
Foundry IronPoint™ 200 Access Point User Guide



4980 Great America Parkway
Santa Clara, CA 95054
Tel 408.207.1700
www.foundrynetworks.com

June 9, 2008

Copyright © 2008 Foundry Networks, Inc. All rights reserved.

No part of this work may be reproduced in any form or by any means – graphic, electronic or mechanical, including photocopying, recording, taping or storage in an information retrieval system – without prior written permission of the copyright owner.

The trademarks, logos and service marks ("Marks") displayed herein are the property of Foundry or other third parties. You are not permitted to use these Marks without the prior written consent of Foundry or such appropriate third party.

Foundry Networks, BigIron, FastIron, IronView, JetCore, NetIron, ServerIron, Turbolron, IronWare, Edgelron, IronPoint, the Iron family of marks and the Foundry Logo are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries.

All other trademarks mentioned in this document are the property of their respective owners.

Contents

Chapter 1.	
About This Guide	1-1
Audience	1-1
Nomenclature	1-1
Warranty Coverage	1-1
Related Publications	1-1
Updates to Manuals and Release Notes	1-2
How to Get Help or Report Errors	1-2
Web Access	1-2
E-mail Access	1-2
Telephone Access	1-2
Summary of Features	1-2
Technical Specifications	1-3
List of Supported Features	1-3
What's New in This Edition	1-6
IronPoint 200 Release 02.2.04	1-6
Chapter 2.	
Initial Configuration and Software Upgrades	2-1
Initially Configuring an Access Point	2-1
Using ADC to Configure An IronPoint Access Point	2-1
Configuring an Access Point when ADC is not Used	2-2
Required Connections	2-2
Logging In	2-3
Setting the IP Address	2-3
Setting Passwords	2-4
Enabling SNMP Management Access	2-4
Trap Receivers	2-5

System Defaults	2-6
Chapter 3.	
Using the Web Management Interface	3-1
Accessing the Web Browser Interface	3-1
Navigating the Web Browser Interface	3-2
Home Page	3-2
Configuration Options	3-3
Menus	3-3
Chapter 4.	
Using the Command Line Interface	4-1
Using the Command Line Interface	4-1
Accessing the CLI	4-1
Console Connection	4-1
Telnet Connection	4-1
Entering Commands	4-2
Keywords and Arguments	4-2
Minimum Abbreviation	4-3
Command Completion	4-3
Getting Help on Commands	4-3
Partial Keyword Lookup	4-4
Negating the Effect of Commands	4-4
Using Command History	4-4
Understanding Command Modes	4-4
Exec Commands	4-5
Configuration Commands	4-5
Command Line Processing	4-6
Chapter 5.	
Complete List of CLI Commands	5-1
Command Groups	5-1
General System Commands	5-2
IP Configuration Commands	5-3
Management Access Commands	5-3
System Information Commands	5-3
System Identification Commands	5-4
System Logging Commands	5-4
System Clock Commands	5-4
SNMP Commands	5-4
Flash/File Commands	5-5
RADIUS Client	5-6
MAC Address Authentication	5-6

802.1x Authentication	5-7
Intrusion Detection and Lockout	5-7
Bridging and Traffic Filtering Commands	5-8
Ethernet Interface Commands	5-8
Management Tunnel (PPPoE) Commands	5-8
Radio Interface Commands	5-9
Wireless Security Commands	5-11
VLAN Commands	5-11
QoS Commands	5-11
TACACS+ and AAA Commands	5-12
SSID Prioritization	5-13
Chapter 6.	
General System and CLI Settings	6-1
Using the General System Commands	6-1
Using the CLI	6-1
Enabling and Disabling ADC	6-9
Using the CLI	6-9
Using the Web Management Interface	6-10
Support for IronPoint Wireless Location Manager	6-10
Using the CLI	6-10
Using the Web Management Interface	6-11
Rate Limiting for Wireless Broadcast or Multicast Frames	6-11
Using the CLI	6-12
Chapter 7.	
Flash and File Commands	7-1
Using the CLI	7-1
Using the Web Management Interface	7-5
Viewing and Editing XML Configuration files	7-8
Chapter 8.	
Configuring IP Settings	8-1
Using the CLI	8-1
Using the Web Management Interface	8-4
Chapter 9.	
Management Access Settings	9-1
Configuring User Names and Passwords	9-1
Using the CLI	9-1
Using the Web Management Interface	9-2
Telnet and SSH Settings	9-4
Using the CLI	9-4
Using the Web Management Interface	9-5

Configuring the Web Server	9-6
Using the CLI	9-6
Using the Web Management Interface	9-8
Using ACLs to Control Management Access	9-10
Configuring Banners	9-15
Using the CLI	9-15
Chapter 10.	
SNMP Configuration	10-1
Enabling SNMP and Setting v1 and v2c Parameters	10-1
Using the CLI	10-1
Using the Web Management Interface	10-6
Configuring SNMPv3 Users	10-9
Using the CLI	10-9
Configuring SNMPv3 Trap Filters	10-12
Using the CLI	10-12
Using the Web Management Interface	10-14
Configuring SNMPv3 Notification Targets	10-15
Using the CLI	10-15
Using the Web Management Interface	10-17
Chapter 11.	
System Identification	11-1
Using the CLI	11-1
Using the Web Management Interface	11-1
Chapter 12.	
System Logging	12-1
Enabling System Logging	12-1
Using the CLI	12-1
Using the Web Management Interface	12-5
Displaying Log Messages	12-5
Using the CLI	12-6
Using the Web Management Interface	12-6
Chapter 13.	
System Clock	13-1
Using the CLI	13-1
Using the Web Management Interface	13-4
Chapter 14.	
Management Tunnel Settings	14-1
Using the CLI	14-1
Using the Web Management Interface	14-7

Chapter 15.	
RADIUS Client Settings	15-1
Using the CLI	15-1
Using the Web Management Interface	15-6
Chapter 16.	
TACACS+ AAA	16-1
TACACS+ Authentication	16-1
TACACS+ Authorization	16-1
TACACS+ Accounting	16-2
Configuration Note	16-2
Defining TACACS+ Servers	16-2
Configuring TACACS+ Authentication	16-7
Configuring TACACS+ Authorization	16-8
Configuring TACACS+ Accounting	16-9
Chapter 17.	
Intrusion Detection and Lockout	17-1
Using the CLI	17-2
Chapter 18.	
Bridging and Traffic Filