified in the following tables per radio standard.

Figure 4-21
Advanced setup dialog box

[802.11a]



Frequency Channel	
149	5745 MHz
153	5765 MHz
157	5785 MHz
161	5805 MHz

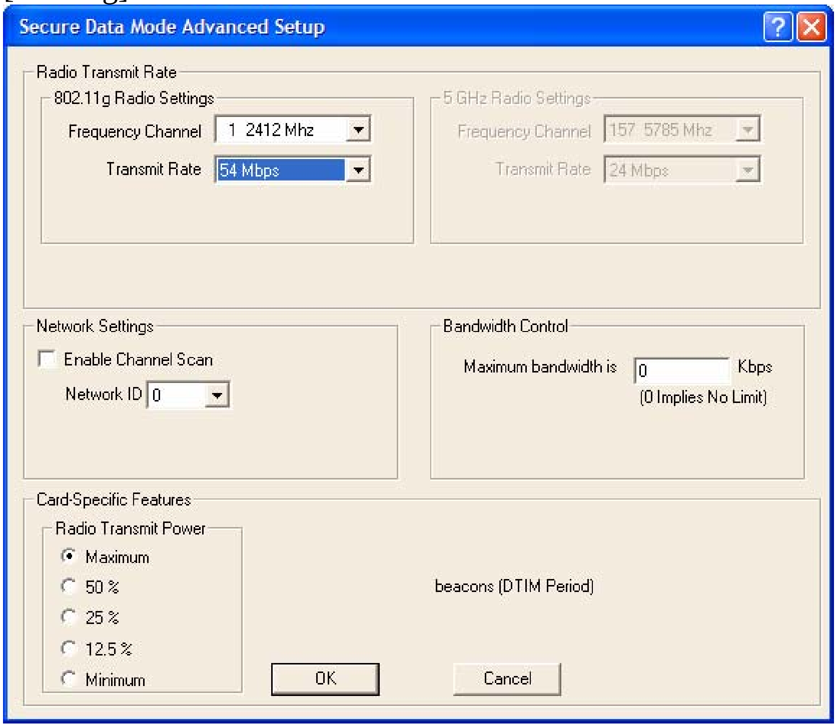
Transmit Rate	
6Mbps	36Mbps
9Mbps	48Mbps
12Mbps	54Mbps
24Mbps	

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(CSU/11A): 12dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (12dBi) except as the built-in type of antenna (ET-5PR12W) designated in Appendix C (Antenna) in case you select 802.11b/g mode as operation radio standard.

Note: It is recommended that you set the transmit power to "Maximum" as the antenna (ET-5PR12W) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

[802.11g]



Secure Data Mode Advanced Setup

Radio Transmit Rate

802.11g Radio Settings

Frequency Channel: 1 2412 Mhz

Transmit Rate: 54 Mbps

5 GHz Radio Settings

Frequency Channel: 157 5785 Mhz

Transmit Rate: 24 Mbps

Network Settings

□ Enable Channel Scan

Network ID: 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

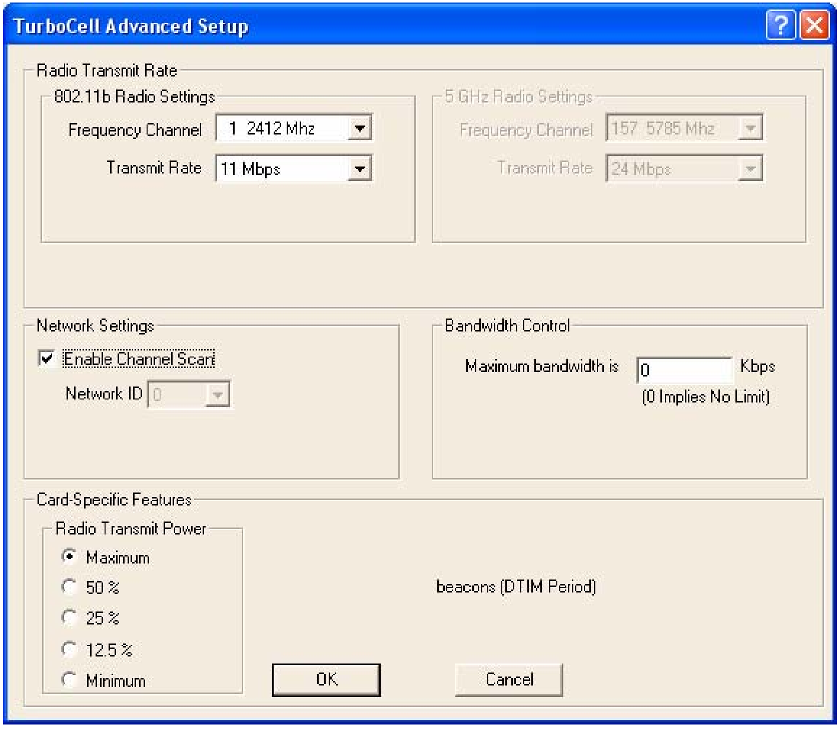
Transmit Rate	
54 Mbps	6 Mbps
48Mbps	11 Mbps
36 Mbps	5.5 Mbps
24 Mbps	2 Mbps
12 Mbps	1 Mbps

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(CSU/11G): 12dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (12dBi) except as the built-in type of antenna (ET-PR12) designated in Appendix C (Antenna) in case you select 802.11b/g mode as operation radio standard.

Note: It is recommended that you set the transmit power to “Maximum” as the antenna (ET-PR12) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

[802.11b]



TurboCell Advanced Setup

Radio Transmit Rate

802.11b Radio Settings

Frequency Channel: 1 2412 Mhz

Transmit Rate: 11 Mbps

5 GHz Radio Settings

Frequency Channel: 157 5785 Mhz

Transmit Rate: 24 Mbps

Network Settings

☑ Enable Channel Scan

Network ID: 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

Transmit Rate
11 Mbps
5.5 Mbps
2 Mbps
1 Mbps

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(CSU/11B): 12dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (12dBi) except as the built-in type of antenna (ET-PR12) designated in Appendix C (Antenna) in case you select 802.11b/g mode as operation radio standard.

Note: It is recommended that you set the transmit power to “Maximum” as the antenna (ET-PR12) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

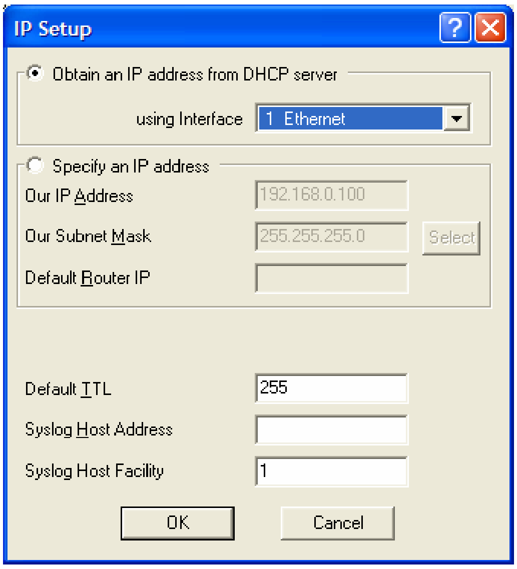
23. Select the Network ID in Network Settings referring to Appendix G “Wireless Network Planning.”

Note: the Secure Data Mode network ID number (0-15) is used to differentiate between multiple Secure Data Mode stations using the same System Access Pass Phrase. This is used to allow a Secure Data Mode CSU to specify the APU mode unit that it wants to connect to if two APU mode units can be seen by the same CSU. Generally, this value should be the same as the Channel Number.

Note: The channel/frequency values are usually determined by network administrators. If you set the channel and frequency in 802.11b/g, ensure that there are at least four numerical channel differences between two overlapping cells to avoid interference. For example, channels 1, 6 and 11 don’t overlap, but channels 1 and 3 do.
In the other side, if you are intended to use 802.11a, please keep in mind that all channels (4 channels) with 20MHz bandwidth are not permitted to be overlapped with each channels in the frequency plan.

24. Click “OK” button.
25. Click the Setup → IP Setup button. The IP Setup screen is displayed, as shown below.

Figure 4-22
IP setup dialog box



● Obtain an IP address from DHCP server

using Interface: 1 Ethernet

○ Specify an IP address

Our IP Address: 192.168.0.100

Our Subnet Mask: 255.255.255.0

Default Router IP:

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

Note: The IP Setup screen allows you to set the Secure Data Mode Station's IP Addressing information. The Secure Data Mode Station must have an IP address assigned to it if you wish to connect to it using the Configurator tool, which makes use of SNMP to connect to the Secure Data Mode Station.

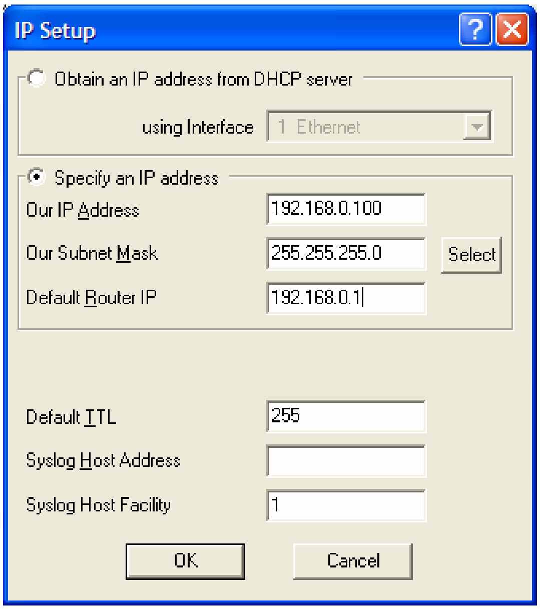
26. Select “Specify an IP address” and type a specific IP address and gateway IP address. Click OK button.

Note: Except for cable modem built-in APU, the CSU to operate as APU mode is required to set a mandatory static IP address for the unit even though it can be set in both static IP and DHCP setup. But, you can set DHCP mode to the CSU (APU mode) so that it can retrieve its IP address from a remote or local DHCP server.

Note: For DHCP client mode, select “1 Ethernet” as the interface which is used to get DHCP IP address from DHCP Server.

Note: If you select the DHCP option, it is recommended (though not required) that you set up your DHCP server to always provide the same IP address to this Secure Data Mode Station system.

Figure 4-23
IP setup dialog box



IP Setup

○ Obtain an IP address from DHCP server

using Interface: 1 Ethernet

● Specify an IP address

Our IP Address: 192.168.0.100

Our Subnet Mask: 255.255.255.0

Default Router IP: 192.168.0.1

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

27. For a more detailed setup, refer to the procedure 3-5(Basic Configuration) and 3-6(Advanced and Optional Configuration).

Procedure 3-3

Basic configuration and Operation Test (CSU-CSU Mode)

Action

Step Action

1. The CSU(CSU mode) has the following factory default parameters:

Factory Default

- IP address: DHCP Client (IEEE 802.11 2)
- Read Write Password: public
- SNMP Secure Configuration Password: public
- IEEE 802.11 Interface Setup
  - Mode Selection: CSU SDM(Secure Data Mode)
  - Base station mode: N/A
  - Frequency
    → 802.11b/g Unit: CH1 (2412 MHz)
    → 802.11a Unit: CH149 (5745 MHz)
  - Network ID: 0
  - Transmit Rate
    → 802.11a/g Unit: 54Mbps
    → 802.11b Unit: 11Mbps

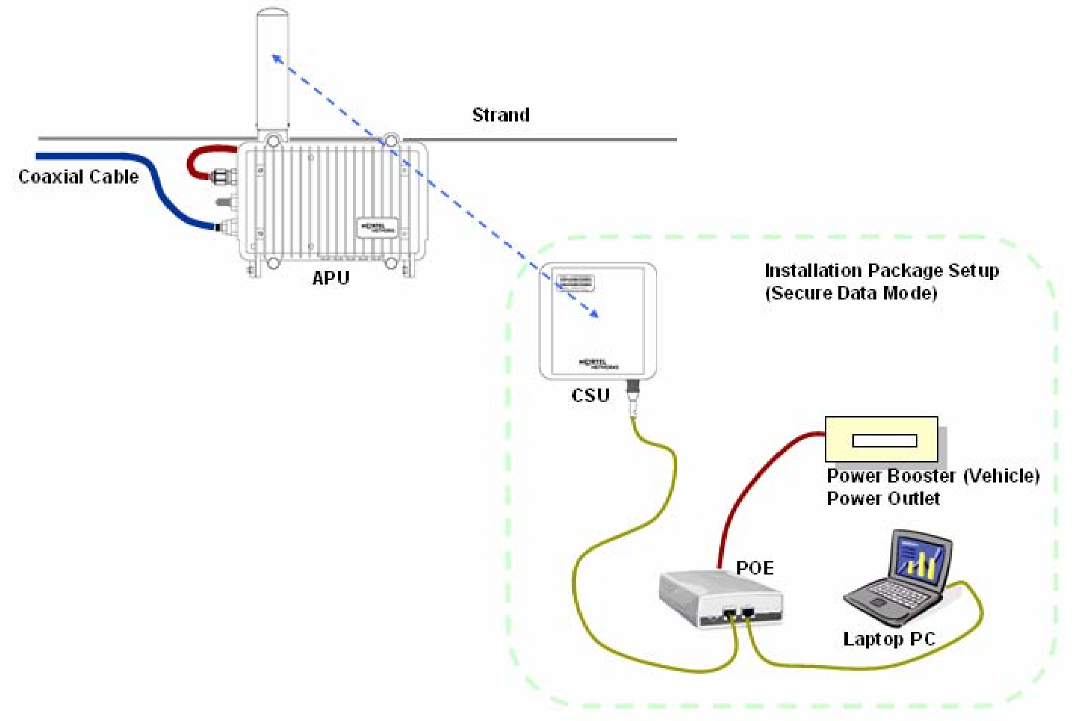
2. The CSU (CSU mode) shall have the common system parameters with that of a factory default parameter of APU to install.

Table 4-2
System Main Parameters

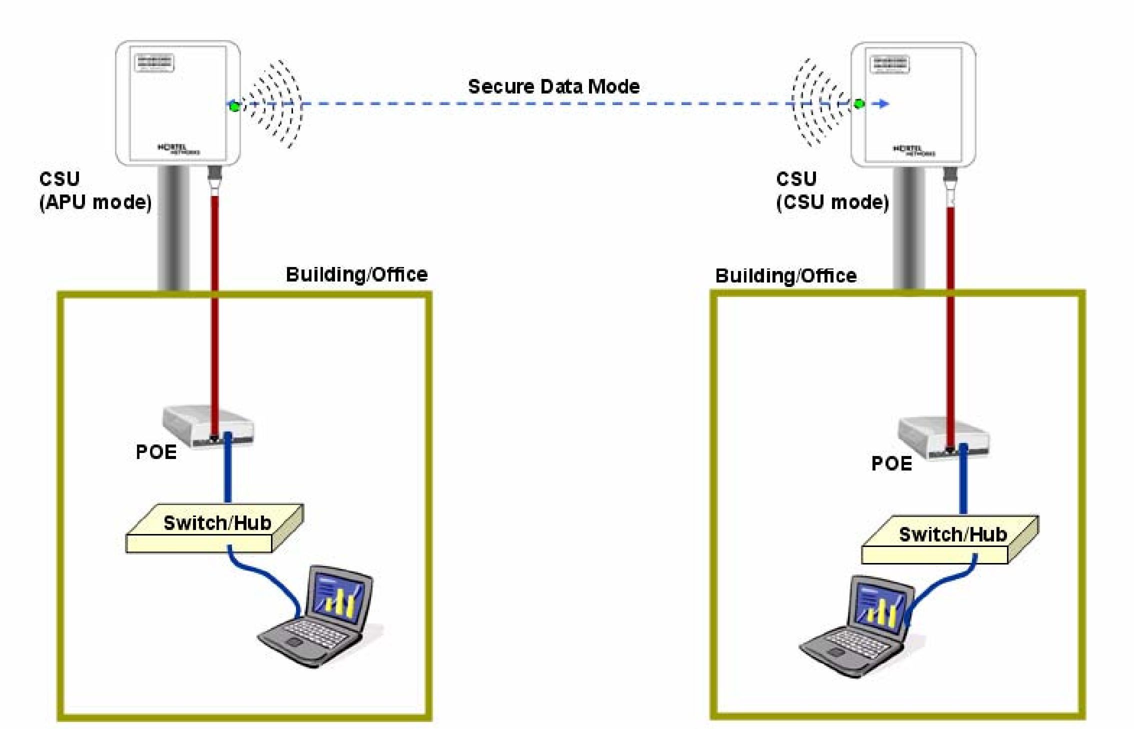
Parameter	CSU(APU mode)	CSU(CSU mode)
IP address	DHCP Client	DHCP Client
Read Write Password	Public	Public
SNMP Secure Configuration Password	Public	Public
Mode Selection	APU Secure Data Mode	CSU Secure Data Mode
Base Station Mode	Polling(Primary)	N/A
Frequency	User specific	User specific
Transmit Rate	User specific	User specific
Network ID	0	0
Others	User-specific	User-specific

Figure 4-24
Test Network Configuration (Radio Connection)

[Case I] APU to CSU (PTP or PMP)



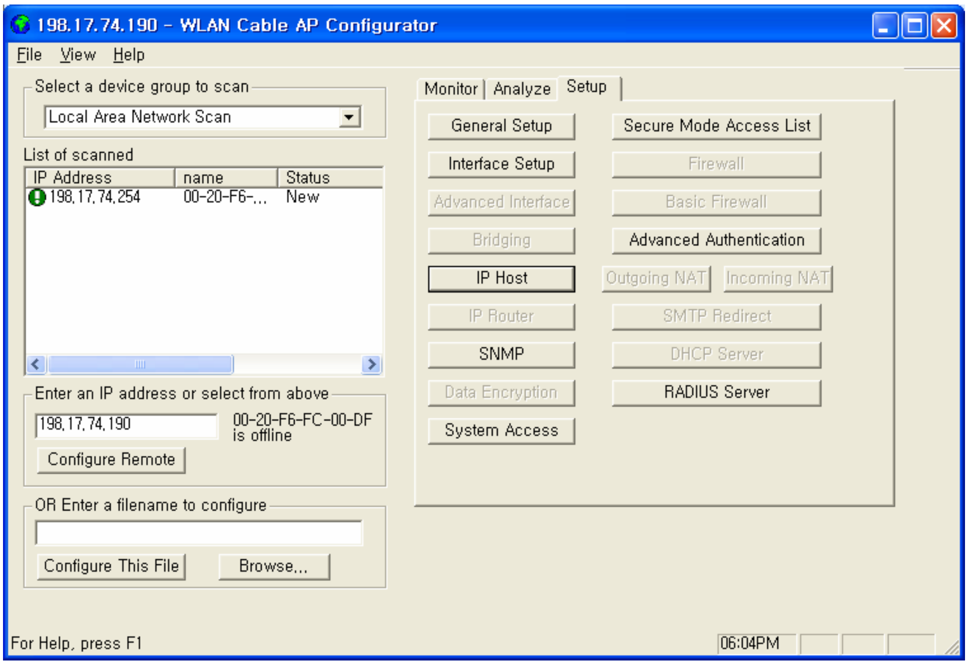
[Case II] CSU to CSU (PTP or PMP)



3. Prepare a Laptop computer and a client unit to test and configure the CSU at the installation location.
4. Connect Laptop PC to CSU Ethernet port with a straight-forward cable to setup.
5. Launch the Configurator by either double clicking the WLAN Cable AP Configurator icon on your desktop or by opening the file config.exe from the directory “C:\Program Files\Nortel\WLAN Cable AP Configurator” where software is installed at.
6. Run the Configurator and the IP Address for your APU (and the IP addresses for any other devices in your network) as appears in the Configurator window below.

Note: In factory default, the CSU have a default IP address as “198.17.74.254” regardless of the software modes (APU, CSU mode). Therefore, when you launch AP configurator at PC with CSU turned on at first, you can find the default IP address of the CSU showing the green exclamation point “198.17.74.254” in the List of Scanned Devices window showing the green exclamation point”198.17.74.254”.

Figure 4-25
Configurator Starting Window



198.17.74.190 - WLAN Cable AP Configurator

Select a device group to scan: Local Area Network Scan

List of scanned

IP Address	name	Status
198.17.74.254	00-20-F6-...	New

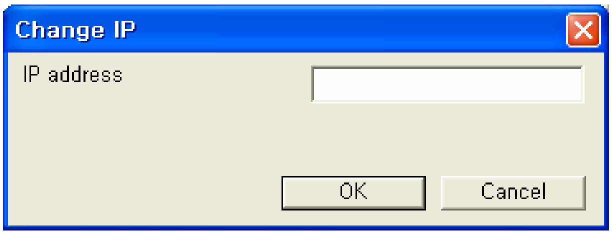
Enter an IP address or select from above: 198.17.74.190 — 00-20-F6-FC-00-DF is offline

OR Enter a filename to configure

For Help, press F1 — 06:04PM

7. Right click on the IP address of CSU, and then select ‘Configure This Device’. or click “Configure Remote” button below the list box.
8. The Change IP window is displayed, as shown in the following screenshot.

Figure 4-26
IP setup dialog box



Change IP

IP address

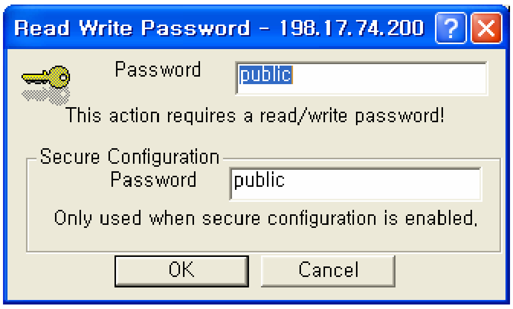
9. Enter an IP address that will be local to the IP of the PC/laptop running the Configurator, and then click the OK button in Read Write Password window.

Note: The IP address to enter should be included in the same subnet area with PC/Laptop Computer for access to CSU.

For example, in case the IP address of Laptop computer is 192.168.0.100/24, the CSU will be allowable in 192.168.0.1/24 ~ 192.168.0.254/24 as the IP address subnet group.

10. The SNMP Password dialog box is displayed, as shown below.
11. Press “Enter” key or enter a new password instead of the default password “public” in the basic SNMP password box.

Figure 4-27
SNMP Read Write Password dialog box



Read Write Password - 198.17.74.200

Password: public

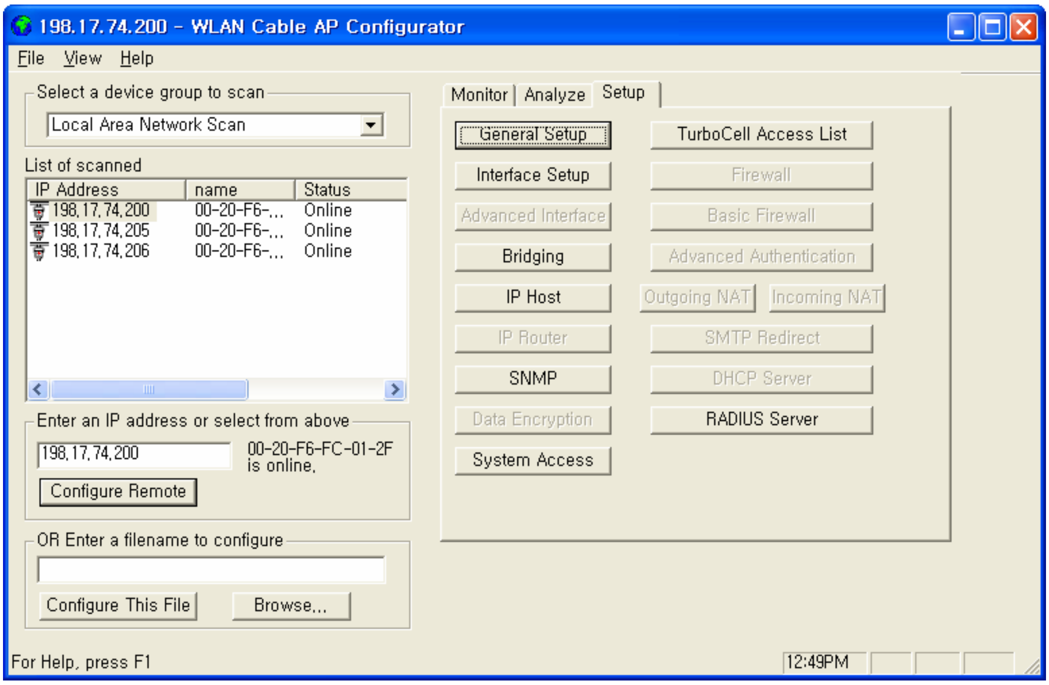
This action requires a read/write password!

Secure Configuration
Password: public

Only used when secure configuration is enabled.

12. The main window is redisplayed.
13. To setup the interface, Click on the Interface Setup button.
14. The Interface Setup screen is enabled and displayed, as shown in the Figure 4-29

Figure 4-28
AP Configurator Main window



198.17.74.200 - WLAN Cable AP Configurator

Select a device group to scan: Local Area Network Scan

List of scanned

IP Address	name	Status
198.17.74.200	00-20-F6-...	Online
198.17.74.205	00-20-F6-...	Online
198.17.74.206	00-20-F6-...	Online

Enter an IP address or select from above: 198.17.74.200

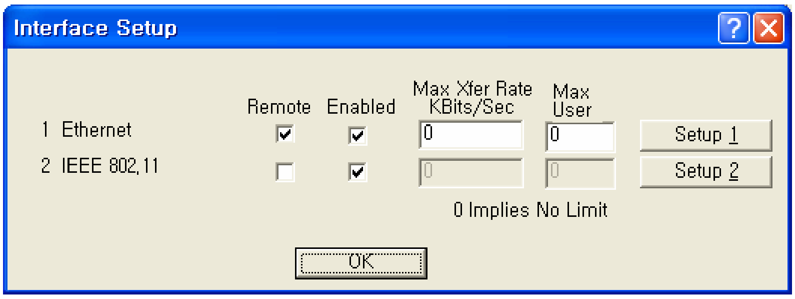
00-20-F6-FC-01-2F is online.

OR Enter a filename to configure

For Help, press F1

12:49PM

Figure 4-29
Interface setup dialog box



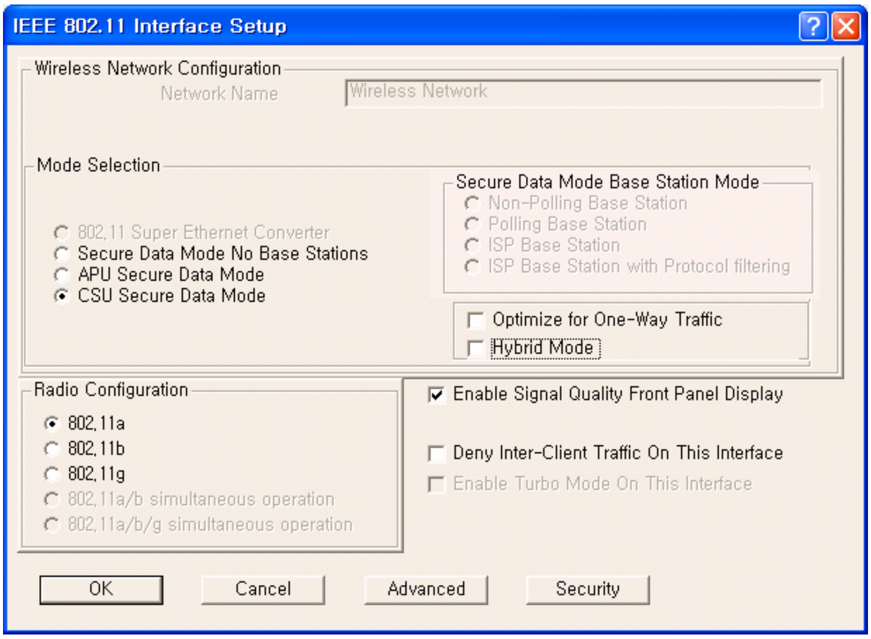
Interface Setup

	Remote	Enabled	Max Xfer Rate KBits/Sec	Max User	
1 Ethernet	☑	☑	0	0	Setup 1
2 IEEE 802.11	□	☑	0	0	Setup 2

0 Implies No Limit

15. If you have an 802.11 radio card, click the Setup 2 button to set up the 802.11 interface.
16. Click the Setup 2 button. The IEEE 802.11 Setup screen is displayed, as shown in Figure 4-30.
17. Select a radio standard to use according to the built-in antenna specification like an operating frequency range.
    Ex) 2.4GHz antenna : 802.11b/g, 5.8GHz antenna: 802.11a
18. Select the Enable Signal Quality Front Panel Display checkbox if your unit has a front panel display that is capable of displaying the signal quality.

Figure 4-30
Interface setup dialog box



IEEE 802.11 Interface Setup

Wireless Network Configuration

Network Name: Wireless Network

Mode Selection

- ○ 802.11 Super Ethernet Converter
- ○ Secure Data Mode No Base Stations
- ○ APU Secure Data Mode
- ● CSU Secure Data Mode

Secure Data Mode Base Station Mode

- ○ Non-Polling Base Station
- ○ Polling Base Station
- ○ ISP Base Station
- ○ ISP Base Station with Protocol filtering

- □ Optimize for One-Way Traffic
- □ Hybrid Mode

Radio Configuration

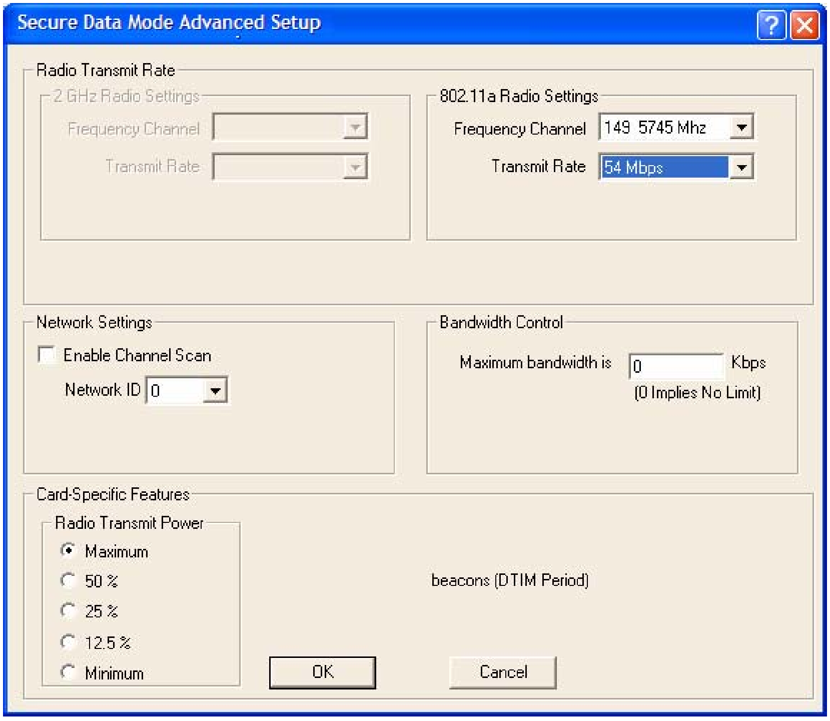
- ● 802.11a
- ○ 802.11b
- ○ 802.11g
- ○ 802.11a/b simultaneous operation
- ○ 802.11a/b/g simultaneous operation

- ☑ Enable Signal Quality Front Panel Display
- □ Deny Inter-Client Traffic On This Interface
- □ Enable Turbo Mode On This Interface

19. Click on the advanced button to set up crucial parameters such as Radio Frequency, Transmit Rate (Bandwidth) and Network ID.
20. The Advanced Setup screen for a Secure Data Mode is shown below.
21. Setup all radio parameters including a frequency channel and transmit power referring to the permitted setting value specified in the following tables per radio standard.

Figure 4-31
Advanced setup dialog box

[802.11a]



Secure Data Mode Advanced Setup

Radio Transmit Rate

2 GHz Radio Settings

Frequency Channel

Transmit Rate

802.11a Radio Settings

Frequency Channel 149 5745 Mhz

Transmit Rate 54 Mbps

Network Settings

□ Enable Channel Scan

Network ID 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

OK

Cancel

Frequency Channel	
149	5745 MHz
153	5765 MHz
157	5785 MHz
161	5805 MHz

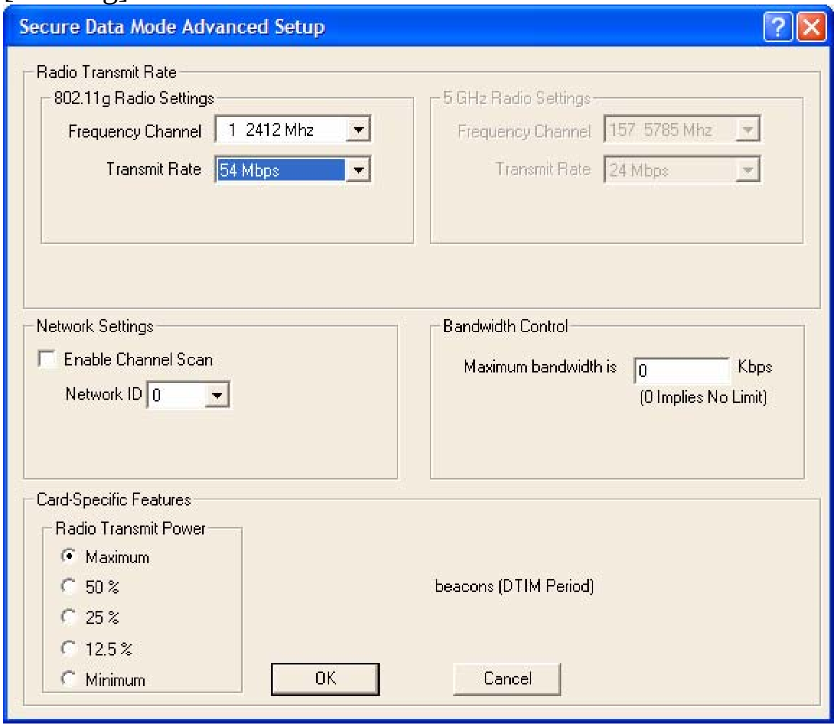
Transmit Rate	
6Mbps	36Mbps
9Mbps	48Mbps
12Mbps	54Mbps
24Mbps	

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(CSU/11A): 12dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (12dBi) except as the built-in type of antenna (ET-5PR12W) designated in Appendix C (Antenna) in case you select 802.11b/g mode as operation radio standard.

Note: It is recommended that you set the transmit power to “Maximum” as the antenna (ET-PR12) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

[802.11g]



Secure Data Mode Advanced Setup

Radio Transmit Rate

802.11g Radio Settings

Frequency Channel: 1 2412 Mhz

Transmit Rate: 54 Mbps

5 GHz Radio Settings

Frequency Channel: 157 5785 Mhz

Transmit Rate: 24 Mbps

Network Settings

□ Enable Channel Scan

Network ID: 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

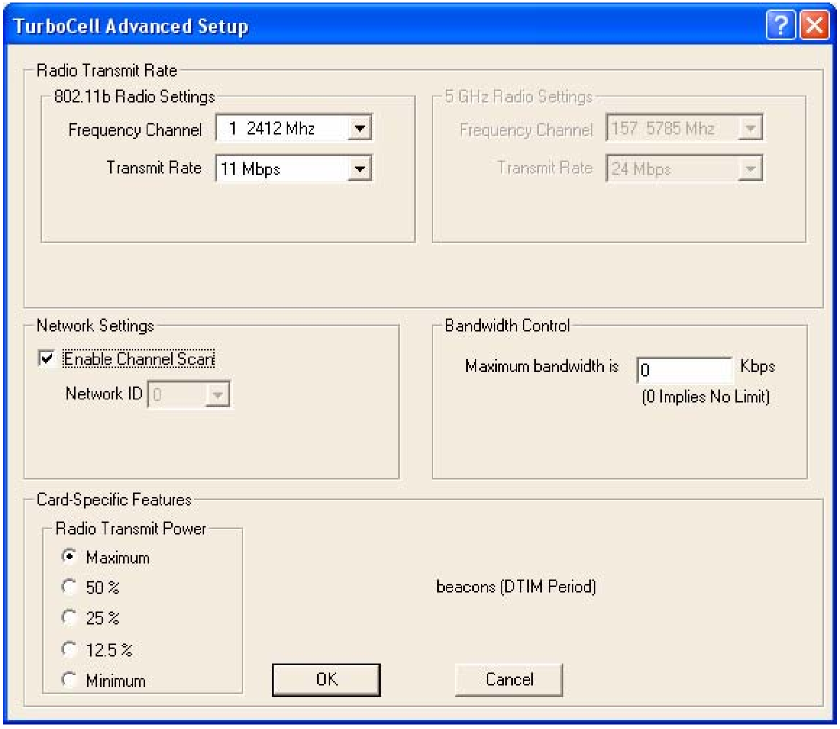
Transmit Rate	
54 Mbps	6 Mbps
48Mbps	11 Mbps
36 Mbps	5.5 Mbps
24 Mbps	2 Mbps
12 Mbps	1 Mbps

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(CSU/11G): 12dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (12dBi) except as the built-in type of antenna (ET-PR12) designated in Appendix C (Antenna) in case you select 802.11b/g mode as operation radio standard.

Note: It is recommended that you set the transmit power to “Maximum” as the antenna (ET-PR12) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

[802.11b]



TurboCell Advanced Setup

Radio Transmit Rate

802.11b Radio Settings

Frequency Channel: 1 2412 Mhz

Transmit Rate: 11 Mbps

5 GHz Radio Settings

Frequency Channel: 157 5785 Mhz

Transmit Rate: 24 Mbps

Network Settings

☑ Enable Channel Scan

Network ID: 0

Bandwidth Control

Maximum bandwidth is 0 Kbps

(0 Implies No Limit)

Card-Specific Features

Radio Transmit Power

● Maximum

○ 50 %

○ 25 %

○ 12.5 %

○ Minimum

beacons (DTIM Period)

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

Transmit Rate
11 Mbps
5.5 Mbps
2 Mbps
1 Mbps

Transmit Power	Antenna Gain
Maximum	Maximum allowable antenna Gain(CSU/11B): 12dBi
50%	
25%	
12.5%	

Caution: Do not use any other antennas exceeding the allowed maximum antenna gain value (12dBi) except as the built-in type of antenna (ET-PR12) designated in Appendix C (Antenna) in case you select 802.11b/g mode as operation radio standard.

Note: It is recommended that you set the transmit power to “Maximum” as the antenna (ET-PR12) have been designed to meet FCC regulation specifying the maximum allowable EIRP at the maximum transmit power.

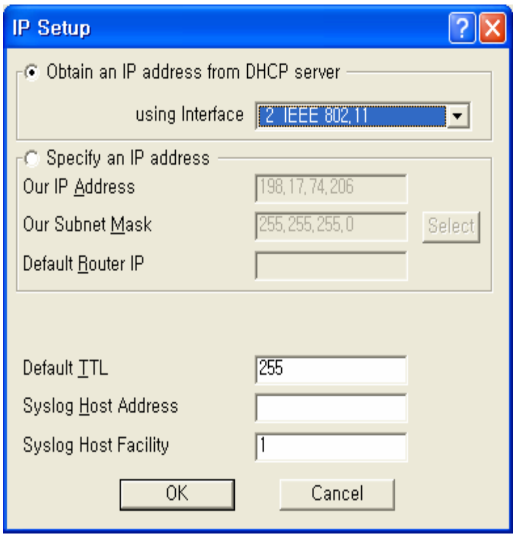
22. Select the Network ID in Network Settings referring to Appendix G “Wireless Network Planning.”

Note: the Secure Data Mode network ID number (0-15) is used to differentiate between multiple Secure Data Mode stations using the same System Access Pass Phrase. This is used to allow a Secure Data Mode CSU to specify the APU mode unit that it wants to connect to if two APU mode units can be seen by the same CSU. Generally, this value should be the same as the Channel Number.

Note: The channel/frequency values are usually determined by network administrators. If you set the channel and frequency in 802.11b/g, ensure that there are at least four numerical channel differences between two overlapping cells to avoid interference. For example, channels 1, 6 and 11 don’t overlap, but channels 1 and 3 do.
In the other side, if you are intended to use 802.11a, please keep in mind that all channels (4 channels) with 20MHz bandwidth are not permitted to be overlapped with each channels in the frequency plan.

23. Click “OK” button.
24. Click the Setup → IP Setup button. The IP Setup screen is displayed, as shown below.

Figure 4-32
IP setup dialog box



IP Setup

● Obtain an IP address from DHCP server

using Interface: 2 IEEE 802.11

○ Specify an IP address

Our IP Address: 198.17.74.206

Our Subnet Mask: 255.255.255.0 [Select]

Default Router IP:

Default TTL: 255

Syslog Host Address:

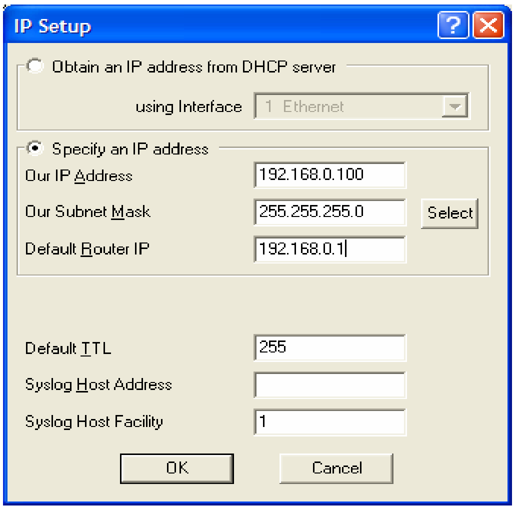
Syslog Host Facility: 1

[OK] [Cancel]

Note: The IP Setup screen allows you to set the Secure Data Mode Station's IP Addressing information. The Secure Data Mode Station must have an IP address assigned to it if you wish to connect to it using the Configurator tool, which makes use of SNMP to connect to the Secure Data Mode Station.

25. Select “Specify an IP address” and type a specific IP address and gateway IP address. Click OK button.

Figure 4-33
IP setup dialog box



IP Setup

○ Obtain an IP address from DHCP server

using Interface: 1 Ethernet

● Specify an IP address

Our IP Address: 192.168.0.100

Our Subnet Mask: 255.255.255.0 [Select]

Default Router IP: 192.168.0.1

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

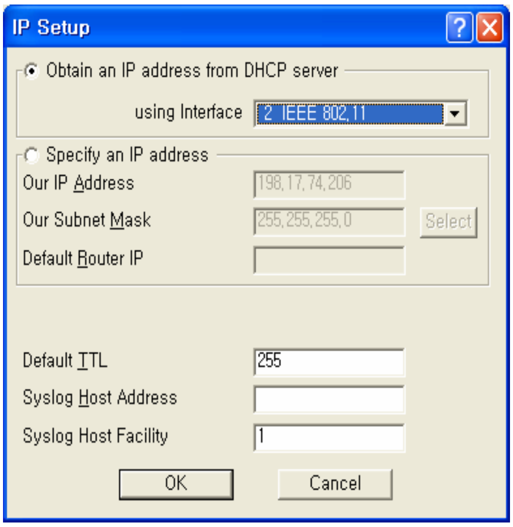
[OK] [Cancel]

Note: Except for cable modem built-in APU, the CSU to operate as CSU mode is required to set a mandatory static IP address for the unit even though it can be set in both static IP and DHCP setup.

For your reference, APU and CSU (APU mode) have DHCP Server feature which can assign an IP address to all networks entities like CSU and PC in the sub-network.

Note: For DHCP client mode, select “2 IEEE 802.11” as the interface which is used to get DHCP IP address from DHCP Server.

Figure 4-34
IP setup dialog box



IP Setup

● Obtain an IP address from DHCP server

using Interface: 2 IEEE 802.11

○ Specify an IP address

Our IP Address: 198.17.74.206

Our Subnet Mask: 255.255.255.0 Select

Default Router IP:

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

OK Cancel

Note: If you select the DHCP option, it is recommended (though not required) that you set up your DHCP server to always provide the same IP address to this Secure Data Mode Station system.

26. For a more detailed setup, refer to the procedure 3-5(Basic Configuration) and 3-6(Advanced and Optional Configuration).

Procedure 3-4
Testing the connection between APU & CSU (APU mode) and CSU

The Configurators Wireless Link Test screen is used to diagnose the wireless link quality between your APU and any CSU associated with the APU.

The Wireless Link Test displays the diagnostic counters that apply to the radio interface and a single remote station connected to this APU.

To assess the overall wireless performance in the wireless area served by the APU, you might need to run Remote Link Tests with multiple CSUs (one by one).

Action

Step Action

1. Prepare a Laptop computer and configure the test network as shown in Figure 4-35.
2. Prepare a CSU module, POE Injector and Power supply system like a Power booster in a vehicle or regular power outlet in the home.

Note: Ensure that the CSU and the Laptop computer are set to DHCP Client so that they can get the IP address dynamically through the APU from the Server.

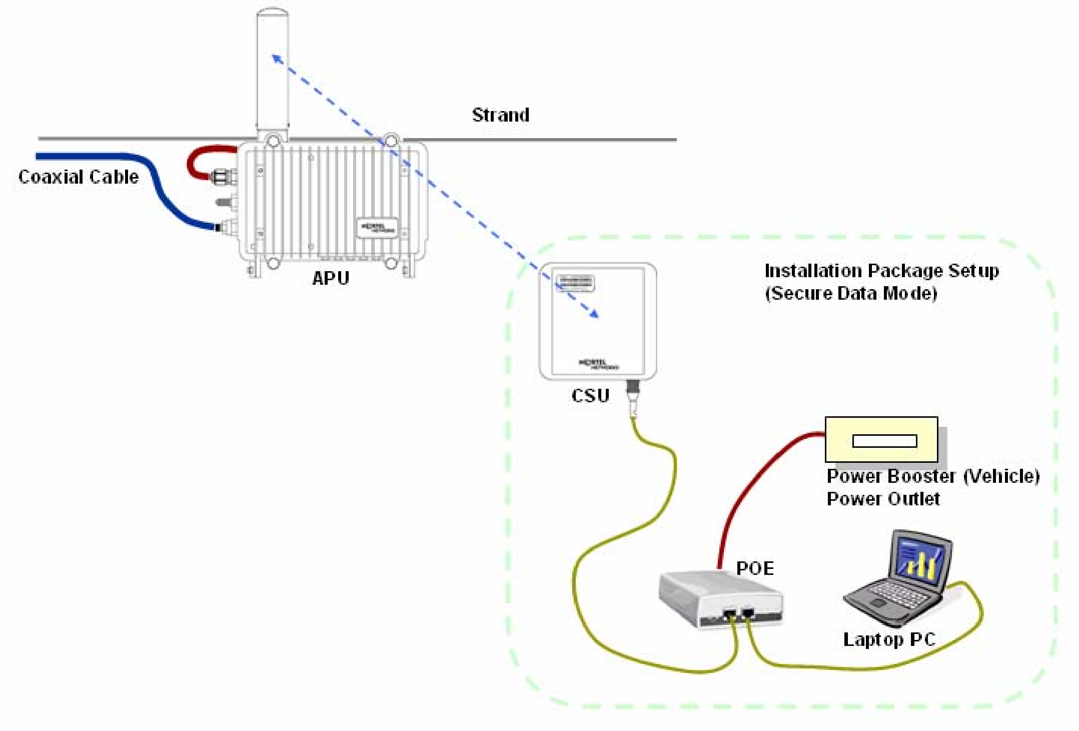
3. The CSU has the same system parameters as the CSU (APU mode). Set the system parameter as follows to test connection.

Table 4-3
System Main Parameters

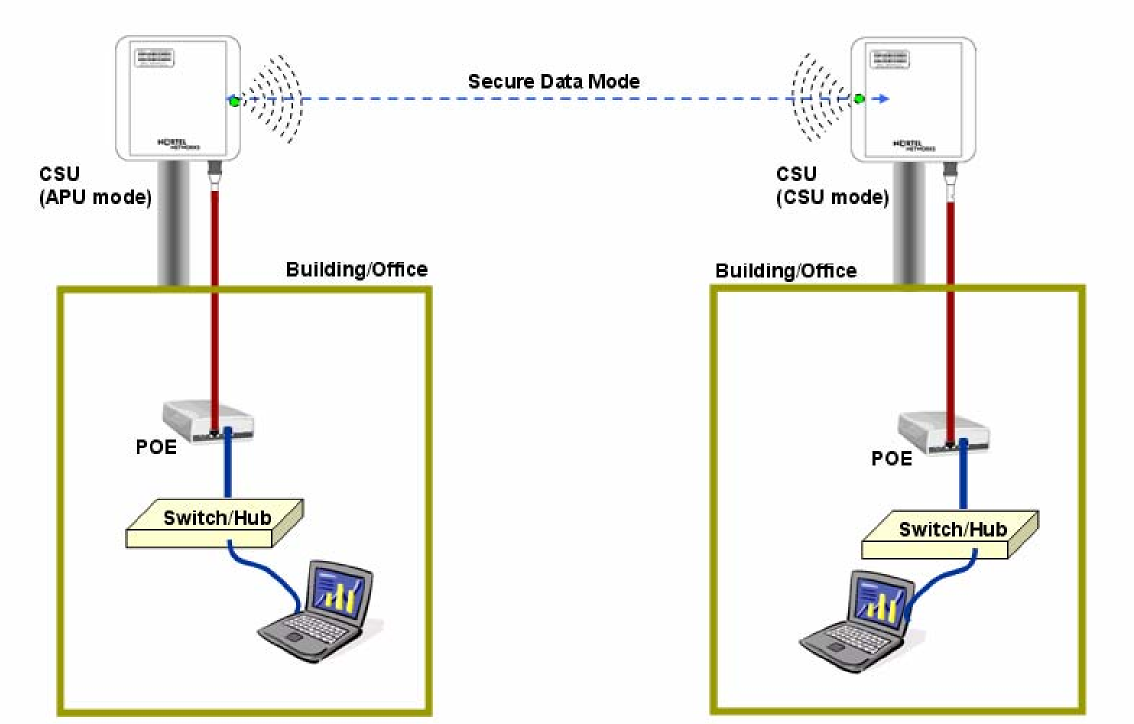
Parameter	APU	CSU
IP address	DHCP Client	DHCP Client
Read Write Password	User-specific	User-specific
SNMP Secure Configuration Password	User-specific	User-specific
Mode Selection	APU Secure Data Mode	CSU Secure Data Mode
Base Station Mode	Polling(Primary)	N/A
Frequency	User-specific	User-specific
Transmit Rate	User-specific	User-specific
Network ID	User-specific	User-specific
Others	User-specific	User-specific

Figure 4-35
Test Network Configuration (Radio Connection)

[Case I] APU to CSU (PTP or PMP)

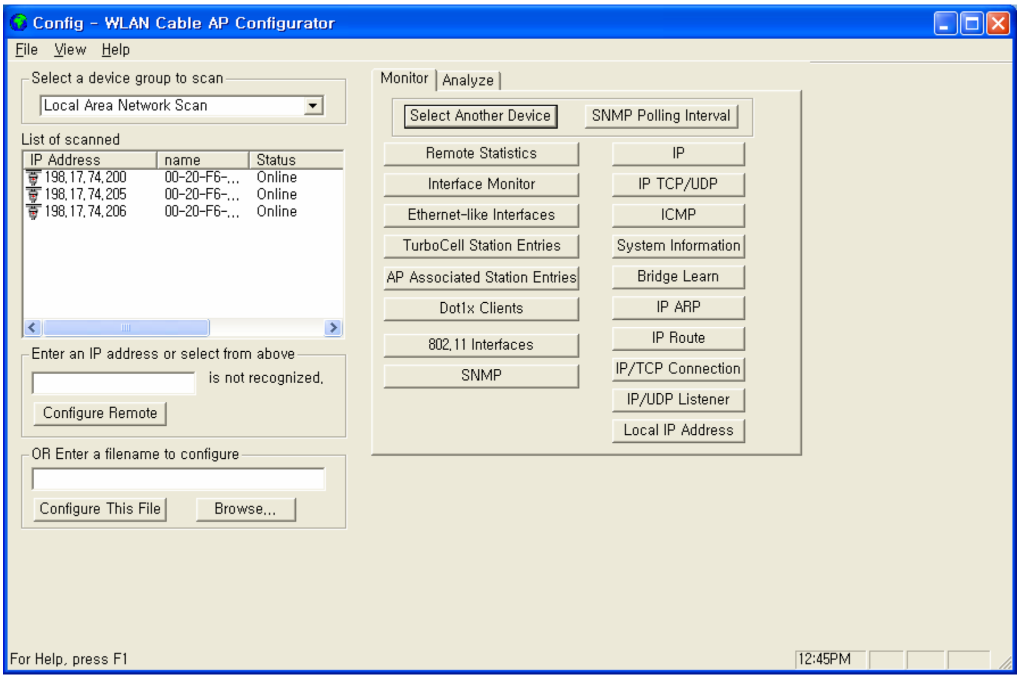


[Case II] CSU to CSU (PTP or PMP)



4. Launch the Configurator by either double clicking the WLAN Cable AP Configurator icon on your desktop or by opening the file config.exe from the directory “C:\Program Files\Nortel\WLAN Cable AP Configurator” where software is installed.
5. The Configurator runs the IP Address for your APU and the Test CSU (and the IP addresses for any other devices in your network) appears in the Configurator window, as shown below.

Figure 4-36
Configurator Starting Window



Select a device group to scan: Local Area Network Scan

List of scanned

IP Address	name	Status
198.17.74.200	00-20-F6-...	Online
198.17.74.205	00-20-F6-...	Online
198.17.74.206	00-20-F6-...	Online

Enter an IP address or select from above

is not recognized.

OR Enter a filename to configure

For Help, press F1

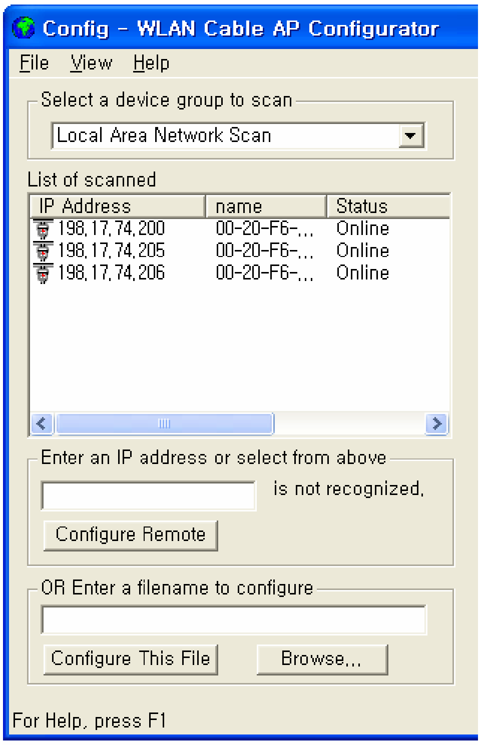
12:45PM

6. Ensure that the laptop computer gets an IP address assigned from the DHCP server at Network Center or statically defined by checking an IP address list box at the left side of the configurator window.
7. Check if all units of APU/CSU (APU mode) and Test CSU have its own IP addresses.
8. If the APU/CSU (APU mode) you wish to configure is on the same network subnet as your computer, you can select it from the list that is automatically displayed in the IP Address window. Press the <F5> key to refresh the scan list. Alternately, you can also right click anywhere in the scan window and select Re-scan the local network.

Note: To differentiate the APU/CSU (APU mode) to be configured, you should check the AP MAC address of the APU/CSU (APU mode) which is printed on the label attached to the side of the APU/CSU (APU mode).

9. If you can find out the IP address of the APU on the IP address window, move the cursor to the appropriate IP address.

Figure 4-37
IP address list box



Select a device group to scan: Local Area Network Scan

List of scanned

IP Address	name	Status
198.17.74.200	00-20-F6-...	Online
198.17.74.205	00-20-F6-...	Online
198.17.74.206	00-20-F6-...	Online

Enter an IP address or select from above

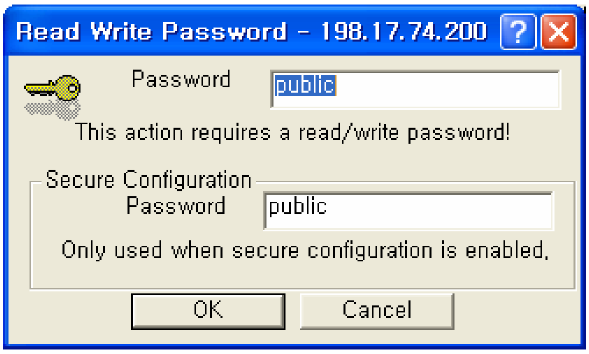
is not recognized.

OR Enter a filename to configure

For Help, press F1

10. Right click on the IP address, and click the Configure button below the list box on the left side of a configurator window. The Read/Write Password screen is displayed, as shown below.

Figure 4-38
SNMP Password (Read/Write)



Password: public

This action requires a read/write password!

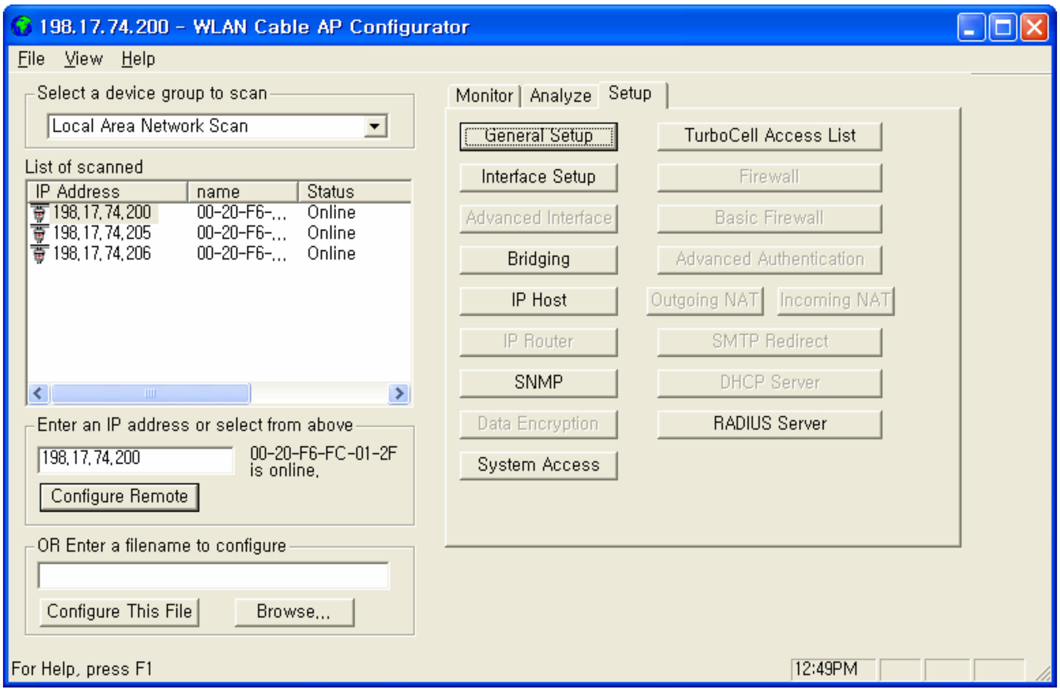
Secure Configuration
Password: public

Only used when secure configuration is enabled.

11. Enter the password “public” for the device you have selected at both text boxes, and then click the OK button.

12. If the Setup tab is displayed in the main window as shown below, SNMP checking is a success.

Figure 4-39
Setup Tab



198.17.74.200 - WLAN Cable AP Configurator

Select a device group to scan: Local Area Network Scan

List of scanned

IP Address	name	Status
198.17.74.200	00-20-F6-...	Online
198.17.74.205	00-20-F6-...	Online
198.17.74.206	00-20-F6-...	Online

Enter an IP address or select from above: 198.17.74.200

00-20-F6-FC-01-2F is online.

OR Enter a filename to configure

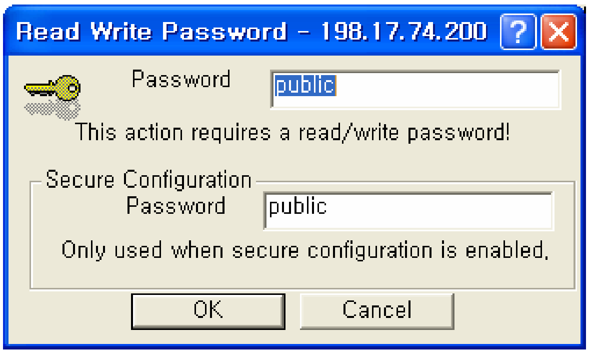
For Help, press F1

12:49PM

Note: When you test the APU/CSU (APU mode) with Test CSU, you don't have to change the parameters of APU/CSU (APU mode) with AP configurator. After all the tests are completed, you should configure the APU/CSU (APU mode) according to your local network design concept.

13. Select Wireless Link Test from the Analyze Tab. The Enter IP Address screen is displayed, as shown below.

Figure 4-40
SNMP Password (Read/Write)



Read Write Password - 198.17.74.200

Password: public

This action requires a read/write password!

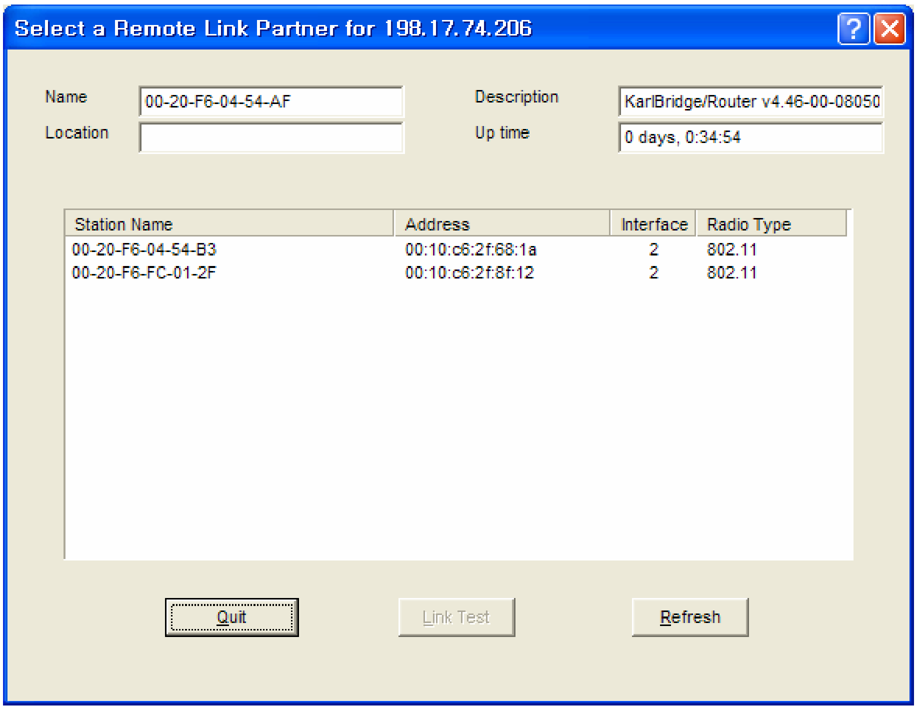
Secure Configuration

Password: public

Only used when secure configuration is enabled.

14. Enter the Remote IP Address and Read/Write password for the wireless station you wish to test. The Select a Remote Link Partner screen is displayed, as shown below.

Figure 4-41
Remote Link List window



Name: 00-20-F6-04-54-AF
Location:
Description: KarlBridge/Router v4.46-00-08050
Up time: 0 days, 0:34:54

Station Name	Address	Interface	Radio Type
00-20-F6-04-54-B3	00:10:c6:2f:68:1a	2	802.11
00-20-F6-FC-01-2F	00:10:c6:2f:8f:12	2	802.11

15. From the list of station names, select the remote station or client you wish to test. Select a station from the list, and then click on the Link Test button to perform a link test.

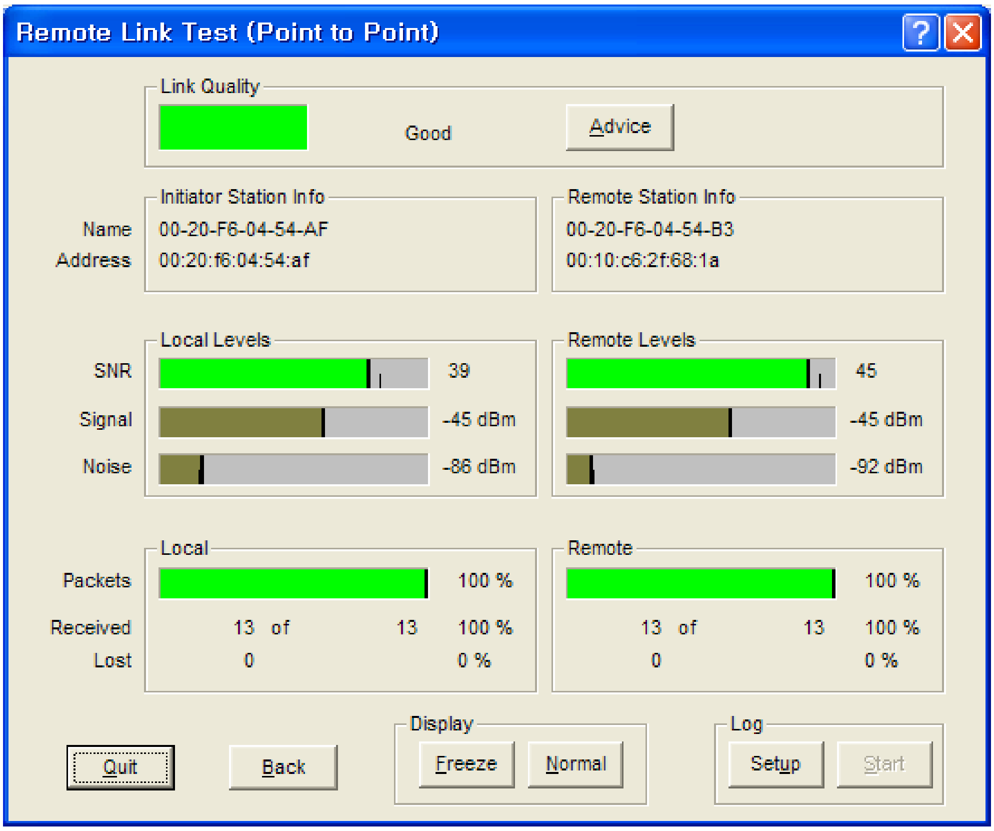
    Note: Clicking the Explore button refreshes the list of stations that can be selected.

16. Click the Link Test button to start the link test.

    Note: When you open this screen, the base station will need approximately 20 seconds to build the list of stations and forward this information to your configurator station. Due to the dynamic characteristics of mobile wireless stations, the base station will rebuild the list of connected stations each time you select a different station, or after clicking the Explore button. If this screen does not display any station, there might be no wireless station up and running in the vicinity of the selected base station.

17. The Remote Link Test screen displays the results of your wireless link test, as shown below.

Figure 4-42
Remote Link Test Status Window



Remote Link Test (Point to Point)

Link Quality: Good

	Initiator Station Info	Remote Station Info
Name	00-20-F6-04-54-AF	00-20-F6-04-54-B3
Address	00:20:f6:04:54:af	00:10:c6:2f:68:1a

	Local Levels	Remote Levels
SNR	39	45
Signal	-45 dBm	-45 dBm
Noise	-86 dBm	-92 dBm

	Local			Remote		
Packets			100 %			100 %
Received	13 of	13	100 %	13 of	13	100 %
Lost	0		0 %	0		0 %

18. The advice button enables you to investigate the outcome of the Remote Link Test assessment in more detail and provides you with troubleshooting hints to improve the quality of the link between the two remote nodes. The following table summarizes the possible results of clicking the Advice button, and what action is warranted based on the results:
19. It is necessary that you adjust the vertical tilt and horizontal angle toward APU at the mounting point of CSU, while monitoring the RF link quality status window so that the SNR and Link status bar for the best quality.

Table 4-4
Radio Link Status

Status	Risk	Action
Excellent	None	▪ You do not need to perform further diagnostics.
Good	None	▪ You may try to optimize antenna placement to see whether this will improve the Link Quality result.
Marginal	Communication is still possible, but this situation may affect the unit's performance.	▪ View Link Test Details to verify. The unit may have to retransmit lost packets. ▪ Verify the Signal Level indicator. A low Signal Level indicates the unit has moved away from the base station. ▪ View Link Test Details to verify the Noise Level indicator. A high Noise Level indicates a source of interference in the signal path between the unit and the base station. ▪ Select another unit to verify if the base station is functioning properly. ▪ Try to optimize antenna placement to improve the Signal Level or move it away from the source of interference.
“No Connection”	Communication is no longer possible. If the unit was in the process of transferring files, data may not have arrived at the intended destination, or it may have been corrupted.	▪ View Link Test Details to verify the Signal Level indicator. A low Signal Level indicates the unit has moved away from the base station. ▪ View Link Test Details to verify the Noise Level indicator. A high Noise Level indicates a source of interference in the signal path between the unit and the base station. ▪ Select another unit to verify if the base station is functioning properly. ▪ Try to optimize antenna placement to improve the Signal Level or move it away from the source of interference.

Quality Indicator is Black	None. The base station may be busy collecting diagnostic measurement results from the unit.	▪ If the indicator remains blank, click the other button to return to the Select a Remote Link Partner screen. Click the Explore button to refresh the list of Link Test Partners. If the initial partner no longer appears, it may have been switched off, or have been moved outside the range of the selected Initiator Station. ▪ Select another Link Test Partner to verify if the base station is functioning properly.

Procedure 3-5
Testing Wireless Network Performance

Testing Wireless Network Performance (Ping Fill Test)

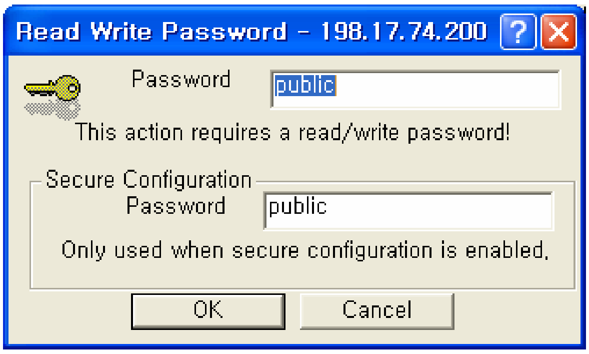
Action

Step Action

1. On the Analyze tab, click the Ping Fill Test button. The Enter IP Address screen is displayed.

   Note: The above IP address should be that of the CSU (Client of APU) which can get the IP address list box at the AP configurator.

Figure 4-43
IP Address Tab



Read Write Password - 198.17.74.200

Password: public

This action requires a read/write password!

Secure Configuration
Password: public

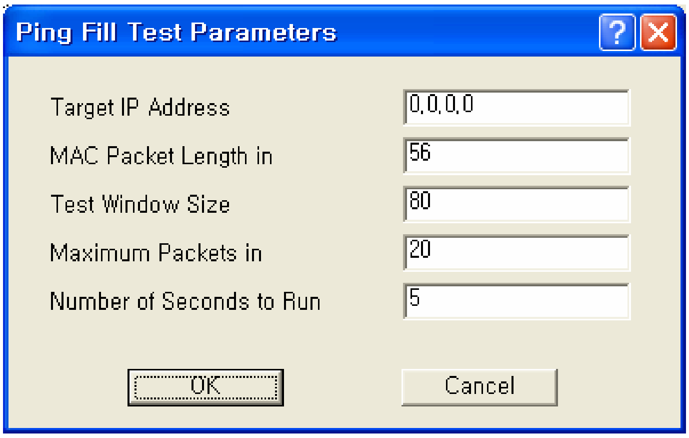
Only used when secure configuration is enabled.

2. Enter the IP address and Read/Write Password of the Internet host with which you would like to test throughput, and click the OK button. The Ping Fill Test Parameters screen is displayed. .

   Note: To test wireless performance, the target system can be one of the APU Secure Data Mode station's clients. You can also use a wired host to test wired interface performance.

3. Enter the Test Window Size, Max Packets, and Test Running Time. Ex) Packet Length: 60, Window size: 80, Maximum Packets: 20, Number of Seconds: 5
4. Click the OK button. You will see some warning messages, and then the Ping Fill test will run. The results of the test are then displayed in the Ping Fill Results screen.
5. Choosing the correct parameters is crucial to obtain the accurate Ping Fill Test results. To find out more about each of the parameters, click in the fields shown in the screenshot below.

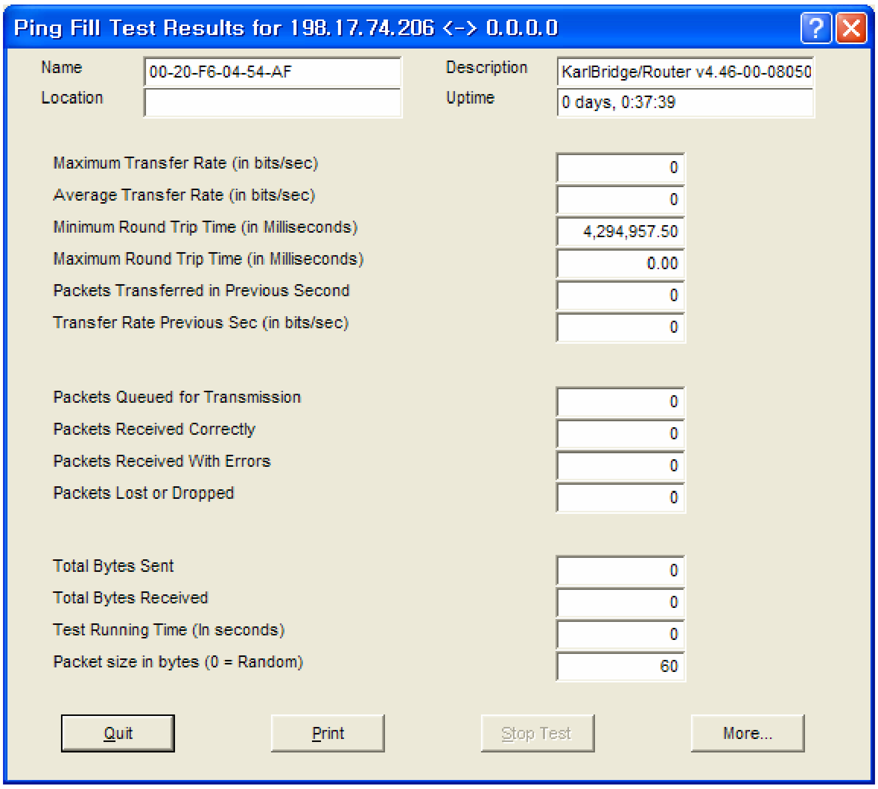
Figure 4-44
Ping Fill Test Parameters



Target IP Address	0,0,0,0
MAC Packet Length in	56
Test Window Size	80
Maximum Packets in	20
Number of Seconds to Run	5

6. As soon as Ping Fill test is over, you can see the result windows as below.
7. Record the results of Average Transfer Rate.
   It is recommended that the results window be captured as a picture and saved in the file.

Figure 4-45
Ping Fill Test Results Window



Name	00-20-F6-04-54-AF	Description	KarlBridge/Router v4.46-00-08050
Location		Uptime	0 days, 0:37:39

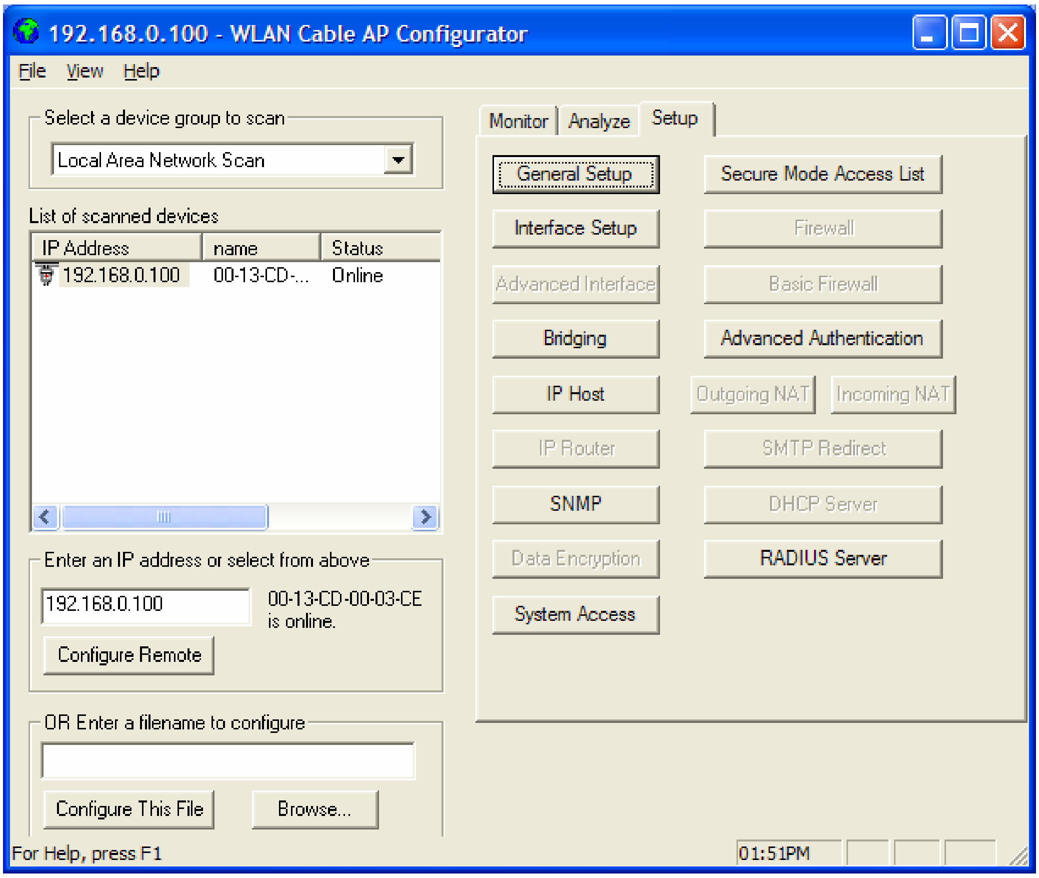
Maximum Transfer Rate (in bits/sec)	0
Average Transfer Rate (in bits/sec)	0
Minimum Round Trip Time (in Milliseconds)	4,294,957.50
Maximum Round Trip Time (in Milliseconds)	0.00
Packets Transferred in Previous Second	0
Transfer Rate Previous Sec (in bits/sec)	0
Packets Queued for Transmission	0
Packets Received Correctly	0
Packets Received With Errors	0
Packets Lost or Dropped	0
Total Bytes Sent	0
Total Bytes Received	0
Test Running Time (In seconds)	0
Packet size in bytes (0 = Random)	60

Procedure 3-5
Basic Configuration

Set Up General Configuration Options

The Setup tab is used to define the configuration options for the device, and the General Setup screen is used to enable various setup options. Click on the Setup tab, then click the General Setup button to display the General Setup screen as shown below:

Figure 4-46
General Setup window



Select a device group to scan: Local Area Network Scan

List of scanned devices

IP Address	name	Status
192.168.0.100	00-13-CD-...	Online

Enter an IP address or select from above: 192.168.0.100

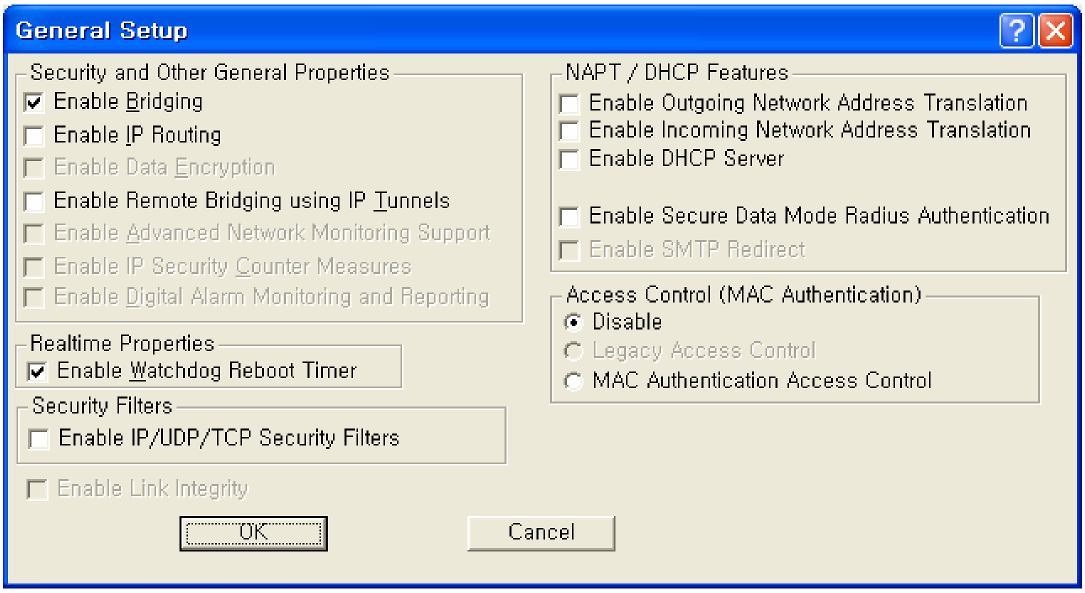
00-13-CD-00-03-CE is online.

OR Enter a filename to configure

For Help, press F1   01:51PM

Note: This menu has been modified for use in this manual. This menu has all the supported features checked (enabled) and is NOT typical of the menu you will see. Each of the fields on the screen is explained below.

Figure 4-47
General Setup window



General Setup

Security and Other General Properties
- ☑ Enable Bridging
- □ Enable IP Routing
- □ Enable Data Encryption
- □ Enable Remote Bridging using IP Tunnels
- □ Enable Advanced Network Monitoring Support
- □ Enable IP Security Counter Measures
- □ Enable Digital Alarm Monitoring and Reporting

Realtime Properties
- ☑ Enable Watchdog Reboot Timer

Security Filters
- □ Enable IP/UDP/TCP Security Filters

□ Enable Link Integrity

NAPT / DHCP Features
- □ Enable Outgoing Network Address Translation
- □ Enable Incoming Network Address Translation
- □ Enable DHCP Server
- □ Enable Secure Data Mode Radius Authentication
- □ Enable SMTP Redirect

Access Control (MAC Authentication)
- ● Disable
- ○ Legacy Access Control
- ○ MAC Authentication Access Control

Enable Bridging

Selecting this checkbox in General Setup will allow you to access the Bridge Setup screen, which you can use to enable your device’s transparent Ethernet bridging feature. This allows for the transference of Ethernet packets between physical networks connected directly to the base station.

If enabled, the base station will transfer Ethernet packets from one interface to the other (for example, between the wireless and the wired networks). The default behavior is to bridge all Ethernet protocols. You can set which Ethernet protocols to bridge or deny, as well as, Ethernet stations that will be allowed or disallowed to send packets over the bridge using Bridge Setup from the Setup tab.

If disabled, only the IP packets with correct the IP Routes set up in the IP Router Setup will be bridged between the base station's various interfaces; general Ethernet packets will not be transferred across the base station. This would be useful in a situation where you want to enable IP traffic, but not general Ethernet traffic between (sub) networks.

Enable IP Routing

Selecting this checkbox in General Setup will enable your hardware device to route IP packets between its various interfaces.

If enabled, you will need to set up routes on the IP Routing screen or you will not be able to access your hardware unit when you exit the Configurator program.

Enable Remote Bridging Using IP Tunnels

This option allows you to encapsulate Ethernet packets of any protocol in IP and then send them to another Secure Data Mode Bridge/Router to de-encapsulation. Select this checkbox to enable this capability.
Some versions of the Secure Data Mode Station support a special feature which will enable Ethernet packets of any protocol type to be encapsulated in IP and then sent to other Secure Data Mode Stations for de-encapsulation. This method can be used to set up "virtual" Ethernet LANs between several points using the IP network as the transport layer. This feature can be used to create a Virtual Private Network when used in conjunction with the Data Encryption option.

Enable Watchdog Reboot Timer

Select this item in General Setup to enable the watchdog timer reboot feature. If packets are not seen on the network for more than 10 minutes, (a very rare occurrence) the Secure Data Mode Station will reboot itself. Once it has rebooted, the 10 minute reboot timer will not activate again until a packet has been seen on one of the interfaces. This is to ensure that only one reboot will occur if the entire network is truly shut down.

Enable IP UDP/TCP Security Filters

Select this option in General Setup to enable the base station's Firewall (IP Security Filter) features. You can set the base station to explicitly or implicitly allow or deny IP connections to specific UDP or TCP ports, and/or between specific IP addresses or subnets. For more information, see Firewall Setup.
Note: This option is only available when the MAC Authentication Access Control button has been selected on the General Setup screen.

Enable Outgoing Network Address Translation

Select this checkbox if you will be using Outgoing NAT to multiplex traffic from all the computers on your internet network through the Secure Data Mode Bridge/Router.
Outgoing Network Address Translation (NAT) allows multiple computers to share a single IP address to connect to an IP network, including the Internet. This allows homes, small businesses, and Internet Service Providers to have Internet service for all of their computers without having to pay for additional IP addresses. The NAT feature

serves as a simple firewall for incoming connections, since only traffic initiated by an interior computer is permitted through the NAT.

Enable Incoming Network Address Translation

Select this checkbox if you will be using Incoming NAT to multiplex traffic from the network to all the computers on the internal network. Incoming Network Address Translations (NAT) is used to redirect requests to servers in the local address space based on the port of the request. If, for example, the client at local address 10.0.1.2 is serving web pages, and a request comes to the access point on that port for a web session, then the request will be forwarded to the web server on 10.0.1.2. The server will respond with the web page to the address of the original request.

Note: Incoming NAT only needs to be configured if servers in the local (private) Address space needs to connect with clients in the global (public) address space.

Enable DHCP Server

Select this checkbox if you are using the Secure Data Mode Bridge/ Router to provide DHCP information to the computers on your network.

Note: If you do not check this option, you will not be able to access the DHCP Server screen.

Enable Secure Data Mode Radius Authentication

Select this checkbox if you wish to enable RADIUS authentication for your Secure Data Mode stations.

Enable Network Address Translation Redirector

Select this checkbox if you wish to enable network address translation (NAT) redirection, which is used to forward the packets sent to a particular port number to a specified IP address, regardless of the original destination IP address.

Access Control Buttons

The access control buttons determine how authentication is controlled. There are three possible means of authentication control:

- Disable - Selecting Disable turns off MAC authentication entirely.
- Legacy Access Control - Selecting Legacy Access Control enables access to the Access Control Setup screen and disables access to the Advanced Authentication screen

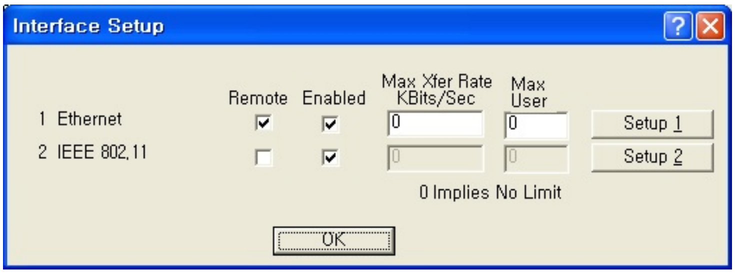
- MAC Authentication Access Control - Selecting MAC Authentication Access Control enables access to the Advanced Authentication Setup screen, which provides more detailed MAC authentication setup options, and disables access to the Access Control Setup screen.

Set Up Interfaces

Once you have enabled various configuration options, you need to define the network interfaces for your hardware device. You will typically set up one or more of the following interfaces:
As the name suggests, the Interface Setup screen is used to set up network interfaces. From the Setup tab, click the Interface Setup button. The Interface Setup screen is displayed, as shown below:

Figure 4-48
Interface setup window

Interface (APU)



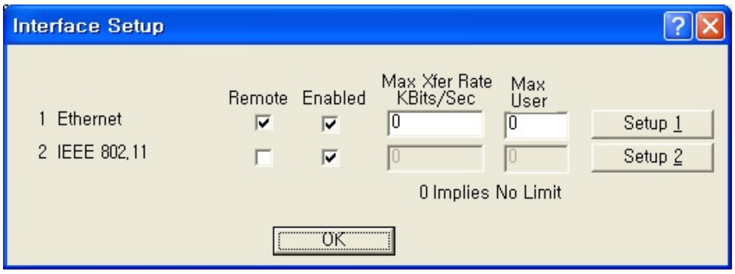
Interface Setup

	Remote	Enabled	Max Xfer Rate KBits/Sec	Max User	
1 Ethernet	☑	☑	0	0	Setup 1
2 IEEE 802.11	□	☑	0	0	Setup 2

0 Implies No Limit

OK

Interface (CSU)



Interface Setup

	Remote	Enabled	Max Xfer Rate KBits/Sec	Max User	
1 Ethernet	☑	☑	0	0	Setup 1
2 IEEE 802.11	□	☑	0	0	Setup 2

0 Implies No Limit

OK

The following rules apply for setting up network interfaces:

- You do not need to set up the Ethernet Interface.
- If you have an 802.11 radio card, click the Setup 2 button to set up the 802.11 interface.

Remote Checkbox -- Select this checkbox if all traffic coming in on this interface is to be viewed as remote traffic for firewall, bridging, filtering, and routing purposes. If this checkbox is not selected, then all traffic on this interface will be considered local traffic. Note that the “Remote” designation is significant only for the Security filters, and does not imply physical location. The security filters will pass (permit) or drop (deny) packets of particular types from being forwarded between interfaces designated as “Local” (unchecked) and those designated as “Remote.”

Note: At least one enabled interface must be a remote interface.

Enabled -- Select this checkbox if this interface should be enabled. If this box is not selected, then the base station will disable the interface and it will not be used, and the interface itself will be "down" from an administrative standpoint.

Note: At least one enabled interface must be a remote interface.

Maximum Transfer Rate (Kbits/sec) -- The maximum transfer rate is the number of bits that can be used for sending and receiving packets. If you wish to limit the maximum data transfer rate for a particular interface, enter the maximum number of kilobits per second that can be transmitted from and to the base station. This helps to reduce the risk of over-powering remote sites and to limit the bandwidth used by a particular base station.

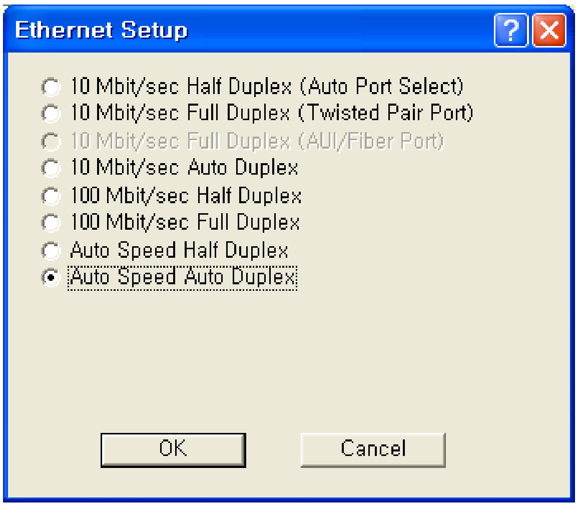
Note: The transfer rate represents the total transfer rate for both sending and receiving packets. For example, if you set the transfer rate to 10,000 Kbits (10 Mbits) per second, then 10 Mbits represents the maximum rate available for both sending and receiving packets. Therefore, if you use 7 Mbits per second in sending the packets, then only 3 Mbits per second are available for receiving packets.

Setup 1, 2, 3 -- The Setup 1, 2 buttons are used to define the available interfaces. In the screenshot shown above, clicking Setup 1 will display the Ethernet Setup screen, clicking Setup 2 will display the 802.11 Setup screen. Each of the Interface Setup screens is explained in more detail below.

Set up Ethernet

Clicking the Setup 1 button on the Interface Setup screen displays the Ethernet Setup screen.

Figure 4-49
Ethernet Setup window



Ethernet Setup

○ 10 Mbit/sec Half Duplex (Auto Port Select)
○ 10 Mbit/sec Full Duplex (Twisted Pair Port)
○ 10 Mbit/sec Full Duplex (AUI/Fiber Port)
○ 10 Mbit/sec Auto Duplex
○ 100 Mbit/sec Half Duplex
○ 100 Mbit/sec Full Duplex
○ Auto Speed Half Duplex
● Auto Speed Auto Duplex

The Secure Data Mode station will automatically set up the Ethernet interface to use the type of medium that has been connected to the unit. By default, the Ethernet connection is set at “Auto speed auto duplex.” Therefore, you do not need to configure special settings for the Ethernet hardware interface. If you wish to customize the Ethernet settings, you can change the settings listed below. However, you do not need to change any settings for your hardware device to be functional.

- The Secure Data Mode Station supports both Ethernet IEEE 802.3 and DIX Ethernet frame types.
- Protocols are set in the Interface Setup window of the Setup Tab.

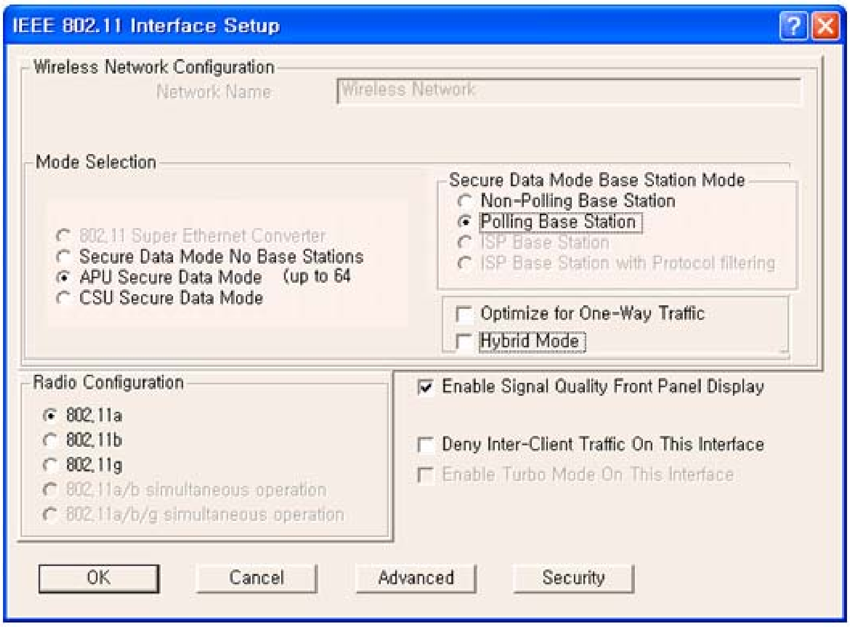
Note: Do not change the default setup “Auto speed Auto Duplex” in this setup window without consulting the manufacturer.

Ethernet Type -- The Ethernet type options provide a variety of Ethernet settings. The default value for Ethernet type will vary, depending on your hardware device. Only the settings that are enabled on your screen are supported by your particular hardware device. If your switch or Ethernet card supports different speeds, you may want to change the speed setting.

Set Up 802.11

Clicking the Setup 2 button on the Interface Setup screen displays the 802.11 Setup screen. The 802.11 Setup screen is used to set up the interface to your 802.11 network devices.

Figure 4-50
802.11 Radio Interface Setup window (APU Secure Data Mode)



IEEE 802.11 Interface Setup

Wireless Network Configuration
Network Name: Wireless Network

Mode Selection
○ 802.11 Super Ethernet Converter
○ Secure Data Mode No Base Stations
● APU Secure Data Mode (up to 64
○ CSU Secure Data Mode

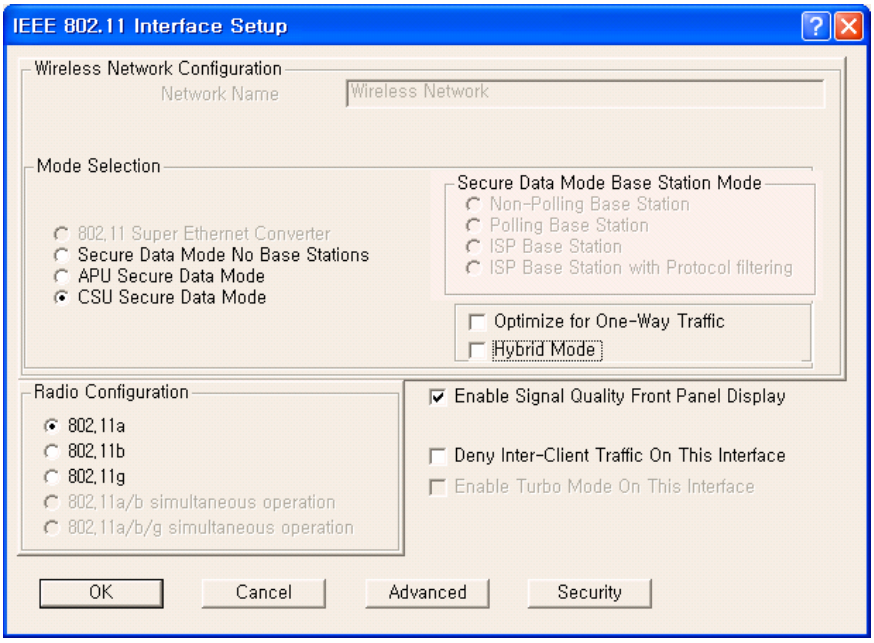
Secure Data Mode Base Station Mode
○ Non-Polling Base Station
● Polling Base Station
○ ISP Base Station
○ ISP Base Station with Protocol filtering

□ Optimize for One-Way Traffic
□ Hybrid Mode

Radio Configuration
● 802.11a
○ 802.11b
○ 802.11g
○ 802.11a/b simultaneous operation
○ 802.11a/b/g simultaneous operation

☑ Enable Signal Quality Front Panel Display
□ Deny Inter-Client Traffic On This Interface
□ Enable Turbo Mode On This Interface

Figure 4-51
802.11 Radio Interface Setup window (CSU Secure Data Mode)



IEEE 802.11 Interface Setup

Wireless Network Configuration
Network Name: Wireless Network

Mode Selection
○ 802.11 Super Ethernet Converter
○ Secure Data Mode No Base Stations
○ APU Secure Data Mode
● CSU Secure Data Mode

Secure Data Mode Base Station Mode
○ Non-Polling Base Station
○ Polling Base Station
○ ISP Base Station
○ ISP Base Station with Protocol filtering

□ Optimize for One-Way Traffic
□ Hybrid Mode

Radio Configuration
● 802.11a
○ 802.11b
○ 802.11g
○ 802.11a/b simultaneous operation
○ 802.11a/b/g simultaneous operation

☑ Enable Signal Quality Front Panel Display
□ Deny Inter-Client Traffic On This Interface
□ Enable Turbo Mode On This Interface

802.11 Network Name-- The 802.11 Network Name is used in standard IEEE 802.11 networks to distinguish stations in your 802.11 network from stations that belong to a neighboring 802.11 network.

The value used for the radio interface on this station should be the same for all wireless stations in the 802.11 network. Only stations configured with the proper 802.11 Network Name will be able to connect to the 802.11 station's radio interface.
The Network Name can be any alphanumeric string in the range of "a" to "z," "A" to "Z" and "0" to "9," and can contain from 1 to 32 characters.

If you wish to allow access to the wireless network to be open to all wireless stations, the Network Name should be set to ANY.

Note: The Network Name is used only when the 802.11 radio interface (for example, Orinoco) is set to run in IEEE 802.11ccess Point Mode.

Secure Data Mode No Base Stations-- Select this option to set your 802.11 device's radio card on this interface to run as a Secure Data Mode Network without a Secure Data Mode Base Station (i.e. peer-to-peer).

Use this setting only in the rare instance when all Secure Data Mode stations are able to "see" each other (i.e., there are no hidden nodes).

When all connected Secure Data Mode Stations are not able to "'see" one another, this setting should not be used. In that case, you should set one of your Secure Data Mode Station stations to Secure Data Mode Base Station, and the others to Remote (Satellite) Secure Data Mode Stations.

APU Secure Data Mode-- Selecting this option sets the Secure Data Mode Station to run as a Secure Data Mode Base Station over the 802.11 device's radio interface. Every system that needs to connect to the wireless network must be able to connect to the Secure Data Mode Base Station.

When you select this Base Station type, you must select one of the Protocol Filtering Modes. The Protocol Filtering Mode determines how the base will interact with the satellite (slave) stations. Is it recommended that you use the Enable Filters between Slaves mode.

The possible base station modes are as follows:

Non-Polling Base Station

The non-polling Secure Data Mode Base Station Mode is provided mostly for compatibility with older Secure Data Mode Networks, but may give increased performance over other (polling) Secure Data Mode Base Station modes in a lightly loaded network, or in a network with only a few satellites.

Setting a base station to non-polling mode may increase performance in the rare case where all satellites can hear one another (i.e. there are no hidden nodes), or when there is sporadic network use. In an environment where most network traffic is with one satellite, and other satellites rarely transmit data, this setting may also increase performance. However, it is highly recommended that you select one of the polling modes.

Selecting this Secure Data Mode Base Station Mode takes full advantage of the features of a Secure Data Mode Network.

Polling Base Station

Selecting this Secure Data Mode Base Station Mode sets the Secure Data Mode Station to run as a Secure Data Mode Base Station which performs a highly optimized Nortel Networks-proprietary polling of the satellite stations for data. In the Non-Polling Base Station mode, all wireless stations must be able to 'hear' each others' traffic, or performance may degrade considerably (the hidden node problem). In polling mode, the Base Station will poll each station for data, and also offer the opportunity for 'free-for-all' sending of data at set intervals.

In conjunction with the standard features of the Secure Data Mode Network, this Secure Data Mode Base Station Mode offers a significant performance increase over other wireless protocols when the network is under a heavy load.

ISP Base Station

Selecting this Secure Mode Base Station sets the Secure Mode Station to run as a base station for connections to Microsoft Windows PC Clients. This mode takes full advantage of the features of a Secure Mode Network and allows Windows clients to connect directly to the base station, eliminating the need for an Ethernet connection to a second Secure Mode Station running as a Remote Secure Mode Station.

The following Windows clients are supported:

- Windows 95a (with the Winsock 2 update)
- Windows 95b
- Windows 98
- Windows NT 4.0
- Windows XP

To filter Ethernet protocols that are transferred between the wireless stations (for example, to disable the Windows Network Neighborhood), select ISP Base Station with Protocol Filtering. Filters set in Bridge

Setup... are not applied to wireless-only traffic in the non-filtering ISP Secure Data Mode Base Station Mode.

We strongly recommend that you set your Secure Data Mode Base Station to ISP Base Station with Protocol Filtering mode when connecting Windows PC Client satellites.

ISP Base Station with Protocol Filtering

Selecting this Secure Data Mode Base Station Mode gives you the same functionality of the ISP Base Station mode, with an added filtering function that applies the bridge filters set in Bridge Setup to traffic sent over the wireless network as well.

With the non-filtering ISP Secure Data Mode Base Station Mode, all traffic between two wireless stations is permitted. Bridge filters do not apply to wireless-only traffic in the non-filtering ISP Secure Data Mode Base Station Mode.
When using the ISP Base Station with the Protocol Filtering setting, you can set the bridge filters so that each wireless machine (or LAN behind another connected Secure Data Mode Station) is 'hidden' from all other machines or LAN's connected to the Secure Data Mode Network. Properly setting up Protocol Filtering will disable the Windows 'Network Neighborhood' from seeing other machines connected on the wireless network. If you do not deny IP and IP-ARP packet types in Protocol Filtering, wireless machines are still able to connect to each other via IP packets, including TCP and UDP. Permitting only IP traffic over the wireless network will allow your wireless clients to interact as if they were connected to the Internet, but not together on a private network. For added security, the firewall features of the bridge can be used to deny certain types of IP packets from flowing between the wireless stations.

We strongly recommend that you select ISP Base Station with Protocol Filtering when the Secure Data Mode Base Station will service satellites running the PC Client.

CSU Secure Data Mode-- Selecting this option in IEEE 802.11 sets the Secure Data Mode Station to Connect to an APU Secure Data Mode Station over this 802.11 device’s radio interface.

To properly use this setting, you must be sure that the following items match the APU Secure Data Mode Station Settings:

- Network ID(NWID)
- System Access Pass phrase
- Frequency Channel

Enable Signal Quality Front Panel Display-- On units that have a front panel display that is capable of displaying the signal quality, selecting this checkbox will enable the signal quality display.

Deny Inter-Client Traffic on this Interface-- Select this checkbox if you wish to prevent wireless stations from sending packets to each other directly. Usually, the AP will repeat station-to-station traffic and will not send it to the bridge and firewall filters. This is because bridging routines historically work between physical interfaces only.

An Ethernet packet sent between two Ethernet hosts on the same Ethernet subnet will automatically be seen by the destination host. With wireless, the packet must be repeated by the AP. This turns off the AP’s packet repeating code.

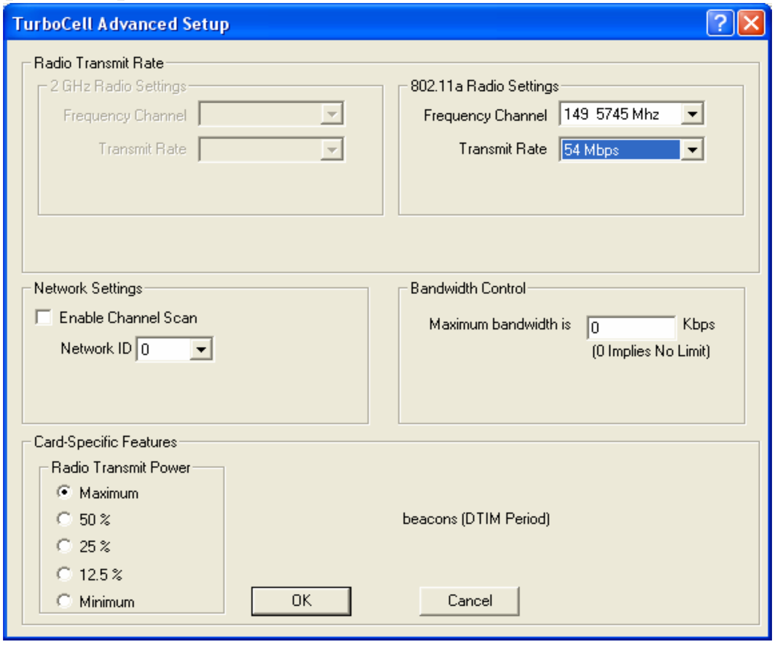
Secure Data Mode Advanced Setup

Clicking the Advanced Button on the 802.11 Setup screen displays the 802.11 advanced Setup screen, which allows you to configure more options related to the setup of your 802.11 network device.

The appearance of the 802.11 Setup screen varies depending on which options are set on the 802.11 Setup screen. The 802.11 Advanced Setup screen for a Secure Data Mode Base Station is shown below.

Figure 4-52
Advanced setup dialog box

[802.11a]



TurboCell Advanced Setup

Radio Transmit Rate

2 GHz Radio Settings
Frequency Channel
Transmit Rate

802.11a Radio Settings
Frequency Channel: 149 5745 Mhz
Transmit Rate: 54 Mbps

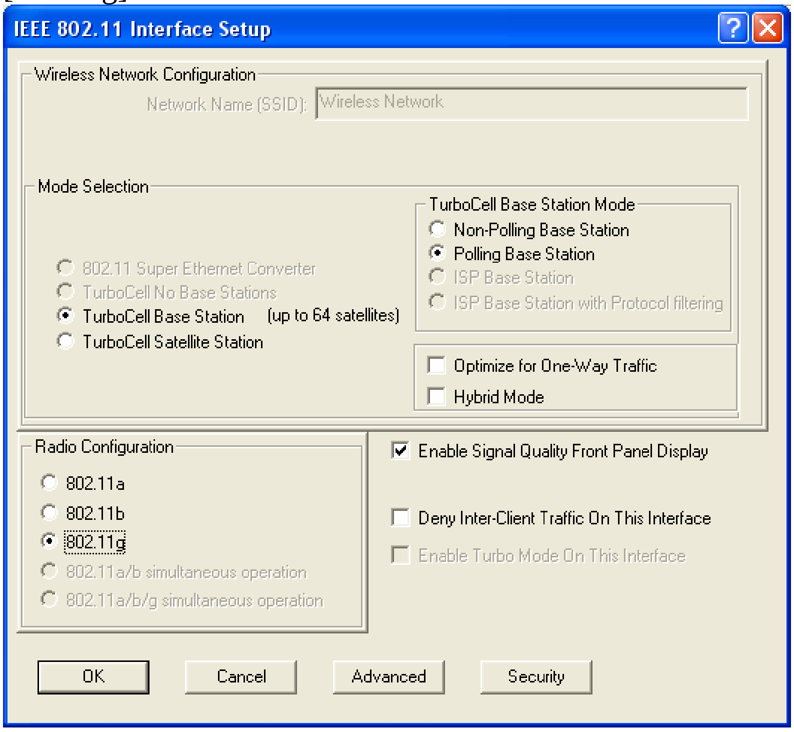
Network Settings
□ Enable Channel Scan
Network ID: 0

Bandwidth Control
Maximum bandwidth is 0 Kbps
(0 Implies No Limit)

Card-Specific Features
Radio Transmit Power
● Maximum
○ 50 %
○ 25 %
○ 12.5 %
○ Minimum

beacons (DTIM Period)

[802.11g]



IEEE 802.11 Interface Setup

Wireless Network Configuration

Network Name (SSID): Wireless Network

Mode Selection

○ 802.11 Super Ethernet Converter
○ TurboCell No Base Stations
● TurboCell Base Station (up to 64 satellites)
○ TurboCell Satellite Station

TurboCell Base Station Mode
○ Non-Polling Base Station
● Polling Base Station
○ ISP Base Station
○ ISP Base Station with Protocol filtering

□ Optimize for One-Way Traffic
□ Hybrid Mode

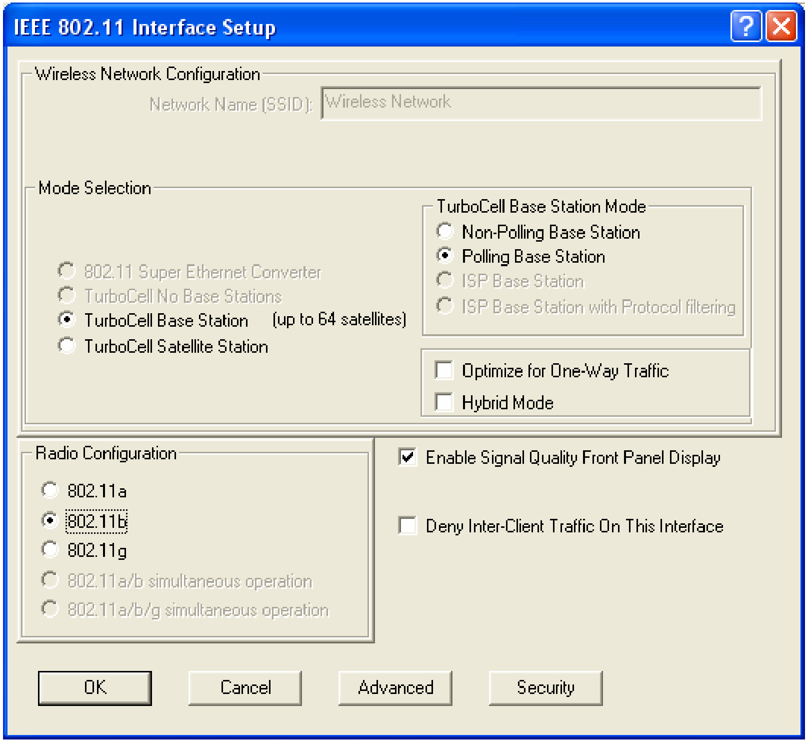
Radio Configuration
○ 802.11a
○ 802.11b
● 802.11g
○ 802.11a/b simultaneous operation
○ 802.11a/b/g simultaneous operation

☑ Enable Signal Quality Front Panel Display

□ Deny Inter-Client Traffic On This Interface

□ Enable Turbo Mode On This Interface

[802.11b]



IEEE 802.11 Interface Setup

Wireless Network Configuration

Network Name (SSID): Wireless Network

Mode Selection

○ 802.11 Super Ethernet Converter
○ TurboCell No Base Stations
● TurboCell Base Station (up to 64 satellites)
○ TurboCell Satellite Station

TurboCell Base Station Mode
○ Non-Polling Base Station
● Polling Base Station
○ ISP Base Station
○ ISP Base Station with Protocol filtering

□ Optimize for One-Way Traffic
□ Hybrid Mode

Radio Configuration
○ 802.11a
● 802.11b
○ 802.11g
○ 802.11a/b simultaneous operation
○ 802.11a/b/g simultaneous operation

☑ Enable Signal Quality Front Panel Display

□ Deny Inter-Client Traffic On This Interface

Network ID-- Enter the Secure Data Mode network ID number (0-15) used to differentiate between multiple Secure Data Mode stations using the same System Access Pass Phrase. This is used to allow a Secure Data Mode satellite to specify the Base Station it wants to connect to if two base stations can be seen by the same satellite. Generally, this value should be the same as the Channel Number.

802.11 Frequency Setup-- Click the Frequency button on the 802.11 Setup screen displays the 802.11 Frequency Setup screens, which allows you to set the Frequency Channel for your 802.11 radio card.

The 802.11 Frequency Setup screen is used to change the channel and frequency for one of the remote devices on your network. Note that this screen is only accessible if you have identified remote devices in your network. If all devices are in your local network, then the Frequency Setup screen is unavailable.

Channel/Frequency-- Select the channel and frequency for the remote device from the drop-down list.   See Frequency Channels for a more detailed explanation of the frequency channels.

[802.11a]

Frequency Channel	
149	5745 MHz
153	5765 MHz
157	5785 MHz
161	5805 MHz

[802.11b/g]

Frequency Channel		6	2437 MHz
1	2412 MHz	7	2442 MHz
2	2417 MHz	8	2447 MHz
3	2422 MHz	9	2452 MHz
4	2427 MHz	10	2457 MHz
5	2432 MHz	11	2462 MHz

Radio Transmit Rate-- Select the radio bit rate used to transmit. Your choices are:

[802.11a]

Transmit Rate	
6Mbps	36Mbps
9Mbps	48Mbps
12Mbps	54Mbps
24Mbps	

[802.11g]

Transmit Rate	
54 Mbps	6 Mbps
48Mbps	11 Mbps
36 Mbps	5.5 Mbps
24 Mbps	2 Mbps
12 Mbps	1 Mbps

[802.11b]

Transmit Rate
11 Mbps
5.5 Mbps
2 Mbps
1 Mbps

A lower signal will increase the noise. In essence, the poorer the signal-to-noise ratio, the lower this rate should be set.

Note: The transmit rate affects only the transmissions made by this station.

Note: In case of 802.11b/g, the channel/frequency values are usually determined by network administrators. If you set the channel and frequency ensure that there are at least four numerical channels difference between two overlapping cells to avoid interference. For example, channels 1, 6 and 11 don't overlap, but channels 1 and 3 do.

In the other side, if you are intended to use 802.11a, please keep in mind that all channels (4 channels) with 20MHz bandwidth are not permitted to be overlapped with each channels in the frequency plan.

Radio Transmit Power -- Select the Transmit power in the list of five (4) power levels as below.

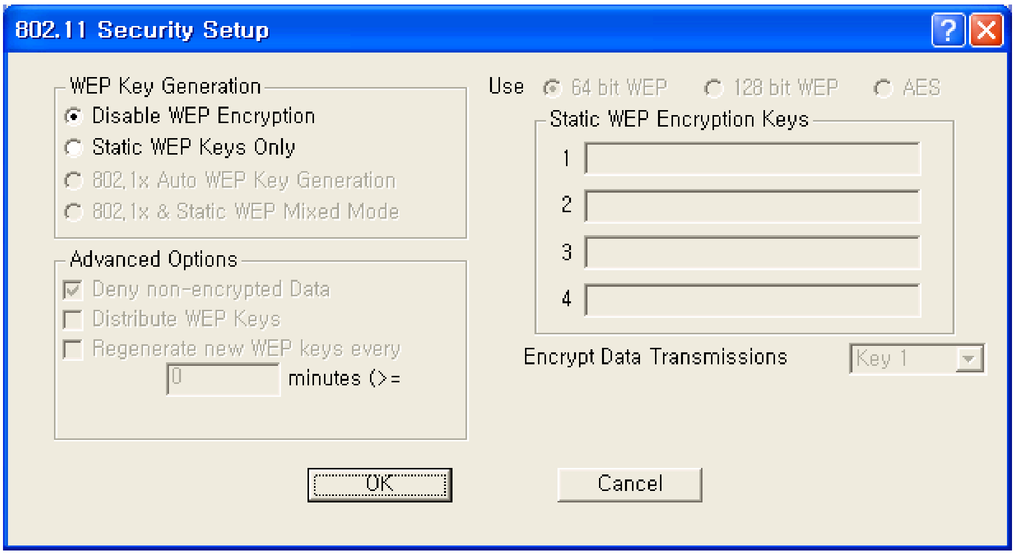
Transmit Power	Antenna Gain
Maximum	The allowed antenna gain per unit varies with actual transmit power of APU and CSU.
50%	
25%	
12.5%	

Note: It is recommended that you set the transmit power to "Maximum" as the antenna listed in Appendix C (Antenna) has been designed to meet FCC regulation to restrict the actual transmit power (EIRP) at the maximum transmit power.

802.11 Security Setup

Clicking the Security button on the 802.11 Setup screen displays the 802.11 Security Setup screen, which allows you to set up security for your 802.11 devices. Note that the fields shown in the screenshot below will vary depending on the version of the Configurator you are using and the options contained in the .bin file. The screen below shows all available options.

Figure 4-53
802.11 Security Setup window



WEP Key Generation
● Disable WEP Encryption
○ Static WEP Keys Only
○ 802.1x Auto WEP Key Generation
○ 802.1x & Static WEP Mixed Mode

Advanced Options
☑ Deny non-encrypted Data
□ Distribute WEP Keys
□ Regenerate new WEP keys every
0 minutes (>=

Use ● 64 bit WEP ○ 128 bit WEP ○ AES

Static WEP Encryption Keys
1
2
3
4

Encrypt Data Transmissions Key 1

Disable WEP Encryption-- Select this button if you wish to disable Wired Equivalent Privacy (WEP) encryption.
If you are not concerned about security (for example, home users using this device only to browse the Internet), and if you are not concerned your AP is used by others, then select this checkbox.

Note: For simple security, you can disable WEP encryption and select the Closed Wireless System checkbox.

Static WEP Keys Only-- Select this button if you wish to enter Wired Equivalent Privacy (WEP) keys identically on each access point/station and Secure Data Mode unit in the network. When you select this button, the four Static EP Encryption key fields are enabled on the right side of the screen.

Deny Non-Encrypted Data-- Select this checkbox if you want to deny all received data that is not encrypted. When this checkbox is selected, any packet received that is not encrypted using one of the four WEP Encryption keys listed above will be dropped. When this checkbox is not selected, unencrypted packets will be accepted and/or forwarded.

Warning: You should always select this checkbox if WEP is enabled in any form. If disabled, clients without WEP can access your network!

Use n-bit WEP Keys-- Select either 64-bit (silver) or 128-bit (gold) encryption keys. The higher bit count provides somewhat higher security.

AES(Advanced Encryption Standard)—If you want more secured encryption than n-bit WEP, you can choose this option with which 16 character string's keys are supportable for Atheros based untis.

Static WEP Encryption Keys-- If you use static encryption keys, you must enter each key in the Static WEP Encryption Keys fields. Note that these keys must be entered identically on each access point/station and Secure Data Mode unit in the network.

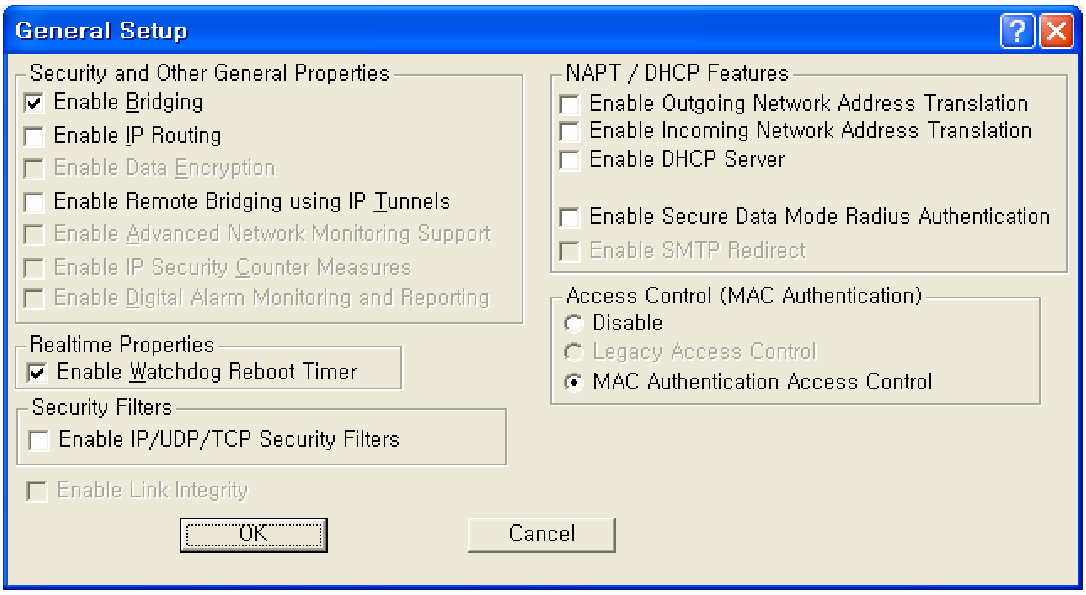
Encrypt Data Transmission Using Key n-- Enter the key number that should be used to encrypt data on this interface. Note that you can receive using any key, but will generally always transmit using a single key. Unicast transmissions to an 802.1x station with dynamic keys will use that's station's dynamic key, but all broadcasts, multicasts, and other unicasts will be encrypted using the key identified in this field.

Configure the APU for Basic MAC Authentication

Advanced Authentication allows you to restrict access to an 802.11 access point by specifying the MAC Addresses of stations that can use the wireless bridge

1. Select the Setup Tab, and then click the General Setup button. The General Setup screen is displayed, as shown below.
2. Select the MAC Authentication Access Control radio button, as shown in the screenshot, then click OK to close the General Setup screen.
3. Click the Advanced Authentication button. The Advanced Authentication Setup screen is displayed, as shown in Figure 4-55.

Figure 4-54
General Setup Window



General Setup

Security and Other General Properties

☑ Enable Bridging
□ Enable IP Routing
□ Enable Data Encryption
□ Enable Remote Bridging using IP Tunnels
□ Enable Advanced Network Monitoring Support
□ Enable IP Security Counter Measures
□ Enable Digital Alarm Monitoring and Reporting

Realtime Properties

☑ Enable Watchdog Reboot Timer

Security Filters

□ Enable IP/UDP/TCP Security Filters

□ Enable Link Integrity

NAPT / DHCP Features

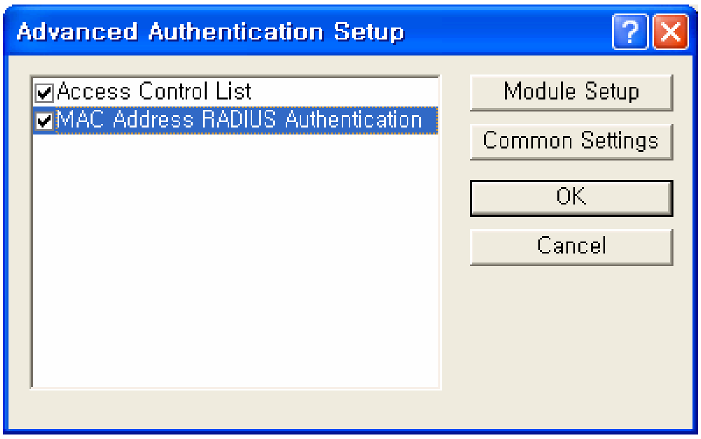
□ Enable Outgoing Network Address Translation
□ Enable Incoming Network Address Translation
□ Enable DHCP Server

□ Enable Secure Data Mode Radius Authentication
□ Enable SMTP Redirect

Access Control (MAC Authentication)

○ Disable
○ Legacy Access Control
● MAC Authentication Access Control

Figure 4-55
Advanced Authentication Setup Window



Advanced Authentication Setup

☑ Access Control List
☑ MAC Address RADIUS Authentication

When a station tries to connect to the hardware device (via Ethernet, 802.11, etc.), the AP can decide whether or not to forward packets to or from that station based on authorization criteria. There are three authentication modules that comprise MAC authentication, but the network administrator determines which of those three modules are used.

- Access Control List (ACL)
- MAC RADIUS Authentication (with optional WARP support)

These modules are enabled on a per-interface basis. This provides greater control for the network administrator. In essence, the

administrator decides whether there will be more or less (or no) authentication on an interface-by-interface basis.
For example, an administrator can permit MAC addresses entered as part of the ACL only on 802.11, but can permit MAC addresses entered through RADIUS Setup for both the Ethernet and 802.11 interfaces.

The modules are checked in the order in which they appear on the Advanced Authentication Setup screen, and the options that have been selected (checked) determine how authentication is carried out. Assuming that all options are selected, the first method used is the Access Control List, followed by MAC Address Radius, followed by 802.1x authentication. If no options are selected, then no authentication takes place. Zero to three of the modules can be enabled, but at least one module must be enabled for advanced authentication to take place.

The process by which authentication takes place is as follows:

- The first module in the list (for example, ACL) checks the source address of the incoming packet to see if it is permitted to send packets on the selected interfaces.
- The module will designate the address as one of the following:

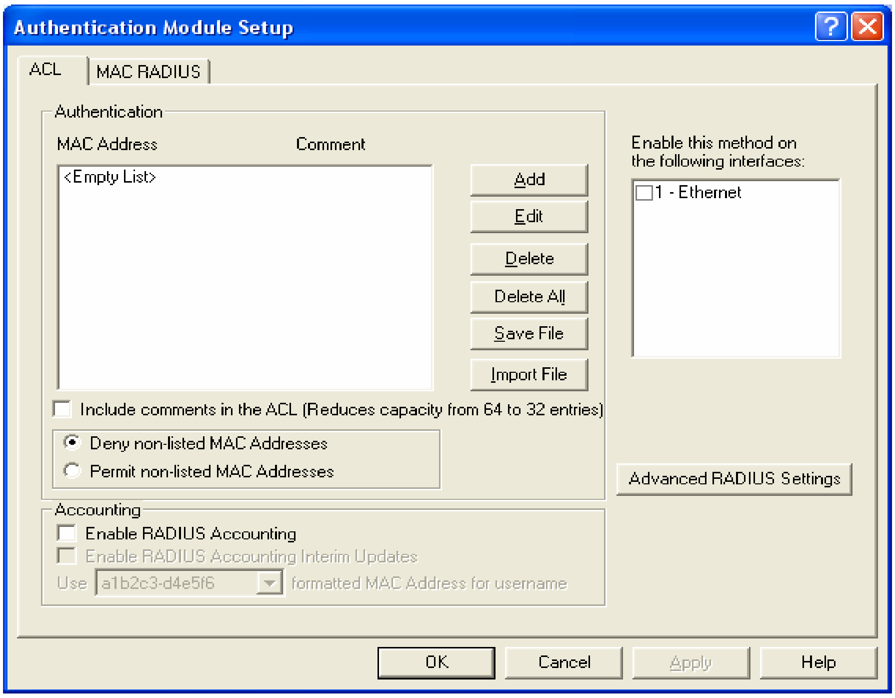
  - **Permit** -- the MAC address is permitted on this interface, and packets are forwarded
  - **Deny** - the MAC address is denied on this interface, and the packets are not sent
  - **Unknown** - the MAC address is not known on this interface, and is passed to the next authentication module

- If the designation is unknown, then it is passed to the next module in the list (for example, from the ACL to MAC RADIUS Authentication), and the process starts again.

- Ensure that the MAC Address RADIUS Authentication checkbox is enabled, and then click the Setup button. The Authentication Module Setup screen is displayed as shown below.

Note: The number of tabs displayed on this screen will vary depending on which Advanced Authentication options you have selected on the Advanced Authentication Setup screen. In the screenshot below, all Advanced Authentication options have been enabled.

Figure 4-56
Authentication Module Setup Window



Authentication Module Setup

ACL | MAC RADIUS

Authentication

MAC Address — Comment

<Empty List>

□ Include comments in the ACL (Reduces capacity from 64 to 32 entries)

● Deny non-listed MAC Addresses

○ Permit non-listed MAC Addresses

Enable this method on the following interfaces:

□ 1 - Ethernet

Accounting

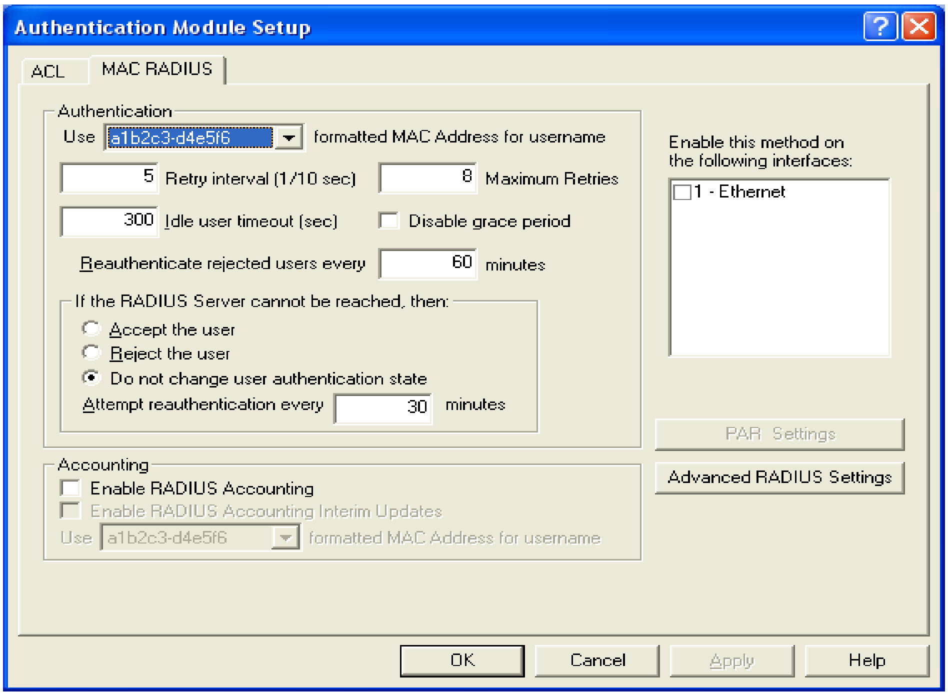
□ Enable RADIUS Accounting

□ Enable RADIUS Accounting Interim Updates

Use a1b2c3-d4e5f6 formatted MAC Address for username

4. Click the MAC RADIUS tab. The MAC RADIUS Setup screen is displayed, as shown below.

Figure 4-57
Authentication Module Setup Windows



Authentication Module Setup

ACL | MAC RADIUS

Authentication

Use a1b2c3-d4e5f6 formatted MAC Address for username

5 Retry interval (1/10 sec) — 8 Maximum Retries

300 Idle user timeout (sec) — □ Disable grace period

Reauthenticate rejected users every 60 minutes

If the RADIUS Server cannot be reached, then:

○ Accept the user

○ Reject the user

● Do not change user authentication state

Attempt reauthentication every 30 minutes

Enable this method on the following interfaces:

□ 1 - Ethernet

Accounting

□ Enable RADIUS Accounting

□ Enable RADIUS Accounting Interim Updates

Use a1b2c3-d4e5f6 formatted MAC Address for username

The MAC RADIUS Setup screen is used to define advanced authentication and accounting options for clients that are authenticated via RADIUS using the client's MAC Address as the RADIUS username. RADIUS authentication and accounting server IP addresses and port numbers are set up using the MAC RADIUS Setup screen. Note that this particular MAC RADIUS module applies only to Ethernet and 802.11 access point interfaces.

This screen is used in conjunction with the RADIUS Server Setup screen to define various authentication options. If you wish to use accounting, you must first set up accounting parameters on the RADIUS Server Setup screen.

5. Enter values in the RADIUS Server Setup screen to configure your RADIUS server. Each field on the screen is explained in more detail below.

Use formatted MAC Address for username-- Select “A1-2B-3C-45-CD-EF” if you wish to use all uppercase formatting for MAC address accounting. This format corresponds to the new RFC RADIUS standards.

Select a1b2c3-d4e5f6 if you wish to use the older formatting of MAC addresses. Select the EAP packet username if you wish to use the EAP packet username (802.1x Authentication only).

Enable this method on the following interfaces.

Select the interfaces used for MAC RADIUS authentication.

Note: You can select either the Ethernet or 802.11 interfaces if you wish to use WARP.

Retry Interval-- The retry interval for authentication, in tenths of a second. The default value is 5, or a retry interval of .5 seconds. You can set the retry interval to any value between 3 (.3 seconds) and 30 (3 seconds).

Maximum Retries-- The number of times the access point will retry to connect with the server. The default value is 8(eight), and the range for retries is between 1(one) and 10(ten).

Idle User Timeout **(**sec**)**

Enter a value in this field if you wish to disconnect users after a period of inactivity. The value entered will be the number of seconds that must pass without activity before users are disconnected.
The default value is 300 seconds (or five minutes). The range of accepted values is between 0 and 3825.

Disable Grace Period -- The grace period allows a client to roam between access points without losing open TCP connections. Select this checkbox if you wish to disable the grace period. If selected, the user does not receive a grace period; if unselected, the user receives a grace period.

Note: The Grace Period must be enabled (unchecked) if you wish to use WARP.

Re-authenticate Rejected Users Every n Minute -- Select the interval at which users who have not been authenticated will be allowed to re-authenticate. The default interval is 60 minutes.

Accept the User-- Select this radio button if you wish to allow network access to the user if the RADIUS server is down.

Reject the User -- Select this radio button if you wish to deny network access to the user if the RADIUS server is down.

Do not change user authentication state-- Select this checkbox if you wish to keep the user authentication state the same as that before the RADIUS server went down. When this checkbox is selected, if the user was authenticated before the server went down, then the user will remain authenticated. If the user was not authenticated before the RADIUS server went down, then the user will remain unauthenticated.

Note: This field is used in conjunction with the "After n Failed Authentication Attempts and "Make users wait n seconds" fields.

Attempt Re-authentication Every n Minutes -- If the RADIUS server cannot be reached, the access point will attempt to authenticate all clients via the RADIUS server according to the interval specified here. The re-authentication interval must be specified in increments of 15 minutes. Valid values are 15, 30, 45, etc.

Enable RADIUS Accounting --Select this button if you wish to enable RADIUS accounting. Accounting keeps track of the number of bytes and packets sent by a client. It also keeps track of the amount of time a client has been authenticated. You will want to select this button if you wish to monitor the amount of traffic a client passes, or the amount of time a user is logged on. Typically, you will do this if you wish to bill the client based on time or traffic.

Note: Accounting must be used with authentication. You cannot use accounting without authentication.

Enable RADIUS Accounting Interim Updates -- Select this checkbox if you wish to allow RADIUS accounting updates. If this feature is enabled, the number of bytes and packets sent by a client will be updated according to the update interval defined on the Advanced RADIUS Setup screen.

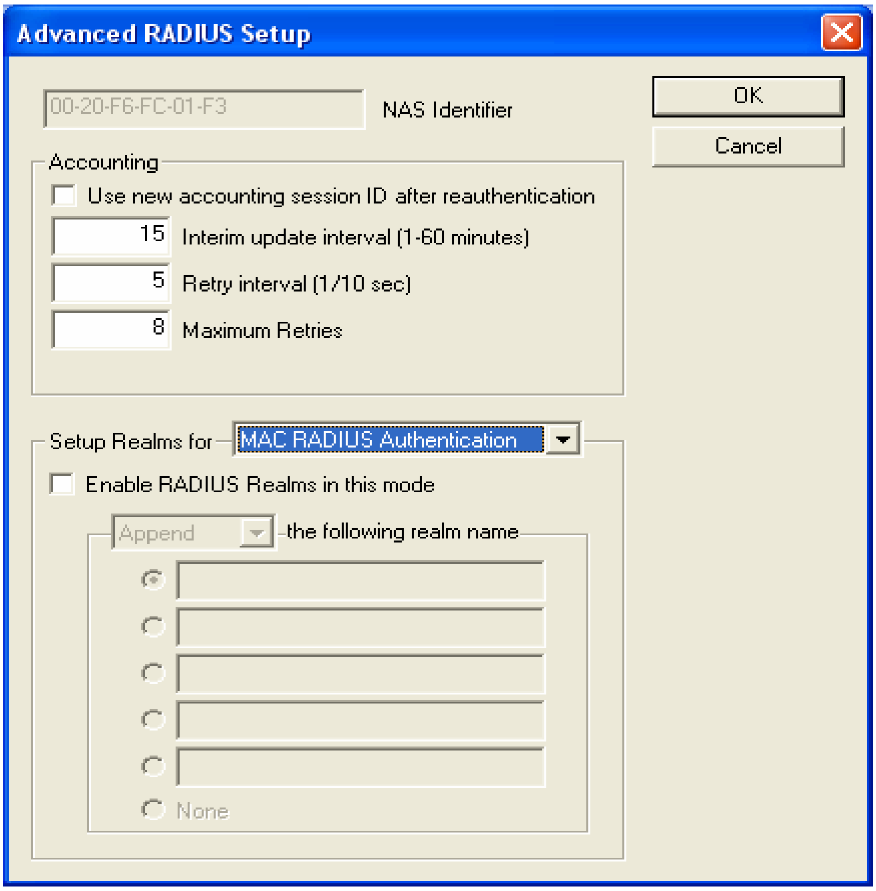
WARP Settings Button -- Clicking this button displays the WARP Settings screen, which allows you to define various IP addresses and ports that will be used for Wireless Authentication and Registration Protocol (WARP).

Advanced RADIUS Settings Button -- Clicking this button displays the Advanced RADIUS Settings screen, which enables you to define more advanced RADIUS parameters.

Configure the APU for Advanced RADIUS MAC Authentication

1. From the MAC RADIUS Setup screen, click the Advanced RADIUS Settings button. The Advanced RADIUS Setup screen is displayed, as shown below.

Figure 4-58
Advanced RADIUS Setup Window



00-20-F6-FC-01-F3 NAS Identifier

Accounting

□ Use new accounting session ID after reauthentication

15 Interim update interval (1-60 minutes)

5 Retry interval (1/10 sec)

8 Maximum Retries

Setup Realms for MAC RADIUS Authentication

□ Enable RADIUS Realms in this mode

Append the following realm name

●
○
○
○
○
○ None

The Advanced RADIUS Setup screen is used to configure optional RADIUS-related parameters.

2. Enter values in the Advanced RADIUS Setup screen, as indicated by the field descriptions below.

NAS Identifier - This field displays your Network Access Server (NAS) name. The access point's SNMP System Name is used as the NAS Identifier, and is shown here for your convenience.

Note: The NAS ID takes the place of the IP address that would normally be used to identify the AP.

Use New Accounting Session ID After Authentication -- Select this checkbox if you wish to use another ID for accounting after authentication has taken place.

Interim Update Interval -- Set the interval (in minutes) between interim updates. The interim update is used to send information in between normal "start/stop" packets. Interim updates are useful because they provide a log of network traffic at a regular interval.

The default value for the interim update interval is 15 minutes. The interim update must be between 1 - 60 minutes.

Retry Interval (1/10 sec) -- The retry interval for accounting, in tenths of a second. The default value is 5 (or a retry interval of .5 seconds). You can set the retry interval to any value between 3 and 30.

Maximum Retries -- The number of times the access point will retry to connect with the server. The default value is 8, and the range for retries is between 1 and 10.

Set Up Realms for -- When an access client sends user credentials, a user name is often included. Within the user name are two elements:

- Identification of the user account name
- Identification of the user account location

For example, for the user name user1@microsoft.com, user1 is the user account name and microsoft.com is the location of the user account. The identification of the location of the user account is known as a realm.

With RADIUS, a realm is used to separate one name space from another. This allows you to create a login such as user@dom1.com and another login such as user@dom2.com. RADIUS realms also allow Internet Service Providers (ISPs) to segment customer logins, so authentications go to the appropriate RADIUS server(s).

A domain is registered with the InterNIC, and used for mapping servers and services to IP addresses, such as Web, e-mail, etc. Typically, a RADIUS realm corresponds to a domain name (e.g., microsoft.com; yahoo.com). However, there is no requirement to do so, and in fact ISPs often assign realms with no top-level domain (for example, user@dom1 -- without a .com extension).

From the dropdown list, select the accounting or authorization feature for which to provide special handling of <RADIUS realms>. Options currently include:

- Access Control List (ACL) RADIUS Accounting
- MAC RADIUS Accounting
- MAC RADIUS Authorization

For each of the above Authentication/Accounting types, special handling of RADIUS Realms can be enabled or disabled using the "Enabled RADIUS Realms in this mode" checkbox. Depending on the selected Authentication/Accounting type, different options are available for how to handle RADIUS realms.

Following Realm Name -- Select the type of behavior that will be used for the realm. The behavior determines how the access point handles the realm. Select one of the following realm types:

Append -- Takes the user supplied user name, and appends the realm name onto it (for example, if the user name is smith and the realm name is microsoft.com, then the append action produces smith@microsoft.com)

Supply -- Supplies the selected realm name if the user does not already have one selected. If the user provided a realm name, then use the provided realm name, and do not use the one provided.

- Example #1: User provided smith, Behavior is set to Supply, and user did not provide a realm name. The supply action produces jsmith@microsoft.com.
- Example #2: User provided smith, Behavior is set to Supply, and user provided the realm name yahoo.com. The supply action produces jsmith@yahoo.com).

Require -- Requires the user to use the selected realm name (or none, if none is selected). If there is a realm name in the realm name field, the user must have the realm name indicated by the radio button. If the user does not, then he or she is not authenticated. If none is selected, then the user is required not to have a realm name.

- Example #1: User provided smith, Behavior is set to require, user has the realm name microsoft.com, but yahoo.com is entered in the realm name field. The user is not authenticated.
- Example #2: User provided smith, Behavior is set to require, user has the realm name microsoft.com and microsoft.com is entered in the realm name field. The user is authenticated.)

Force -- Replaces any realm name supplied by the user with the selected realm name, or strips off the realm name supplied by the user in the case of none.

- Example: User provided smith, Behavior is set to Force, user provides the realm name microsoft.com, but yahoo.com is entered in the realm name field. The user is authenticated as jsmith@yahoo.com)

Note: The available behaviors vary depending on the type of accounting or authorization realm selected. The following table shows the types of behaviors available for each type of accounting or authorization realm.

Table 4-5

Type of Accounting/Authorization Realm	**Behavior(s) Available**
ACL Radius Accounting	• Append
MAC RADIUS Accounting	• Append
MAC RADIUS Authentication	• Append

Configure the RADIUS Server

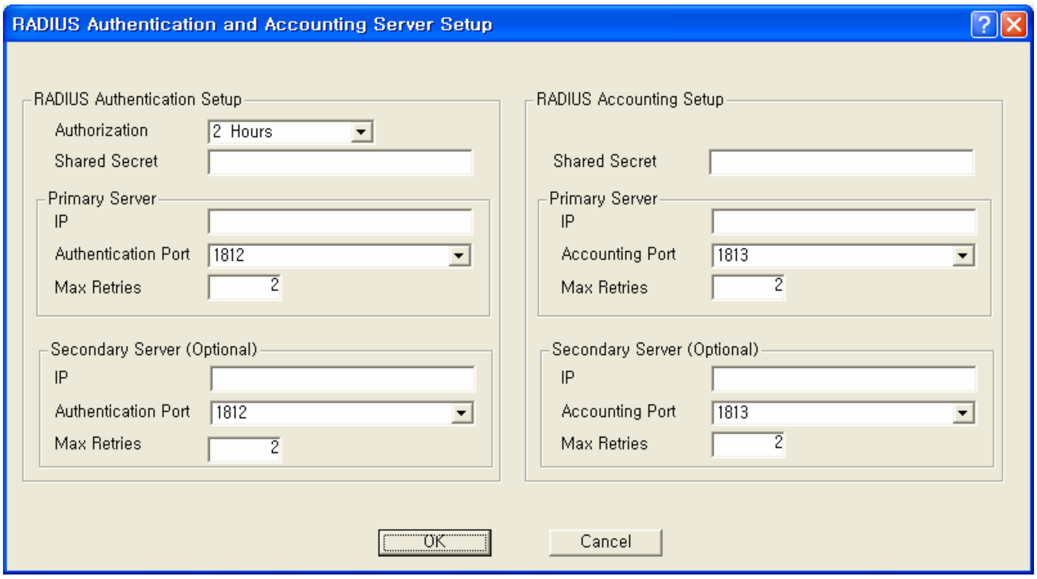
Once the AP has been configured for basic operation, you are ready to configure the device for HotSpot Mode and Firewall functionality.
This is a four-step process:

- Configure the RADIUS Server for Authentication (and, optionally, Accounting)
- Configure the APU for Basic RADIUS MAC Authentication.
- Configure the APU for Advanced RADIUS MAC Authentication.

Each step is explained in more detail below. Note that this section assumes that you have launched the AP Configurator and that you have completed all steps in Configure the Access Point for Basic Operation section.

From the Setup tab on the Configurator, click the RADIUS Server button. The RADIUS Authentication and Accounting Server Setup screen is displayed, as shown below.

Figure 4-59
RADIUS Setup Window



RADIUS Authentication and Accounting Server Setup

RADIUS Authentication Setup
Authorization: 2 Hours
Shared Secret:
Primary Server
IP:
Authentication Port: 1812
Max Retries: 2
Secondary Server (Optional)
IP:
Authentication Port: 1812
Max Retries: 2

RADIUS Accounting Setup
Shared Secret:
Primary Server
IP:
Accounting Port: 1813
Max Retries: 2
Secondary Server (Optional)
IP:
Accounting Port: 1813
Max Retries: 2

The RADIUS Server Setup screen is used to configure authentication and accounting parameters for terminal servers that speak the RADIUS protocol.
RADIUS is the de-facto standard protocol for authenticating users and for recording accounting information. Accounting keeps track of the number of bytes and packets sent by a client. It also keeps track of the amount of time a client has been authenticated. It is commonly used by

Terminal Servers or Network Access Servers (NASs) whenever a user logs on and off a dialup Internet service.

Note: This screen is only available if the MAC Authentication Access Control button on the General Setup screen has been selected.

There are two main sections in the RADIUS server setup dialog: RADIUS Authentication Setup and RADIUS Accounting Setup

In most cases you will want to set up both, although you do not have to set up Accounting. The two are almost identical except for the Authorization Lifetime, which appears only with Authentication.

To set up RADIUS authentication and accounting:

1. Enter values in the RADIUS Authentication and Accounting Server Setup screen to configure your RADIUS server. Each field on the screen is explained in more detail below.

Authorization Lifetime -- Authorization lifetime is the length of time the authorization is valid. Users will need to be-authenticated/re-authorized after this time expires. You should set this value to the maximum time you wish a user to be able to use your service without the need to be re-authenticated.

Shared Secret -- The client file for your RADIUS server contains the IP address and password for the base station you are setting up. You must add the IP address and password (shared secret) from this file in the RADIUS Server Setup screen.

Note: There are separate shared secrets (passwords) for authentication setup and accounting setup. The shared secret is an ASCII string that should be between 2 - 32 characters and should not start with a space.

Primary Server IP Address -- In the RADIUS dialog, enter the IP address for the RADIUS server (the host).

Primary Server Authentication Port -- In the RADIUS dialog, enter the authentication port (default = 1812) for the RADIUS server (the host).

Secondary Server IP Address -- If you are using a second RADIUS server for network robustness, enter the IP address of that RADIUS server.

Primary Server Accounting Port -- In the RADIUS dialog, enter the accounting port (default = 1812) for the RADIUS server (the host).

Secondary Server Authentication Port -- If you are using a second RADIUS server for network robustness, enter the authentication port (default = 1812) for that RADIUS server (the host).

Secondary Server Accounting Port -- If you are using a second RADIUS server for network robustness, enter the accounting port (default = 1812) for that RADIUS server (the host).

Procedure 3-6
Advanced and Optional **Configuration**

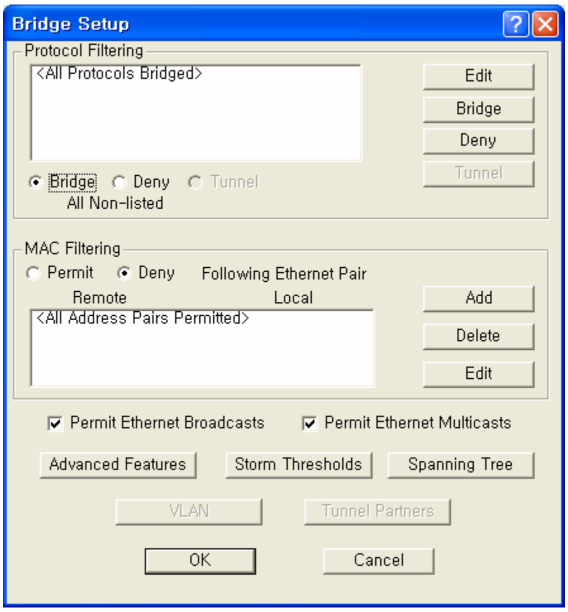
Once you have set up the basic network configuration, you may choose to set up one or more optional or advanced configuration components. This chapter describes how to configure the following optional and advanced components:

Set Up the Bridge

The Bridge Setup screen is used to set up the bridge. In addition, you may use the following screens to set up optional bridge components: The Bridge Setup screen is used to set up the parameters used for bridging. In most cases you will not need to modify the factory configured Bridge Setup. If you are working with an extensive network environment, however, and if you are an experienced network administrator, you may want to modify some of the parameters to fit specific network requirements.
The top half of the screen allows you to define different handling options based on different protocols. The bottom half of the screen allows you to define different handling options based on individual MAC addresses.

Note: This screen is only available when the Enable Bridging checkbox has been selected on the General Setup screen.

Figure 4-60
Bridge Setup window



Bridge Setup

Protocol Filtering
<All Protocols Bridged>
● Bridge ○ Deny ○ Tunnel
All Non-listed

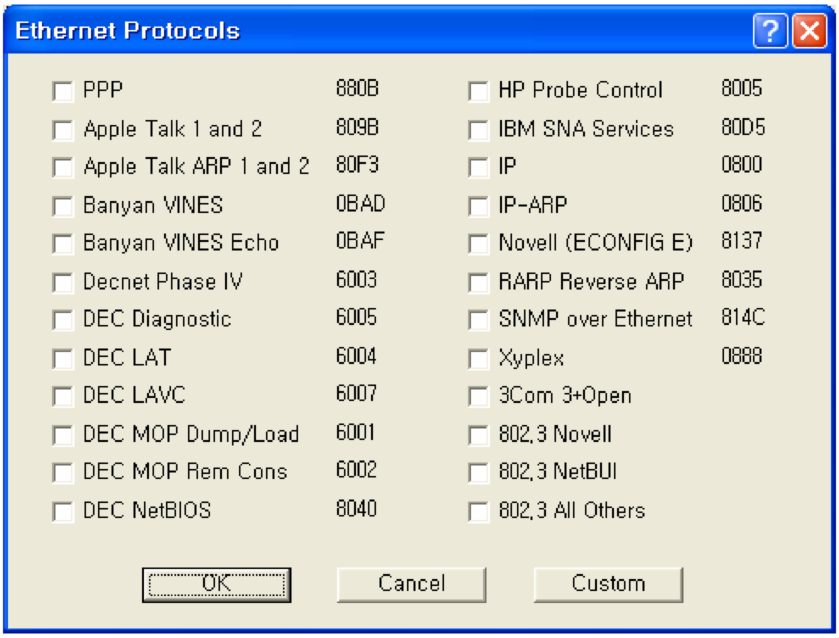
MAC Filtering
○ Permit ● Deny Following Ethernet Pair
Remote Local
<All Address Pairs Permitted>

☑ Permit Ethernet Broadcasts ☑ Permit Ethernet Multicasts

Protocol Filtering

The Protocol Filtering section of the Bridge Setup screen allows you to select a handling method (Bridge, Deny, or Tunnel) for the most common protocols.

Figure 4-61
Protocol Filtering Setup window



☐ PPP	880B	☐ HP Probe Control	8005
☐ Apple Talk 1 and 2	809B	☐ IBM SNA Services	80D5
☐ Apple Talk ARP 1 and 2	80F3	☐ IP	0800
☐ Banyan VINES	0BAD	☐ IP-ARP	0806
☐ Banyan VINES Echo	0BAF	☐ Novell (ECONFIG E)	8137
☐ Decnet Phase IV	6003	☐ RARP Reverse ARP	8035
☐ DEC Diagnostic	6005	☐ SNMP over Ethernet	814C
☐ DEC LAT	6004	☐ Xyplex	0888
☐ DEC LAVC	6007	☐ 3Com 3+Open	
☐ DEC MOP Dump/Load	6001	☐ 802.3 Novell	
☐ DEC MOP Rem Cons	6002	☐ 802.3 NetBUI	
☐ DEC NetBIOS	8040	☐ 802.3 All Others	

1. Select the protocols from the list that you wish to handle separately, or click the Custom button to add an unlisted protocol. Click the OK button when finished to re-display the Bridge Setup screen. Note that the protocols you have selected are listed in the Protocol Filtering window, and that all protocols are denied by default.
2. If you wish to Bridge or Tunnel any of the protocols in the list, select the protocol, then click either the Bridge or Tunnel buttons
3. At the bottom of the Protocol Filtering list, click the Bridge, Deny, or Tunnel button to define how all other non-listed protocols should be handled.

Note: You can add new protocols to the list at any time by clicking the Edit button and checking additional protocol check boxes.

Tunnel Button--The Tunnel button is used in conjunction with the protocols listed in the Protocol Filtering list. Select a protocol from the list and click the Tunnel button to indicate that the selected protocol should be tunneled.

Deny Button-- the Deny button is used in conjunction with the protocols listed in the Protocol Filtering list. Select a protocol from the list and click the Deny button to indicate that the selected protocol should be denied.

Bridge Button-- the Bridge button is used in conjunction with the protocols listed in the Protocol Filtering list. Select a protocol from the list and click the Bridge button to indicate that the selected protocol should be bridged.

Bridge MAC Address Filtering Overview

You can specify static MAC Address filters in Bridge Setup to optimize the performance and increase security on your wireless (and wired) network. You can permit or deny access to individual stations by specifying their particular MAC Addresses, or to multiple stations by using an X as a wildcard character. You can also permit or deny Ethernet multicast address all traffic that does not match one of the pairs explicitly listed in the Ethernet pair list will be permitted or denied based on your selection.

Table 4-6
Traffic Filtering

Selection	Traffic Matching Listed Pairs	Traffic Not Matching Listed Pairs
Permit Following Ethernet Pair	Permit	Deny
Deny Following Ethernet Pair	Deny	Permit

Stations to be filtered are identified by their MAC Address and whether they are on a remote or local interface. The Interface parameter indicates whether the station with the specified MAC Address is located on the wired or wireless interface of the base station. Use the Add, Delete, and Edit buttons to modify the entries of the list.

Permit Ethernet Broadcasts-- If you wish to deny broadcast traffic in your bridged network, deselect this option. Normally, however, you will select this option to permit Ethernet broadcasts.

Note: This option applies to all Ethernet interfaces, and not simply to Ethernet traffic.

Permit Ethernet Multicasts-- If you wish to deny multicast traffic in your bridged network, deselect this option. Normally, however, you will select this option to permit Ethernet multicasts.

Note: This option applies to all Ethernet interfaces, and not simply to Ethernet traffic.

Advanced Bridging Features

The Advanced Bridge features can be accessed by clicking the Advanced Features button on the Bridge Setup screen.

MAC Layer (Ethernet) Filters allow you to filter Ethernet traffic due to bad or unknown

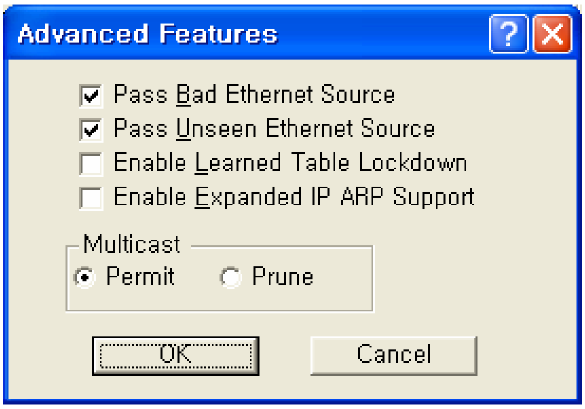
DHCP Filtering allows you to limit DHCP responses to a particular DHCP server.

IP/ARP Filtering allows you to prevent unnecessary IP/ARP packets from being sent over the wireless link.

Incoming Broadcast Filters allow you to prevent broadcast and multicast packets arriving from the remote interface(s) from being transmitted on the local interface(s).

Outgoing Broadcast Filters allow you to prevent broadcast and multicast packets sent from the local interface(s) from being transmitted out the remote interface(s).
Miscellaneous Statistics Gathering allows you to enable some miscellaneous advanced bridging features.

Figure 4-62
Advanced Bridging Setup window



Advanced Features

☑ Pass Bad Ethernet Source
☑ Pass Unseen Ethernet Source
□ Enable Learned Table Lockdown
□ Enable Expanded IP ARP Support

Multicast
● Permit ○ Prune

Permit Multicast Button-- Select this checkbox if you wish to permit multicast.

Prune Multicast Button-- Select this checkbox if you wish to prune multicast.

Enable Learned Table Lockdown--A standard Bridge/Router watches the source addresses of each packet it receives on any of its interfaces.
As new addresses are seen, entries are added in the “learned table” that contain the particular source address and the interface number that address was received on. If that source address is later seen on a different interface, the Bridge will immediately change the interface number in the learned entry table. This condition could happen in a correctly functioning network if someone moved the computer to a different part of the network.
This could also happen if someone was trying to capture network packets by spoofing the Bridge. Enabling learned table lockdown will prevent the interface number from being changed once the source address has been seen.

A standard Bridge will also time-out the learned table records every ten (10) minutes. If learned table lockdown is enabled, these records will not be timed-out. Once a record is learned, it will not be changed or deleted until either the Secure Data Mode station reboots or the learned table becomes completely filled and needs to be reset.

Note: A typical Secure Data Mode learned table can contain over 12,000 records.

Enable Expanded IP/ARP Support

Enabling this feature will cause the Secure Data Mode station to watch the IP/ARP packets that occur on the network. Normally, no action is taken in response to an IP/ARP packet that is not destined for a host that is being Proxy ARPed by the Secure Data Mode station. When this function is selected, the Secure Data Mode station will add the IP address to its IP/ARP table when it sees an ARP packet from another source. This feature is helpful on an ARP network because it will build a database of MAC layer address to IP address pairs.

Note: The IP/ARP table is never timed out in this mode.

Storm Threshold Setup

The Storm Thresholds screen is used to set threshold values for broadcast and multicast messages.

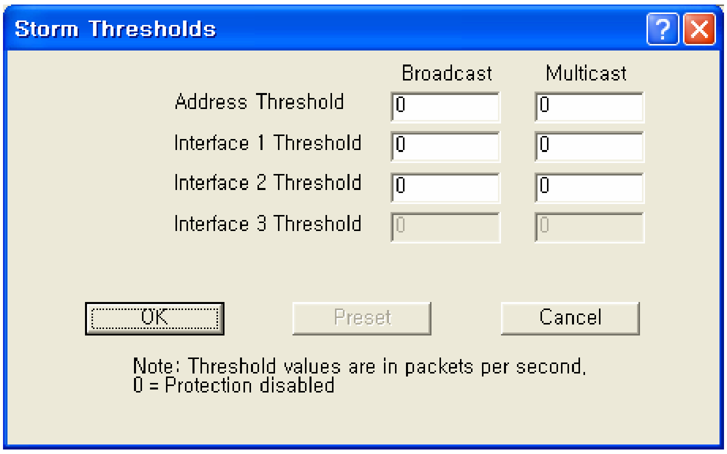
In most situations, you will not need to set the Storm Thresholds. However, if intensive multicast or broadcast messaging is typical of the network protocols used in your network environment, you may wish to control the maximum number of broadcast and multicast messages. If the maximum value of broadcast or multicasts per second is exceeded, the Secure Data Mode Station will ignore all subsequent messages issued by the particular network device, or ignore all messages of that type coming on that particular interface.

You can use the Storm Threshold screen to:

- Specify a maximum value as received from a single network device (identified by its MAC address).
- Specify an absolute maximum of messages per second per Interface.

You can specify a set of thresholds for each Interface of the Secure Data Mode Station access point, identifying separate values for the number of Broadcast messages/second and Multicast messages/second.

Figure 4-63
Broadcast Storm Setup window



Storm Thresholds

	Broadcast	Multicast
Address Threshold	0	0
Interface 1 Threshold	0	0
Interface 2 Threshold	0	0
Interface 3 Threshold	0	0

Note: Threshold values are in packets per second.
0 = Protection disabled

Broadcast Address Threshold

Enter the maximum number of broadcast messages per second that will be received from a single network device (identified by its MAC address).

Multicast Address Threshold-- Enter the maximum number of multicast messages per second that will be received from a single network device (identified by its MAC address).

Broadcast Interface 1 Threshold-- Enter the maximum number of broadcast messages per second that will be received on Interface 1 (typically Ethernet).

Multicast Interface 1 Threshold-- Enter the maximum number of multicast messages per second that will be received on Interface 1 (typically Ethernet).

Broadcast Interface 2 Threshold-- Enter the maximum number of broadcast messages per second that will be received on Interface 2 (typically 802.11).

Multicast Interface 2 Threshold-- Enter the maximum number of multicast messages per second that will be received on Interface 2 (typically 802.11).

Broadcast Interface 3 Threshold-- Enter the maximum number of broadcast messages per second that will be received on Interface 3 (typically 802.11a).

Multicast Interface 3 Threshold-- Enter the maximum number of multicast messages per second that will be received on Interface 3.

Preset Button-- Clicking the Preset button sets all broadcast and multicast rates to their default values. The default values are as follows:

Table 4-7
Default Threshold values

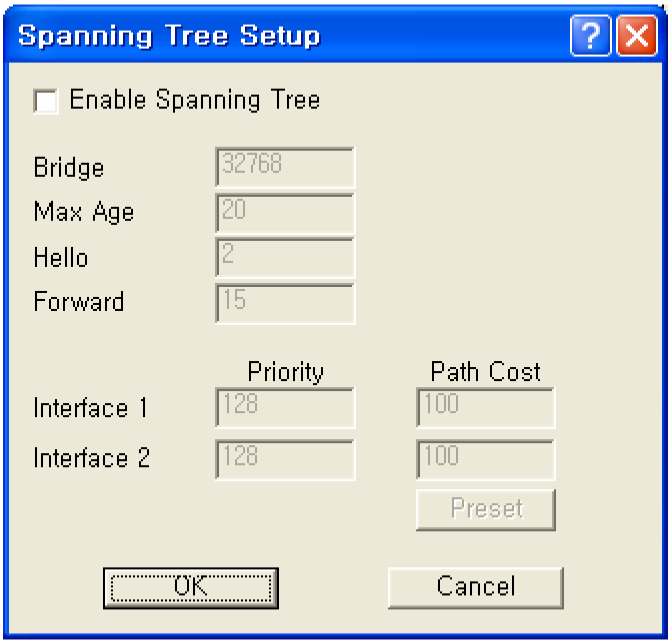
Item	Broadcast	Multicast
Address Threshold	30	30
Interface1 Threshold	60	60
Interface2 Threshold	60	60
Interface3 Threshold	60	60

Spanning Tree Setup

The Spanning Tree Setup screen allows you to configure your bridges so that they will dynamically discover a loop-free subset of the LAN topology (a tree), that provides the most efficient level of connectivity between every pair of physically connected Local Area Network segments. See Spanning Tree for more information about how the spanning tree algorithm works. The default settings for the Spanning Tree Algorithm will provide satisfactory performance for most Local Area Network (LAN) topologies.

Enable Spanning Tree -- Select this checkbox if you wish to enable Spanning Tree capabilities.

Figure 4-64
VLAN Spanning Tree Setup window



Spanning Tree Setup

□ Enable Spanning Tree

	Priority	Path Cost
Bridge	32768	
Max Age	20	
Hello	2	
Forward	15	
Interface 1	128	100
Interface 2	128	100

Bridge Priority -- The Bridge Priority parameter allows you to influence the choice of the Root Bridge and Designated Bridge as calculated by the Spanning Tree Algorithm.

Valid Values:	0 - 65000
Default:	32768

A low numerical value makes the bridge more likely to become the designated bridge or root bridge (typically 0).
The recommended value is 32768.

You may assign a duplicate priority value to multiple bridges, provided that it is a non-zero value. Bridges that have an identical Bridge Priority level are typically not intended to function as the root bridge.

Max Age -- The Max Age parameter identifies the maximum age of received Spanning Tree protocol information.

When the bridge receives protocol information that exceeds the Max Age value, the bridge will discard the information and start the Forward Delay timer to allow other bridges to forward updated topology information (for example, that another bridge has become the Root Bridge).

Note: Recommended Value (20 seconds)

A low Max Age value occasionally may cause the Spanning Tree to reconfigure unnecessarily, resulting in temporary loss of connectivity throughout the network.
A high Max Age value will cause the LAN to take longer than necessary to rebuild the Spanning Tree whenever a link or bridge unit breaks down or becomes available again.

Hello Time -- The Spanning Tree Hello Time parameter identifies the time interval between Configuration PBDU transmitted by a root bridge, or a bridge that is attempting to become the root bridge.

Note: Recommended Value (2 seconds)

Shortening the Hello Time will make the protocol more robust, especially when the probability of loss of configuration messages is high.

Lengthening the Hello Time will lower the overhead of the algorithm since the interval between the transmissions of configuration messages will be longer.

Forward -- The Forward Delay is a timer that prevents a bridge to forward data packets when:

- The bridge receives information that the active Spanning Tree topology must be updated (for example when a bridge breaks down or when somebody modified the Bridge Priority or Path Cost value of a particular bridge).
- The bridge registers that the protocol information exceeds the specified Max Age value.
- Changes in the Spanning Tree topology must be communicated to all bridges in the bridged network. The Forward Delay timer will compensate for the propagation delays that occur in passing the protocol information, allowing all bridges to close the old data paths, before the new data paths are activated.

Note: Recommended Value (15 seconds)

A lower value may result in temporary loops as the Spanning Tree Algorithm converges.

A higher value may result in longer partitions after the Spanning Tree reconfigures.

Port Priority-- Normally the Bridge Port priority in Spanning Tree topologies is imposed by the Root Bridge and the applicable values of the Path Cost to the Root Bridge.
When concurrent bridge ports of a single bridge unit are connected in a loop, this parameter enables you to influence which port should be included in the Spanning Tree.

Valid Values:	0 - 255
Default:	128

A lower value makes a port more likely to become selected in the Spanning Tree than the concurrent one that has a higher numerical value.
A higher value makes a port less likely to be selected in the Spanning Tree than a port with a lower numerical value.

Path Cost-- The Path Cost value is used to determine the preferred data paths between bridges throughout the network and the root bridge.
The Root Bridge transmits BPDU messages throughout the Local Area Network. When a bridge unit receives a BPDU message at one of its ports, it will add the value in the Path Cost field for that port to the value in the Root Path Cost Field of the BPDU message before forwarding the message again. This will help the other bridges to determine the Total Path Cost to the Root Bridge via this port.

Valid Values:	0 - 255
Default:	100

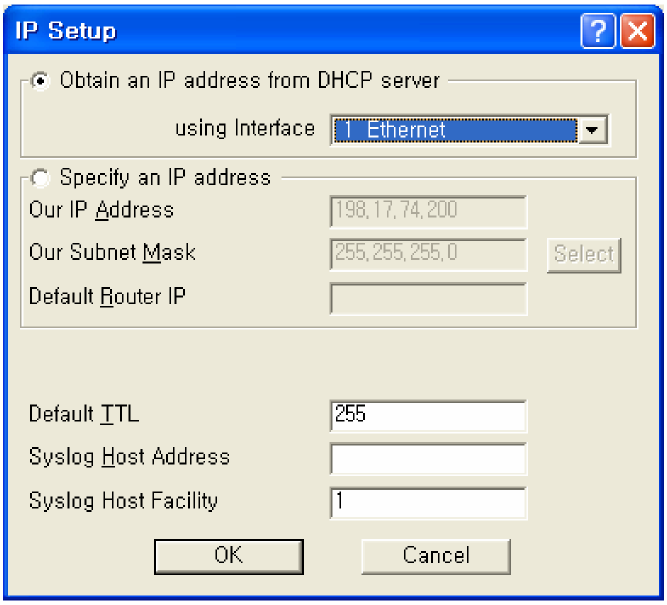
A lower Path Cost value would typically be used for ports to LAN segments closer to the Root Bridge.
A higher Path Cost value would typically be used for ports to LAN segments that are the "leafs" of the Spanning Tree.
For example, when using the Secure Data Mode Station as an access point for wireless stations to the Ethernet, a high Path Cost for the wireless interface will minimize unnecessary use of the bandwidth for the wireless medium (recommended value 255).
When using Secure Data Mode Stations in a wireless point-to-point link to interconnect two LAN segments, a low Path Cost for the wireless interface will prioritize this link as compared to other physical links, such as a leased line or low-bandwidth connections.

Set Up IP for APU and CSU

The IP Setup screen allows you to set the Secure Data Mode Station's IP Addressing information. The Secure Data Mode Station must have an IP address assigned to it if you wish to connect to it using the Configuration tool, which makes use of SNMP to connect to the Secure Data Mode Station.

Note: This screen is only available when the Enable IP Routing, Enable Outgoing Network Address Translation, and Enable Incoming Network Address Translation checkboxes been de-selected on the General Setup screen.

Figure 4-65
IP Setup window



IP Setup

● Obtain an IP address from DHCP server

using Interface: 1 Ethernet

○ Specify an IP address

Our IP Address: 198.17.74.200

Our Subnet Mask: 255.255.255.0

Default Router IP:

Default TTL: 255

Syslog Host Address:

Syslog Host Facility: 1

You can choose to set up the base station to obtain an IP address from DHCP server. If you select this option, you must also choose the interface on which you would like the base station to send the request. This option causes your base station to send a broadcast request for its IP address, subnet mask, and default router over the given interface at base station startup time. If you select the DHCP option, it is recommended (though not required) that you set up your DHCP server to always provide the same IP address to this Secure Data Mode Station system.

You can also manually specify an IP Address to set the IP Address for the base station yourself:

You can set the life expectancy for packets originating from this Secure Data Mode Station using the Default TTL (Time to Live) field.

You can use syslog messages to log information such as logins, service errors and general configuration information. Since there is no storage on a base station, a general purpose computer is needed to log these messages. To set the syslog host that will accept syslog messages, use the Syslog Host Address and Syslog Host Facility fields.

Obtain an IP Address from DHCP Server-- Select this radio button if you wish to obtain an IP address from the DHCP Server.

If you select this option, you must also choose the interface on which you would like the base station to send the request. This option causes your base station to send a broadcast request

For its IP address, subnet mask, and default router over the given interface at base station startup time. If you select the DHCP option, it is recommended (though not required) that you set up your DHCP server to always provide the same IP address to this Secure Data Mode Station system.

Using Interfaces-- Select the interface for which you wish to obtain an IP address. A base station has several network interfaces to which it may be connected. The network interfaces are numbered (1, 2, 3...), and the interface numbers may be found by selecting Interface Setup from the Setup Menu.

Specify an IP Address-- Select this radio button if you wish to enter an IP address manually.

Our IP Address-- This is the address of the Secure Data Mode Bridge/Router itself. If you wish to configure or monitor your Secure Data Mode Bridge/Router, or if your network supports IP and you wish to enable the Ping support and IP/SNMP support of the Secure Data Mode Bridge/Router, set this to a valid IP address. After setting this address to 0.0.0.0, enter the IP address of the base station.
Please note that unless you enable IP Routing on the IP Router Setup screen, the Bridge/Router is not an IP router. It has only one IP address, and that address applies to both the remote and local networks (i.e., both sides of the Bridge). Having two Ethernet interfaces with the same IP address is different than a standard IP host, but is appropriate for a Transparent Bridge. The Ethernet address of both interfaces is also the same.

Note: This field is only enabled when the Specify an IP Address radio button has been selected.

Our Subnet Mask-- Enter the subnet mask for the base station.

Note: This field is only enabled when the Specify an IP Address radio button has been selected.

Default Router IP-- Enter the IP address of the router.

Note: This field is only enabled when the Specify an IP Address radio button has been selected.

Select Button-- Clicking this button displays the IP Mask List screen, which allows you to select a particular IP mask.

IP Mask List-- The IP Mask List window displays a list of common IP subnet masks for a given size IP subnet.

Default TTL-- The Time To Live (TTL) counter avoids endless forwarding of message frames with incorrect addressing by defining a maximum number of hops a packet can take. Each time the frame is forwarded by a router, the TTL counter decreases by one.
When the TTL = 0, the frame is rejected.

Syslog Host Address-- Syslog messages can be used to log information such as logins, service errors and general configuration information. Since there is no storage on a base station, a general purpose computer is needed to log these messages.
The Syslog Host Address is the IP Address of the system which accepts "syslog" system logging packets from the base station.

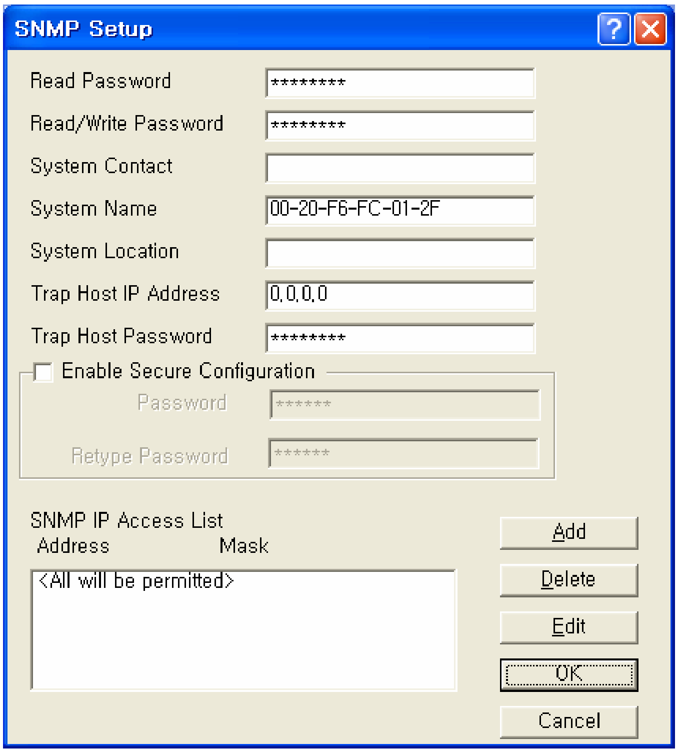
Syslog Host Facility

Syslog messages can be used to log information such as logins, service errors and general configuration information. Since there is no storage on a base station, a general purpose computer is needed to log these messages.
The Syslog Host Facility describes the part of the system generating the syslog message, and in UNIX-based systems usually uses one of the following keywords: auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, and local0 through local7.
The base station is capable of sending messages using the local0-local7 facilities. Enter the correct syslog facility number (0-7) that corresponds to the local facility type on your syslog host.

Set Up SNMP

The SNMP Setup screen allows you to manage a network environment that includes multiple base stations where you can use the Simple Network Management Protocol (SNMP).
SNMP setup allows you to create multiple authorization levels for network management that are password protected.

Figure 4-66
SNMP Setup window



SNMP Setup

Read Password: *********
Read/Write Password: *********
System Contact:
System Name: 00-20-F6-FC-01-2F
System Location:
Trap Host IP Address: 0.0.0.0
Trap Host Password: *********

☐ Enable Secure Configuration
Password: ******
Retype Password: ******

SNMP IP Access List
Address Mask
<All will be permitted>

Read Password-- This password enables you to create a network management level where a local LAN Administrator can view, but not modify, the SNMP parameters.

Read/Write Password-- This password enables you to create a network management level where only a Network Supervisor knowing the right Read/Write password will be able to view or modify the SNMP parameters.

Contact-- Optionally, enter the name or address of the Network Administrator.

System Name-- Optionally, enter the logical location of a base station (for example, the network segment to which the base station has been connected).

System Location-- The optional field to identify the physical location of a base station. For example, the building or room where the base station is located at

Trap Host IP Address-- The IP Address of the network management station that collects the SNMP Trap messages.

The Trap Host is the station in an SNMP managed network where SNMP trap messages are collected. Trap messages are sent to the trap host when certain events occur, such as rebooting.

Trap Host Password-- The Trap Host is the station in a SNMP managed network where SNMP trap messages are collected. Trap messages are sent to the trap host when certain events occur, such as rebooting.

Enter a password that corresponds to the password set at the Trap Host to filter unsolicited or unauthorized SNMP Trap messages at the Trap Host.

The Trap Host IP Password will be embedded in the SNMP Trap messages sent by this base station. If the Trap Host receives a message without or with an unknown password, the Trap message will be ignored.

SNMP IP Access List-- The SNMP IP Access List displays the IP addresses and subnet masks of those stations that you have designated as stations that will manage networks using SNMP.

In addition to the Read and Read/Write passwords, you can use the SNMP Access List to prevent unauthorized users from modifying the SNMP setup of your base stations.

The SNMP IP Access List enables you to authorize SNMP management to a restricted group of SNMP Management stations identified by:

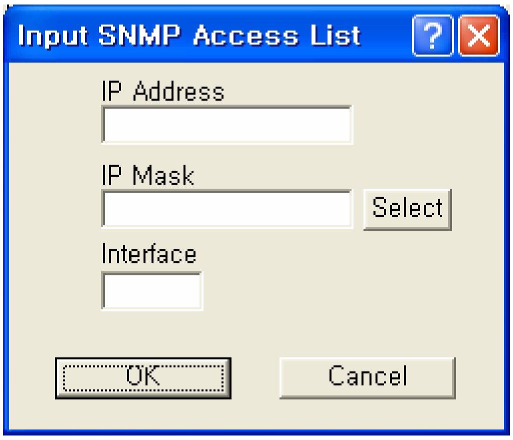
- The unique IP address of the Management Station(s)
- The interfaces via which the base station will be accessed.

Click the Add button to display the Input SNMP Access List to add new IP addresses to the list.

Input SNMP Access List Dialog - Overview

Clicking the Add button displays the SNMP Access List Dialog, which allows you to enter the IP addresses and subnet masks of those stations that you have designated as stations that will manage networks using SNMP.

Figure 4-67
Input SNMP Setup window



IP Address-- The unique IP address of the SNMP management station you wish to add or edit.

IP Mask-- Enter the Subnet mask, or clicks the Select button to display the IP Mask List and select a mask from the list.

Note: A subnet mask value of 255.255.255.255 will authorize only the station with the address specified in the IP address. A subnet mask value of 255.255.255.0 will authorize all stations that have an IP address within the range of that particular subnet (the IP address field will display the value xxx.xxx.xxx.0).

Warning: The subnet mask value 0.0.0.0 will authorize any station to view or modify SNMP IP setup of the base station via the interface identified in the Interface field.

Interface-- The number of the interfaces over which packets on this route is sent.

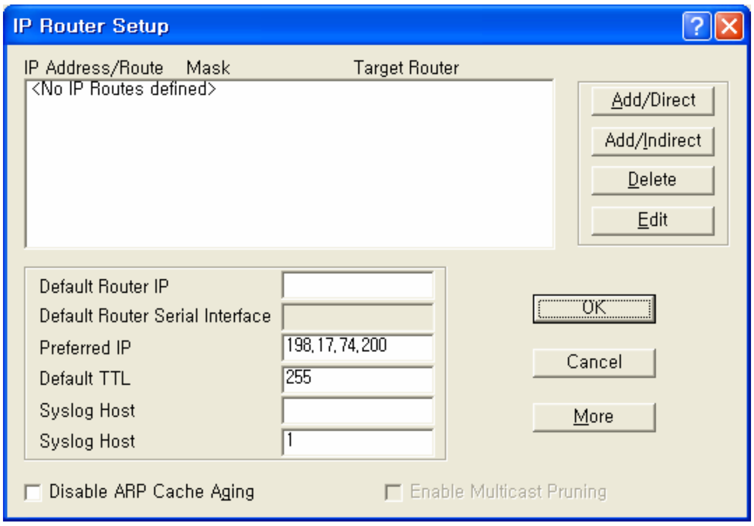
Select Button-- Clicking this button displays the IP Mask List screen, which allows you to select a particular IP mask.

Set Up IP Routing

The IP Router Setup screen is used to set up IP Routing. This enables the base station to send IP packets to the appropriate subnet or router. Once you have set up the basic IP Router configuration, you may also want to set up the following optional components:

Note: This option is only available if the Enable IP Routing checkbox on the General Setup screen has been selected.

Figure 4-68
IP Router Setup window



IP Router Setup

IP Address/Route Mask Target Router

<No IP Routes defined>

Default Router IP
Default Router Serial Interface
Preferred IP 198.17.74.200
Default TTL 255
Syslog Host
Syslog Host 1

☐ Disable ARP Cache Aging
☐ Enable Multicast Pruning

IP Route List

This pane displays the list of IP Routes that this Router has been configured to use. To add additional direct or indirect routes, click on the Add/Direct or Add/Indirect buttons.

Table 4-8
IP Route List

IP Route List	This pane displays the list of IP Routes that this Router has been configured to use. To add additional direct or indirect routes, click on the Add/Direct or Add/Indirect buttons.
Mask	The Subnet Mask of the IP Address, which shows which addresses should be routed using this route.
Target	For a Direct Route, the word Direct appears in this field. For an Indirect Route, this field shows the Default Router.
Interface/Cost	For direct routes, the interface to use when sending packets using this route. For indirect routes, the cost metric of using this route (used to determine the best route to use for a given packet).

Default Router IP Address-- Enter the IP Address of the router that the base station should use to communicate with networked devices outside its current subnet.

Default Router Serial Interface-- The Secure Data Mode station has several network interfaces to which it may be connected. An interface number is required for the Secure Data Mode station to know which interface to use to send packets addressed to a given destination. This field displays the serial interface that the router will use by default.

Preferred IP Address-- From time to time, the Secure Data Mode Bridge/Router will transmit unsolicited IP packets such as SNMP traps, Syslog, RIP, or IP/ARP packets. Most routers randomly use one of the IP addresses from one of the router interfaces as the source IP address for these packets. However, in the Preferred IP Address field, you can specify the source IP address that you prefer to use for these packets.

Default TTL-- The Time To Live (TTL) counter avoids endless forwarding of message frames with incorrect addressing by defining a maximum number of hops a packet can take. Each time the frame is forwarded by a router, the TTL counter decreases by one. When the TTL = 0, the frame is rejected.

Syslog Host Address-- Syslog messages can be used to log information such as logins, service errors and general configuration information. Since there is no storage on a base station, a general purpose computer is needed to log these messages.

The Syslog Host Address is the IP Address of the system that accepts "syslog" system logging packets from the base station.

Syslog Host Facility-- Syslog messages can be used to log information such as logins, service errors and general configuration information. Since there is no storage on a base station, a general purpose computer is needed to log these messages.
The Syslog Host Facility describes the part of the system generating the syslog message, and in UNIX-based systems usually uses one of the following keywords: auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, and local0 through local7.

The base station is capable of sending messages using the local0-local7 facilities. Enter the correct syslog facility number (0-7) that corresponds to the local facility type on your syslog host.

Disable ARP Cache Aging-- Select this checkbox to stop the Address Resolution Protocol (ARP) table from removing entries after a certain period of time. The IP ARP table relates each (wired or wireless) station's IP address to its physical MAC Address so the base station knows how to address Ethernet messages bound for a particular IP Address. If you disable (uncheck) ARP cache aging, the base station will not remove entries from this table, and it may fill up over time. The base station can hold up to 10,000 entries in the ARP table.

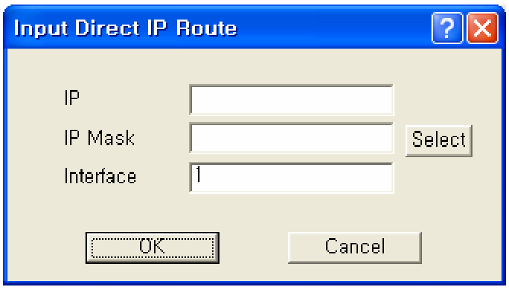
Enable Multicast Pruning-- Select this checkbox if you want to enable multicast pruning.

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients and homes.
Without multicast pruning, multicast traffic is treated in the same manner as broadcast traffic. That is, it is forwarded to all ports. However, with multicast pruning, you choose to permit only the packets that are a part of multicast group in your network. Multicast pruning generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

Add Direct IP Routes

Clicking the Add/Direct button displays the Add Direct IP Route screen, which allows you to add new direct IP routes.
When the Secure Data Mode station has two or more IP subnets directly attached to its different interfaces, it can route IP packets between those subnets using a direct route. This screen is used to specify the direct routes for each of the interfaces on the Secure Data Mode Bridge/Router. A direct route consists of an IP address, which specifies the basic IP address to route, a Subnet Mask which defines the basic class of IP addresses that will be routed, and an interface number which specifies where the IP subnet is attached. When IP packets addressed to a system arrives at the Secure Data Mode station, the Secure Data Mode station will send it directly to the target machine on the interface specified.

Figure 4-69
Direct IP Route Setup window



Input Direct IP Route

IP

IP Mask

Interface 1

IP Address-- The IP address specifies the basic IP address to route.

IP Mask-- The Subnet Mask which defines the basic class of IP addresses that will be routed. Clicking the Select button displays the IP Mask List, which the shows the IP Masks that can be used as public or private IP masks for IP routing. The list consists of all possible subnet masks, and represents the range of addresses that will be translated.

Interface-- An interface number specifies where the IP subnet is attached.

Add Indirect IP Routes

The Add Indirect IP Route screen is used to add indirect IP routes.

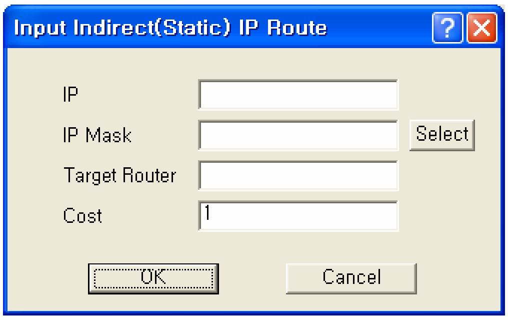
When the base station needs to send IP packets between IP subnets which are not directly connected to one of its interfaces (i.e., not on the same network segment), it must have an indirect route for sending those packets.

An indirect route consists of:

- An IP Address which specifies the basic IP address to route,
- A Subnet Mask which defines the class of IP addresses that will be routed,
- A Target Router that will relay the IP packet, and
- A Cost value, which specifies the number of "hops" required for the indirect route.

When an IP packet addressed to a system on the indirectly routed subnet arrives at the base station, the base station will route it over the interface specified to the Target Router to be further routed.

Figure 4-70
Indirect IP Route Setup window



Input Indirect(Static) IP Route

IP

IP Mask

Target Router

Cost 1

IP Address-- The IP Address which specifies the basic IP address to route.

IP Mask-- Enter the IP subnet mask for the IP address to be routed, or click the Select button and choose a subnet mask from the list. Clicking the Select button displays the IP Mask List, which the shows the IP Masks that can be used as public or private IP masks for IP routing. The list consists of all possible subnet masks, and represents the range of addresses that will be translated.

Target Router-- Enter the IP address of the router that you wish to use as the target router.

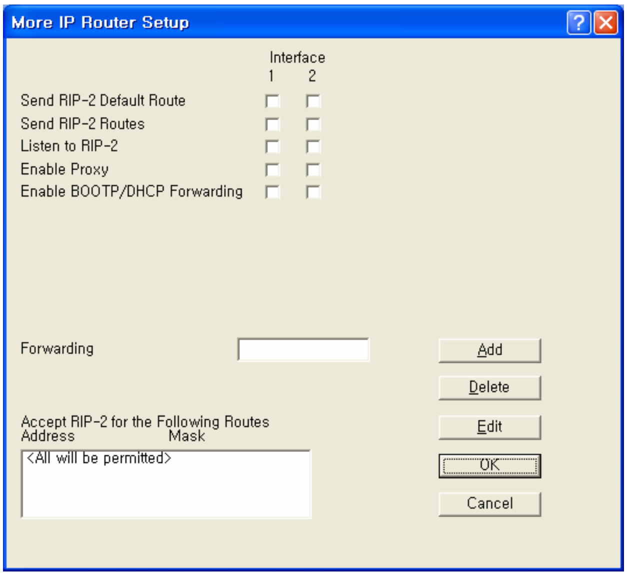
A target router is the IP address of the router that knows how to handle the IP packet that is being routed. When used in indirect routes, it could specify the router that is attached directly to the subnet of the packet's final destination, or a router that knows where to send it.

Cost-- The cost value reflects the number of "hops" required for the connection.   The default value of 1 indicates that only one "hop" is required. The lower the cost value, the more likely that route will be chosen.

Advanced IP Routing Setup

The More IP Router Setup screen is used to set up advanced IP router interfaces.

Figure 4-71
Advanced IP Routing Setup window



More IP Router Setup

	Interface 1	2
Send RIP-2 Default Route	□	□
Send RIP-2 Routes	□	□
Listen to RIP-2	□	□
Enable Proxy	□	□
Enable BOOTP/DHCP Forwarding	□	□

Forwarding

Accept RIP-2 for the Following Routes
Address Mask
<All will be permitted>

Send RIP-2 Default Route-- If the base station sends the Routing Information Protocol (RIP) default route (0.0.0.0) to other routers and hosts attached to a particular interface, select that interface's checkbox on the Send RIP Default Route line. By default, the base station will not send the Default Route on a particular interface unless this box is checked.

In the example shown in the screenshot, the base station will send RIP routes only on interfaces 1 and 2.

Send RIP-2 Routes -- If the base station should SEND Routing Information Protocol (RIP) Routes for routes of which it has knowledge to other routers on a particular interface, select that interface's checkbox on the Send RIP Routes line. By default, the base station will not send RIP Routes on a particular interface unless this box is checked.
For the given example, the base station will send RIP Routes only on interface 1.

Listen to RIP-2-- If the base station should ACCEPT Routing Information Protocol (RIP) routes from other routers on a particular interface, select that interface's checkbox on the Listen to RIP line. By default, the Secure Data Mode Station will not accept RIP Routes from other routers, so you must select the interfaces if you wish to listen to RIP. For the given example, the Secure Data Mode Station will listen to RIP Routes on Interfaces 1 and 2, but will not accept RIP routes sent to it on interface 3.

Enable Proxy ARP-- Enabling Proxy ARP for a particular interface tells the base station that when it receives an ARP request for a particular client connected by that interface, that the base station itself should respond to the ARP Request, fulfilling the request with information that is in its IP ARP Table.

For example, Proxy ARP is enabled on interface 2. The IP ARP Table contains (among others) the following entry:

Table 4-9
IP ARP Table

Interface	**Physical Address**	**IP Address**	**Media Type**
2	00:60:1d:04:4d:88	10.7.3.5	dynamic

Since Proxy ARP is enabled for interface 2, when the base station receives a broadcast ARP Request for 10.7.3.5, instead of passing the ARP on to 10.7.3.5, the base station will answer the request with information its own IP ARP table, that is: IP Address 10.7.3.5 -> MAC Address 00:60:1d:04:4d:88.

Proxy ARP is useful in many situations to reduce unnecessary network traffic, but is especially useful when you have clients in power-save mode, to prevent them from being 'woken up' whenever an ARP is done.

Enable BOOTP/DHCP Forwarding -- Select the interfaces for which you would like the base station to forward BOOTP and DHCP requests on to the BOOTP/DHCP server, which is specified in 'Forwarding Host'. Forwarding BOOTP and DHCP requests is necessary when the BOOTP/DHCP clients are not on the same IP subnet as the BOOTP/DHCP server.

If you are using BOOTP/DHCP, forwarding should most likely be DISABLED for the interface through which the BOOTP/DHCP server is located, and ENABLED for the other interfaces.

In the displayed screen, the BOOTP/DHCP Server is located via interface 1, so forwarding is enabled for interfaces 2 and 3, since clients on interfaces 2 and 3 have no other way of accessing the BOOTP/DHCP server.

Forwarding Host -- If you have enabled BOOTP/DHCP forwarding for one or more interfaces, enter the IP address of the BOOTP/DHCP server or relay agent to which you should forward BOOTP/DHCP requests.

In this example, the BOOTP/DHCP Forwarding host is 10.2.3.1.

Accept RIP-2 for the Following Routes-- In addition to the other Advanced IP Router features which allow you to accept RIP routes from particular interfaces, you can specify which RIP Routes you would like to accept. You are also able to specify the interfaces from which you would like to accept those particular RIP Routes.

The base station will accept RIP only for three particular routes. In the More IP Router Setup screen, it was specified that the base station should listen to RIP Routes on interfaces 1 and 2. This section further specifies that the base station should listen to the following RIP Routes ONLY:

- 10.17.42.0 (mask 255.255.255.0) only if it comes from interface 1
- 10.20.24.0 (mask 255.255.248.0) only if it comes from interface 2
- 10.220.23.0 (mask 255.255.255.0) on any interface

All other RIP routes will be ignored.

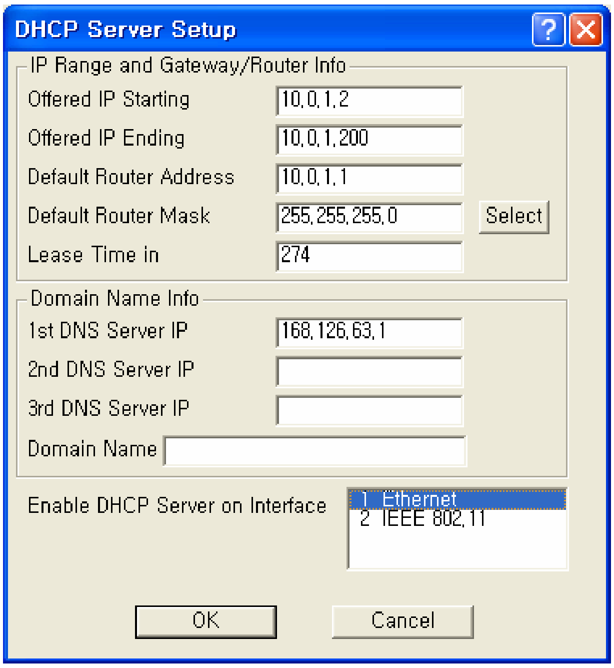
DHCP Server Setup

The DHCP Server Setup screen is used to set up the base station's Dynamic Host Configuration Protocol (DHCP) Server feature. The DHCP Server feature is a basic DHCP Server that can enable any and all wireless (or other) clients that connect to the base station to obtain their IP Address information from this Secure Data Mode.

Warning: If you have set up the base station to Obtain IP Address from DHCP Server on the IP Host Setup screen, do not enter anything in the Domain Name Info section of this screen. When the base station gets its own IP Address by DHCP, it will automatically determine the correct Domain Name information. You should, however, set up the IP Range and Gateway/Router Info section and select the correct interface.

Note: This screen is only available when the Enable DHCP Server checkbox has been selected on the General Setup screen.

Figure 4-72
DHCP Server Setup window



DHCP Server Setup

IP Range and Gateway/Router Info

Offered IP Starting: 10.0.1.2

Offered IP Ending: 10.0.1.200

Default Router Address: 10.0.1.1

Default Router Mask: 255.255.255.0

Lease Time in: 274

Domain Name Info

1st DNS Server IP: 168.126.63.1

2nd DNS Server IP:

3rd DNS Server IP:

Domain Name:

Enable DHCP Server on Interface: 1 Ethernet (selected), 2 IEEE 802.11

Offered IP Address-- Enter the beginning and ending IP addresses for the IP address range that the Secure Data Mode Station should offer to DHCP clients. When DHCP requests are received by the Secure Data Mode Station, it will offer the IP Starting Address to the first client, and increment the IP address offered to each consequent DHCP client until it reaches the IP Ending Address. IP Address leases must be renewed by the DHCP client within the given Lease Time, or the IP Address will be made available to another client.

Note: The Secure Data Mode Station does NOT store DHCP address assignments between restarts. If the Secure Data Mode Station is rebooted, it will ARP for each address in the provided address range, recording which client is using which IP address.

Note: Be careful not to include the default router's IP address in the Offered IP Address range.

Default Router Address-- Enter the default router IP address for the Secure Data Mode Station's DHCP clients.

Note: The default router IP address must be outside of the range defined by the Offered IP Starting Address and Offered IP Ending Address.

Default Router Mask-- Enter the subnet mask for the default router, or click the Select button to display the IP Mask List, and select a subnet mask from the list.

Lease Time in Minutes-- A DHCP lease is the amount of time that the DHCP server grants permission to the DHCP client to use a particular IP address. Enter the lease time (in minutes) for your DHCP server.

DNS Server IP Addresses-- Enter the IP address for the DNS server.

Warning: If you have set up the base station to Obtain IP Address from DHCP Server on the IP Host Setup screen, do not enter any DNS server IP addresses or a domain name. When the base station gets its own IP Address by DHCP, it will automatically determine the correct Domain Name information. You should, however, set up the IP Range (IP starting and ending addresses) and Gateway/Router Info section and select the correct interface.

Domain Name-- Enter the name of the domain.

Warning: If you have set up the base station to obtain IP Address from DHCP Server on the IP Host Setup screen, do not enter any DNS server IP addresses or a domain name. When the base station gets its own IP Address by DHCP, it will automatically determine the correct Domain Name information. You should, however, set up the IP Range (IP starting and ending addresses) and Gateway/Router Info section and select the correct interface.

Enable DHCP Server on Interface-- Select the interface on which you wish to enable the DHCP server.

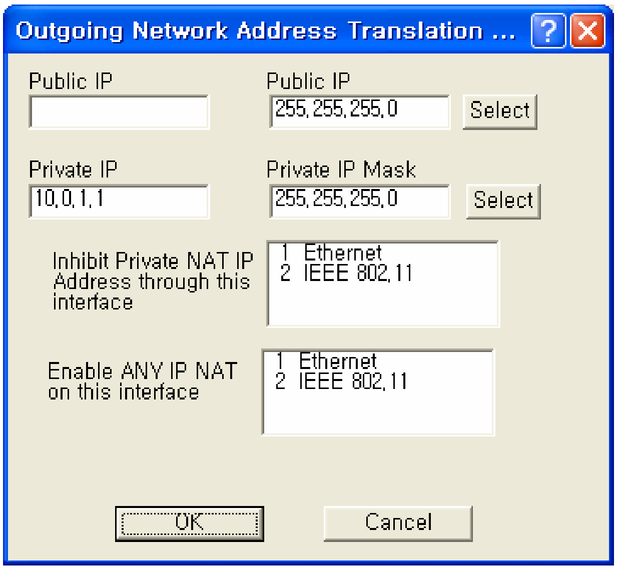
Set Up Outgoing Network Address Translation (NAT)

Outgoing Network Address Translation (NAT) allows multiple computers to share a single IP address to connect to an IP network, including the Internet. This allows homes, small businesses, and Internet Service Providers to have Internet service for all of their computers without having to pay for additional IP addresses. The NAT feature serves as a simple firewall for incoming connections, since only traffic initiated by an interior computer is permitted through the NAT.
In the screen shown below, when the client 10.0.1.1 wants to send data to the Internet, the access point will take the packet, replace the return address of 10.0.1.1 with 140.254.5.147, and then send the packet to the Internet. When a response comes from the Internet, the access point sends it to the correct client in the local address space.

Note: This screen is only available when the Enable Outgoing NAT checkbox has been selected on the General Setup screen.

Note: You do not need to turn on Outgoing NAT if you are using Incoming NAT, and vice versa. Incoming NAT only needs to be configured if servers in the local (private) address space need to connect with clients in the global (public) address space.

Figure 4-73
Outgoing NAT Setup window



Outgoing Network Address Translation ...

Public IP:

Public IP: 255.255.255.0

Private IP: 10.0.1.1

Private IP Mask: 255.255.255.0

Inhibit Private NAT IP Address through this interface:
1 Ethernet
2 IEEE 802.11

Enable ANY IP NAT on this interface:
1 Ethernet
2 IEEE 802.11

Public IP Address-- The IP address/mask seen by the external network.

Note: The IP address and subnet mask must be the same as the one in the IP Setup dialog under the Setup menu.

Public IP Mask-- The IP mask seen by the external network.

Note: The IP address and subnet mask must be the same as the one in the IP Setup dialog under the Setup menu.

Select IP Mask Button-- Clicking this button displays the IP Mask List, which the shows the IP Masks that can be used as public or private IP masks for outgoing NAT. The list consists of all possible subnet masks, and represents the range of addresses that will be translated.

Private IP Address-- The IP address that is seen by the local/internal network.

Note: The IP will be combined with the subnet mask, and the range of addresses that results will be translated. This range of IP set must match the addresses of the clients that connect to the base station.

Private IP Mask-- The IP mask that is seen by the local/internal network.

Note: The IP will be combined with the subnet mask, and the range of addresses that results will be translated. This range of IP set must match the addresses of the clients that connect to the base station.

Inhibit Private NAT IP Address through this interface

This option allows you to select one or more interfaces in which NAT will not be permitted. By default, no interfaces are selected. To select more than one interface, hold down the <Ctrl> key and click the names of the interfaces you wish to inhibit. Typically, you will inhibit the public interfaces because you will generally have users behind the private side (i.e., the private side is NATed to the public side).

Therefore, you must inhibit the interface used on the public side, whichever it may be. For example, in the screen shown below, the Ethernet 10.* network is NATed to the 140.* public wireless network. Therefore, NAT must be inhibited on the public interface, in this case the 802.11 interface. To do this, you would select 802.11 from the list, and click the OK button.

Set Up Incoming Network Address Translation (NAT)

Incoming Network Address Translations (NAT) is used to redirect requests to servers in the local address space based on the port of the request. If, for example, the client at local address 10.0.1.2 is serving web pages, and a request comes to the access point on that port for a web session, then the request will be forwarded to the web server on 10.0.1.2. The server will respond with the web page to the address of the original request.

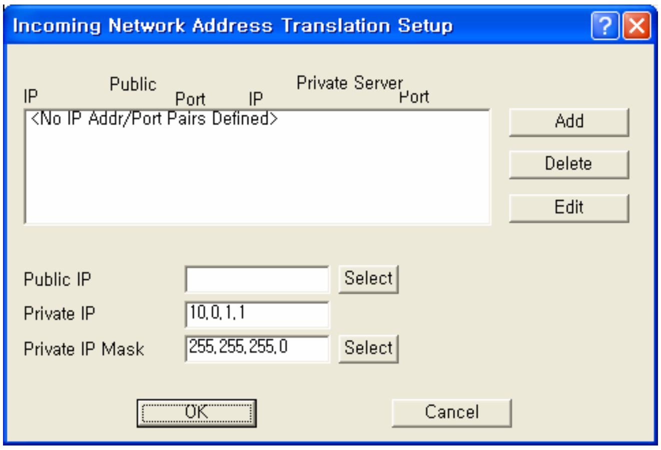
Note: This screen is only available when the Enable Incoming NAT checkbox has been selected on the General Setup screen.

Note: Incoming NAT only needs to be configured if servers in the local (private) address space need to connect with clients in the global (public) address space. You do not need to turn on Incoming NAT if you are using Outgoing NAT, and vice versa.

To set up incoming NAT:

1. From the Setup tab, select General Setup. The General Setup screen is displayed.
2. Make sure that the Enable IP Routing checkbox is unchecked.
3. Select the Enable Incoming Network Address Translation checkbox, and then click OK to close the General Setup screen.
4. Click the Incoming NAT button on the Setup tab. The Incoming Network Address Translation Setup screen is displayed, and any public and private IP address/port pairs that you have previously defined are displayed in the window.

Figure 4-74
Incoming NAT Setup window



Incoming Network Address Translation Setup

<No IP Addr/Port Pairs Defined>

Public IP:
Private IP: 10.0.1.1
Private IP Mask: 255.255.255.0

IP Addresses/Ports-- This window displays the public and private IP address/port pairs that you have previously defined.

Public IP Mask-- The public subnet mask for your local (internal) servers in the dialog. The public IP mask is paired with the Public IP address on the Input IP Address screen, as shown in the screens below.

Note: The public IP Mask must be the same subnet mask that was used in the setup of the external (or global) address of the base station.

Private IP Address-- The private IP address for your local (internal) servers in the dialog.

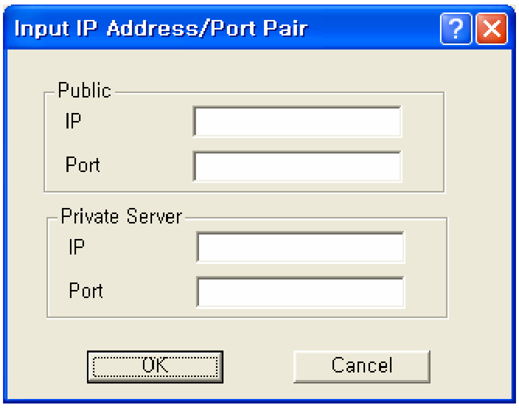
Note: The Private IP Address must be the same as the address and subnet mask that was selected for your internal network.

Private IP Mask-- The private subnet mask for your local (internal) servers in the dialog.

Note: The private IP Mask must be the same as the subnet mask that was selected for your internal network.

Add IP Address/Port Pairs-- Clicking the Add button displays the Add IP Address/Port Pair screen is used to add new pairs of incoming ports, and the IP address to which they should be directed.

Figure 4-75
Input IP address/Port (NAT) Setup window



Public IP Address-- The public IP address for the service you wish to use. On the incoming NAT, there can only be one public address. You can map ports to specific local servers, but you must use the same public IP address, as configured on the incoming NAT screen.

Note: The Public IP address is paired with the Public IP mask on the Incoming Network Address Setup screen, as shown in the screenshots below.

Public Port-- The public port for the service you wish to use. For a discussion of the ports on which well known services run, see http://www.tatanka.com/doc/technote/tn0081.htm.

Note: The public IP address must be the same for different local servers, but the port will be different (e.g. different ports for SMTP, FTP, web servers, etc.).

Private Server IP Address-- The local (private) IP address of the server to which the request should be forwarded.

Private Server Port-- The local (private) port on the server to which the request should be forwarded.

Set up IP/UDP/TCP Filters-- Select the Firewall option from the Setup Tab to set up the IP TCP/UDP firewall (filtering) features.

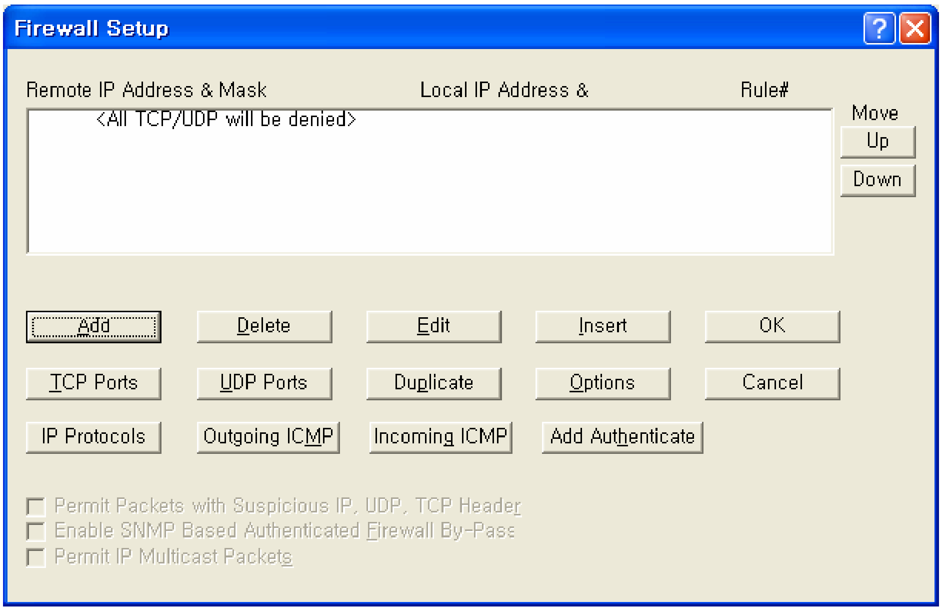
IP Firewalls are used to restrict access between (sub) networks to certain IP hosts, types of IP packets, or connections to certain ports. You can set up the firewall to completely block all external IP traffic, or restrict access to certain machines, ports, or packet types.

Note: You must select the Enable IP/TCP/UDP Security Filters checkbox on the General Setup screen in order to access this screen.

Remote IP Address and Mask-- This column of the TCP/UDP Filter List displays the IP Address and Subnet Mask of the (un-trusted) remote sub network or machine for which you have chosen to set up this IP UDP/TCP filter.

Local IP Address and Mask-- This column of the TCP/UDP Filter List displays the IP Address and Subnet Mask of the local sub network or machine that is being protected by this particular firewall filter.

Figure 4-76
Firewall Setup window



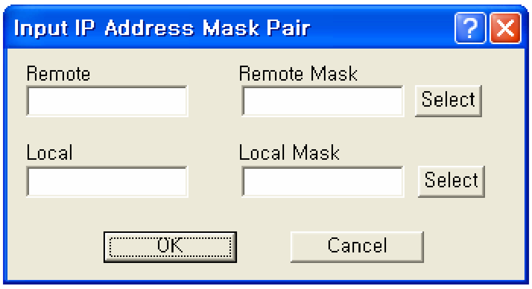
<All TCP/UDP will be denied>

☐ Permit Packets with Suspicious IP, UDP, TCP Header
☐ Enable SNMP Based Authenticated Firewall By-Pass
☐ Permit IP Multicast Packets

Add/Edit IP Address Mask Pair

The Add/Edit IP Address Mask Pair screen is used to enter both the IP Address and Subnet Mask of both the local network (or machine) you would like to protect and the remote network (or host) you would like to protect it from.
A particular filter is applied only to traffic between the specific local and remote networks (or hosts) shown in the list. If you wish to filter all traffic, set the Remote IP Address and Subnet Mask both to '0.0.0.0'.

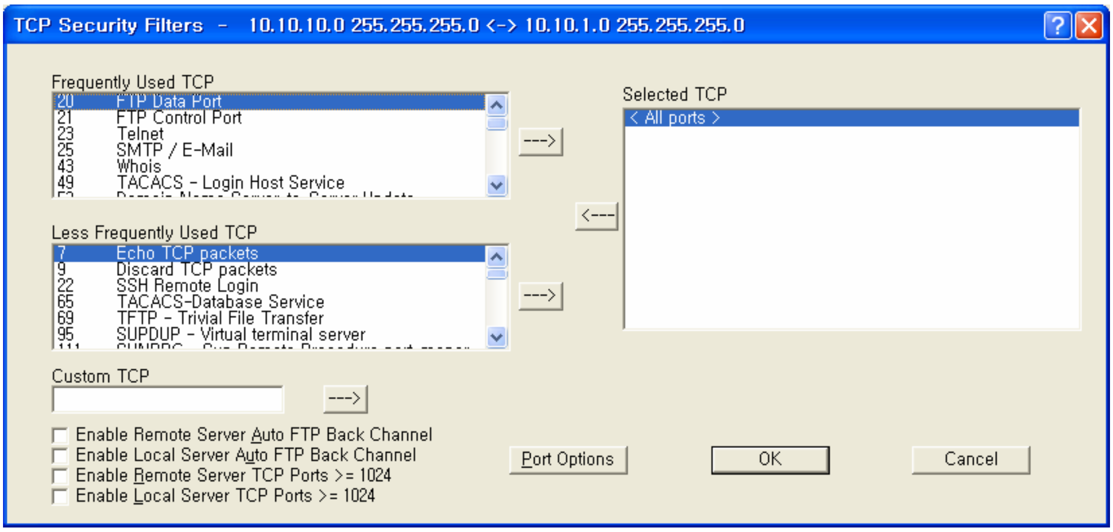
Figure 4-77
Input IP address (Firewall) Setup window



TCP Security Filters

To set the TCP ports to which a given filter will be applied, select the filter you want to modify in the TCP/UDP Filter List and click the TCP Ports button.

Figure 4-78
TCP Security Filter Setup window



TCP Security Filters - 10.10.10.0 255.255.255.0 <-> 10.10.1.0 255.255.255.0

Frequently Used TCP

20	FTP Data Port
21	FTP Control Port
23	Telnet
25	SMTP / E-Mail
43	Whois
49	TACACS - Login Host Service

Less Frequently Used TCP

7	Echo TCP packets
9	Discard TCP packets
22	SSH Remote Login
65	TACACS-Database Service
69	TFTP - Trivial File Transfer
95	SUPDUP - Virtual terminal server

Selected TCP

< All ports >

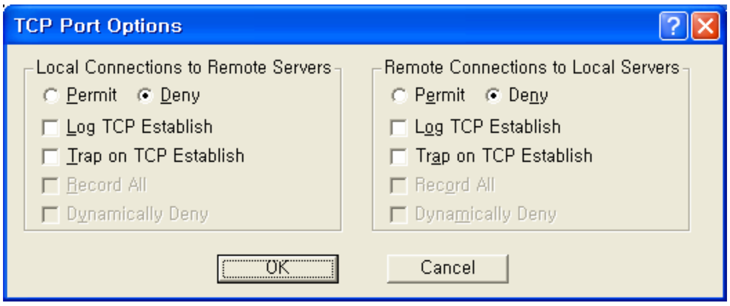
Custom TCP

□ Enable Remote Server Auto FTP Back Channel
□ Enable Local Server Auto FTP Back Channel
□ Enable Remote Server TCP Ports >= 1024
□ Enable Local Server TCP Ports >= 1024

TCP Port Options

Clicking the Port Options button on the TCP Security Filter screen displays the TCP Port Options screen. To set how the firewall filter is applied for a given port, select the port (or the line labeled 'All other ports') from the Selected TCP Ports list, and click on the 'Port Options' button. This will display the window below, which you can click on for more information. If you select the line 'All Other Ports' and then click the 'Port Options' button, you will see a screen similar to the one described in the UDP Port Options screen.

Figure 4-79
TCP Port Options Setup window



TCP Port Options

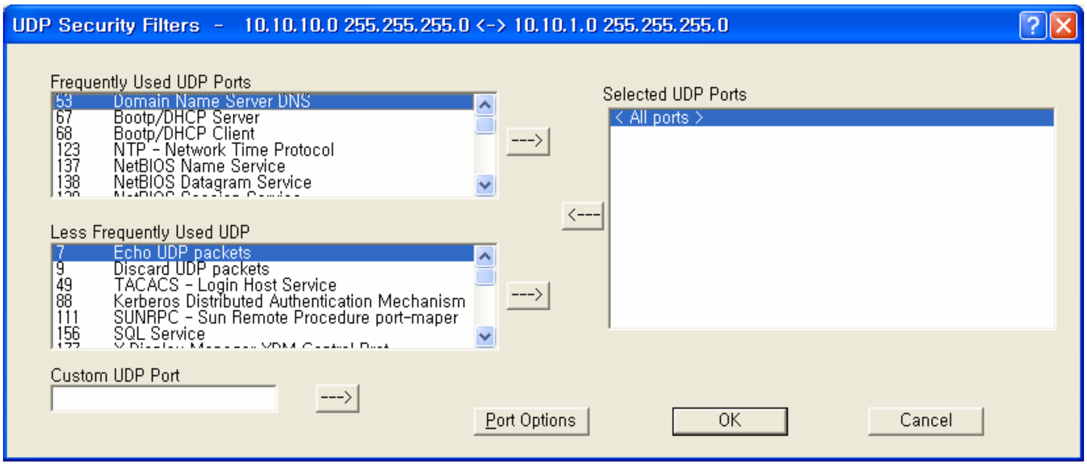
Local Connections to Remote Servers
○ Permit ● Deny
□ Log TCP Establish
□ Trap on TCP Establish
□ Record All
□ Dynamically Deny

Remote Connections to Local Servers
○ Permit ● Deny
□ Log TCP Establish
□ Trap on TCP Establish
□ Record All
□ Dynamically Deny

UDP Port Filters

To set the UDP ports to which a given filter will be applied, select the filter you want to modify in the TCP/UDP Filter List and click the 'UDP Ports' button.

Figure 4-80
UDP Port Options Setup window



UDP Security Filters - 10.10.10.0 255.255.255.0 <-> 10.10.1.0 255.255.255.0

Frequently Used UDP Ports

```
53    Domain Name Server DNS
67    Bootp/DHCP Server
68    Bootp/DHCP Client
123   NTP - Network Time Protocol
137   NetBIOS Name Service
138   NetBIOS Datagram Service
```

Less Frequently Used UDP

```
7     Echo UDP packets
9     Discard UDP packets
49    TACACS - Login Host Service
88    Kerberos Distributed Authentication Mechanism
111   SUNRPC - Sun Remote Procedure port-maper
156   SQL Service
```

Custom UDP Port

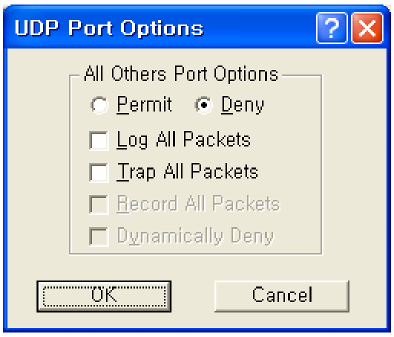
Selected UDP Ports

< All ports >

UDP Port Options

Clicking the Portion Options button on the UDP Security Filters screen displays the UDP Port Options screen. To set how the firewall filter is applied for a given port, select the port (or the line labeled 'All other ports') from the Selected UDP Ports list, and click on the 'Port Options' button. The window displayed below is for the 'All Other Ports' line, which sets the filter settings for all ports not explicitly listed in the Selected UDP Ports list. See TCP Port Options for an example using a specific port.

Figure 4-81
UDP Port Options Setup window



UDP Port Options

All Others Port Options

○ Permit ● Deny

□ Log All Packets

□ Trap All Packets

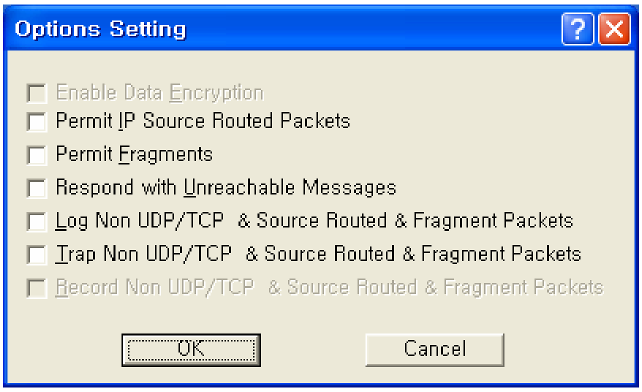
□ Record All Packets

□ Dynamically Deny

Firewall Setup Options

The Firewall Setup Options screen allows you to set handling options for a particular filter. Select the filter from the list on the Firewall Setup screen, and then click the Options button to display the following options. Alternately, you can simply double click the filter in the list to display the Firewall Setup Options screen.

Figure 4-82
Firewall Option Setup window



□ Enable Data Encryption
□ Permit IP Source Routed Packets
□ Permit Fragments
□ Respond with Unreachable Messages
□ Log Non UDP/TCP & Source Routed & Fragment Packets
□ Trap Non UDP/TCP & Source Routed & Fragment Packets
□ Record Non UDP/TCP & Source Routed & Fragment Packets

Enable Data Encryption-- Select this option if you wish to enable the data in packets sent between the IP hosts or subnets specified in this filter to be encrypted/decrypted by the Secure Data Mode Station. This option is not available if Data Encryption is not enabled on the General Setup screen.

Permit Non UDP/TCP Packets-- Select this option if you would like the Secure Data Mode Station to allow IP packets that are neither TCP nor UDP, such as ICMP. The firewall does not have specific filters for IP protocols other than TCP, UDP, and ICMP. If you want to deny other relatively rare protocols, do not select this checkbox.

Permit IP Source Routed Packets-- Select this option if you want the Secure Data Mode Station to allow Source-Routed IP packets to the local hosts protected by this filter. Source-Routed packets contain routing information inside the packet headers, instead of allowing network routers to decide the best route for the packet. They are primarily used in network troubleshooting, but may be used to 'fool' the firewall that the packets are coming from a trusted host. We strongly recommend that you do not permit source routed packets.

Permit Fragments-- Select this option if you would like the Secure Data Mode Station to permit fragmented IP packets to be passed through the firewall. IP packets may be incorrectly fragmented, creating security problems for hosts that may not properly handle incorrectly fragmented IP packets.

Respond with Unreachable Messages-- Select this option if you want the Secure Data Mode Station to respond to remote hosts attempting to connect to local machines with Destination Unreachable messages when the connection is denied by this security filter.

Log Non UDP/TCP & Source Routed & Fragment Packets-- Select this option if you want to log to the syslog for all packets that are not UDP/TCP, are source-routed, or are fragmented.

Trap Non UDP/TCP & Source Routed & Fragment Packets-- Select this option if you want the Secure Data Mode Station to SNMP Trap messages whenever a non-TCP or non-UDP, Source Routed, or Fragmented IP packet is received by the Secure Data Mode Station. SNMP Traps are sent to the SNMP Trap Host specified in SNMP Setup.

Record Non UDP/TCP & Source Routed & Fragment Packets-- Select this option if you want the Secure Data Mode Station to record all packets that are not UDP/TCP, are source-routed, or are fragmented.

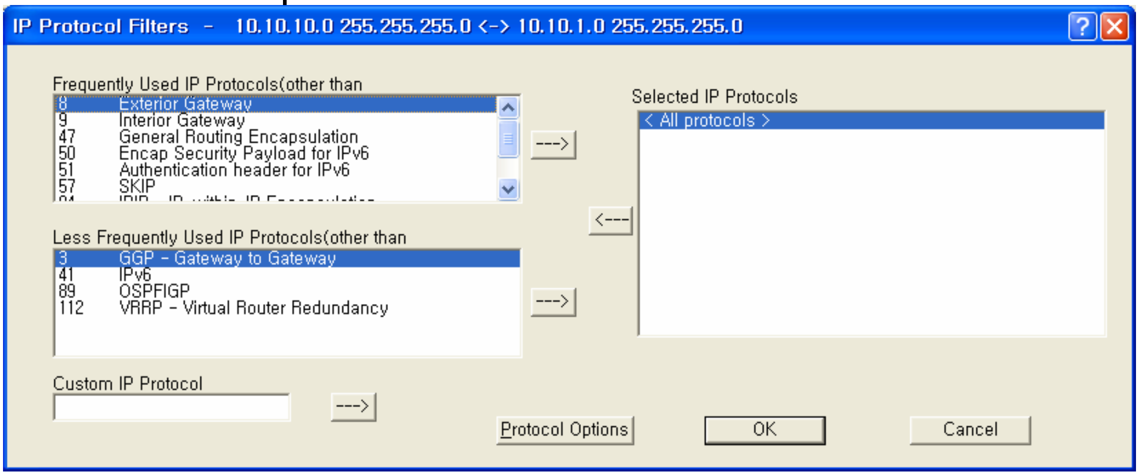
IP Protocol Filters

Clicking the IP Protocols button displays the IP Protocol Filters screen, which allows you to set the IP protocols to which a given filter will be applied. Select the filter you want to modify on the Firewall Setup screen, and click the IP Protocols button.

Less Frequently Used IP Protocols-- This list displays some of the less commonly used protocols that run over IP If you wish to filter one of these protocols, select it and click the [->] button. Then set the action to take using the Protocol Options button.

Selected IP Protocols-- Select one of the protocols added to the list and then click the Protocol Options button to set the action for this protocol. Select “All Protocols" or "All Other Protocols" to set a default action when a packet is received from a protocol for which no action has been defined.

Figure 4-83
IP Protocol Filter Setup window



IP Protocol Filters - 10.10.10.0 255.255.255.0 <-> 10.10.1.0 255.255.255.0

Frequently Used IP Protocols(other than

8	Exterior Gateway
9	Interior Gateway
47	General Routing Encapsulation
50	Encap Security Payload for IPv6
51	Authentication header for IPv6
57	SKIP
94	IPIP - IP within IP Encapsulation

Less Frequently Used IP Protocols(other than

3	GGP - Gateway to Gateway
41	IPv6
89	OSPFIGP
112	VRRP - Virtual Router Redundancy

Selected IP Protocols

< All protocols >

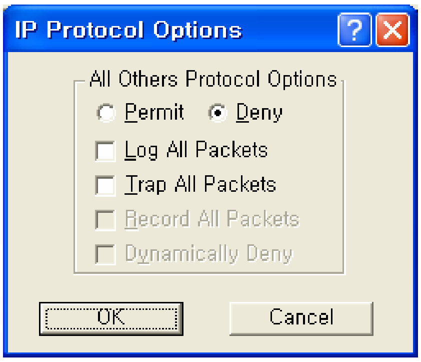
Custom IP Protocol

Custom IP Protocol-- If you wish to explicitly allow or deny access to a given IP protocol not listed in the two panels above, you can add that protocol to the list by simply typing it in the Custom IP Protocol field and clicking on the right arrow button [->] next to the text field. You do not need to add a protocol to the list unless you have specific requirements for that particular protocol.

IP Protocol Options

Clicking the Protocol Options button displays the IP Protocol Options screen, which allows you to define an action to take when data using that protocol is sent or received. When you select a protocol to filter, you will need to define an action to take when data using that protocol is sent or received. Initially, you will need to indicate whether you wish to permit or deny that protocol. In addition, you can optionally choose to log, trap, or record all packets, and to dynamically deny all other protocols.

Figure 4-84
IP Protocol Option Setup window



All Others Protocol Options

○ Permit ● Deny

□ Log All Packets

□ Trap All Packets

□ Record All Packets

□ Dynamically Deny

Permit All Other Protocols Button-- Select this button if you wish to permit all other protocols.

Deny All Other Protocols Button-- Select this button if you wish to deny all other protocols.

Log All Packets-- Select this checkbox if you wish to log all packets.

Trap All Packets-- Select this checkbox if you wish to trap all packets.

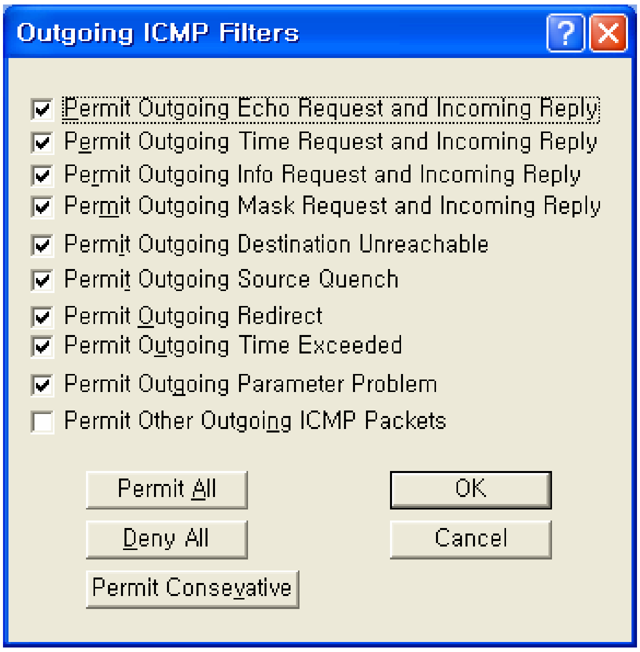
Record All Packets-- Select this checkbox if you wish to record all packets.

Dynamically Deny All Other Protocols-- Select this checkbox if you wish to dynamically deny all other protocols.

Outgoing ICMP Filters

Clicking on the Outgoing ICMP button on the Firewall Setup screen displays the Outgoing ICMP Filters screen, which allows you to permit or deny ICMP packets from going out from the local to remote interfaces. This allows you to deny diagnostic messages requested by internal (private) sources in this filter from being sent to external (un-trusted) machines.

Figure 4-85
Outgoing ICMP Filter Setup window



☑ Permit Outgoing Echo Request and Incoming Reply
☑ Permit Outgoing Time Request and Incoming Reply
☑ Permit Outgoing Info Request and Incoming Reply
☑ Permit Outgoing Mask Request and Incoming Reply
☑ Permit Outgoing Destination Unreachable
☑ Permit Outgoing Source Quench
☑ Permit Outgoing Redirect
☑ Permit Outgoing Time Exceeded
☑ Permit Outgoing Parameter Problem
□ Permit Other Outgoing ICMP Packets

Permit Outgoing Echo Request and Incoming Reply-- Permit Echo (ping) Requests sent from local stations to remote stations, and the remote stations' replies.

Permit Outgoing Time Request and Incoming Reply-- Permit local stations' Time Requests sent to remote stations and the replies from remote machines.

Permit Outgoing Info Request and Incoming Reply-- Permit local stations' Information Request packets sent to remote stations, and the remote stations' replies.

Permit Outgoing Mask Request and Incoming Reply-- Permit local stations' Mask Request packets sent to remote stations, and the remote stations' replies.

Permit Outgoing Destination Unreachable-- Permit Destination Unreachable packets generated on the (private) local network to be sent to external machines
Permit Outgoing Source Quench-- Permit Source Quench messages generated by gateways on the local network to be sent to remote machines sending packets to that gateway.

Permit Outgoing Redirect-- Permit Redirect messages generated by gateways on the local network to be sent to remote machines sending packets to that gateway.

Permit Outgoing Time Exceeded-- Permit Time Exceeded messages generated by gateways on the local network to be sent to remote machines sending packets to that gateway.

Permit Outgoing Parameter Problem-- Permit the local network to send Parameter Problem messages to the remote network when there was a problem with the header parameters of a packet.

Permit Other Outgoing ICMP Packets-- Permit other ICMP packets not listed above to be sent from the local network to the remote network.

Permit All Button-- Clicking this button selects all checkboxes on the Outgoing ICMP Filters screen.

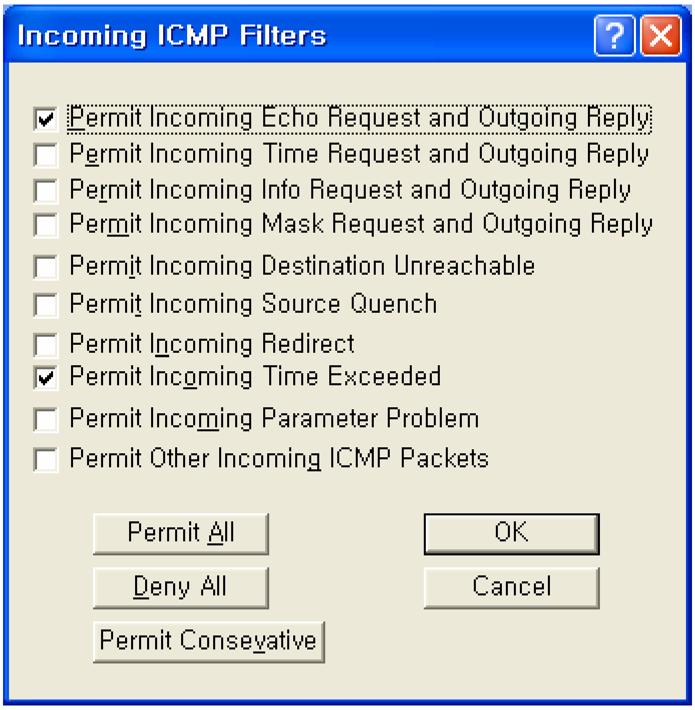
Deny All Button-- Clicking this button de-selects (un-checks) all checkboxes on the Outgoing ICMP Filters screen.

Permit Conservative Button-- Clicking this button automatically selects all checkboxes on the Outgoing ICMP Filters screen except for the Permit Other Outgoing ICMP Packets checkbox.

Incoming ICMP Filters

Clicking on the Incoming ICMP button on the Firewall Setup screen displays the Incoming ICMP Filter screen, which allows you to permit or deny ICMP packets from coming in from 'remote' to 'local' interfaces. This allows you to deny diagnostic messages requested from external (un-trusted) sources in this filter from being sent to your local (private) machines.

Figure 4-86
Incoming ICMP Filter Setup window



☑ Permit Incoming Echo Request and Outgoing Reply
□ Permit Incoming Time Request and Outgoing Reply
□ Permit Incoming Info Request and Outgoing Reply
□ Permit Incoming Mask Request and Outgoing Reply
□ Permit Incoming Destination Unreachable
□ Permit Incoming Source Quench
□ Permit Incoming Redirect
☑ Permit Incoming Time Exceeded
□ Permit Incoming Parameter Problem
□ Permit Other Incoming ICMP Packets

Permit Incoming Echo Request and Outgoing Reply-- Permit Echo Requests sent from remote (un-trusted) computers to be sent to machines on the local (private) network, and allow the local machine to reply to them.
Permit Incoming Time Request and Outgoing Reply-- Permit Timestamp Requests sent from remote (un-trusted) computers to be sent to machines on the local (private) network, and allow the local machine to reply to them.

Permit Incoming Info Request and Outgoing Reply-- Permit Information Request packets sent from remote (un-trusted) computers to be sent to machines on the local (private) network, and allow the local machine to reply to them.

Permit Incoming Mask Request and Outgoing Reply-- Permit Mask Request packets sent from remote (un-trusted) computers to be sent to machines on the local (private) network, and allow the local machine to reply to them.

Permit Incoming Destination Unreachable-- Permit Destination Unreachable messages generated by remote computers to be sent to machines on the local network.

Permit Incoming Source Quench-- Permit Source Quench packets generated by gateways on the remote network to be sent to gateways on the local network.

Permit Incoming Redirect-- Permit ICMP Redirect packets generated by gateways on the remote network to be sent to machines on the local network.

Permit Incoming Time Exceeded-- Permit Time Exceeded messages generated by machines on the remote network to be sent to machines on the local network.

Permit Incoming Parameter Problem-- Permit Parameter Problem messages generated by machines on the remote network to be sent to machines on the local network.

Permit Other Incoming ICMP Packets-- Permit other ICMP packets not listed above to be sent from the (un-trusted) remote network to the (private) local network.

Permit All Button-- Clicking this button automatically selects all checkboxes on the Incoming ICMP Filters screen.

Deny All Button-- Clicking this button automatically de-selects (un-checks) all checkboxes on the Incoming ICMP Filters screen.

Permit Conservative Button-- Clicking this button automatically selects the following checkboxes on the Incoming ICMP Filters screen:

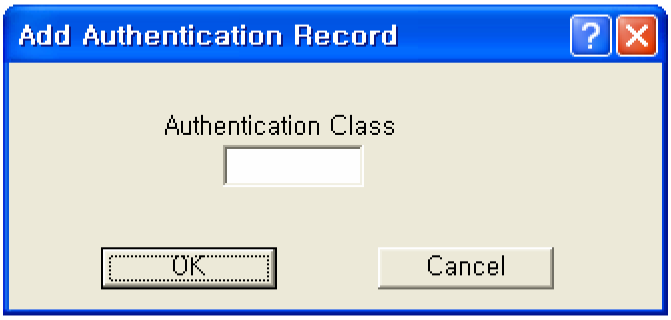
- Permit Incoming Echo Request and Outgoing Reply
- Permit Incoming Destination Unreachable

All other checkboxes are automatically de-selected (unchecked).

Add Authentication Record

The Add Authentication Record screen is used to add an SNMP-based username/password firewall authentication bypass class. The Authentication class works much like a UNIX user group does; you can specify what types of packets a person in this authentication class can pass through the firewall when logged in with the approved username and password.

Figure 4-87
SNMP Authentication Record Setup window



Authentication Class Number-- Enter a number for an SNMP-based username/password firewall authentication bypass class. The Authentication class works much like a UNIX user group does; you can specify what types of packets a person in this authentication class can pass through the firewall when logged in with the approved username and password.

Administration

The WLAN Cable Access Point 6220 CSU has the following management and operational features listed below:

Saving Configuration

Loading new Configuration

Uploading Software

Rebooting the remote station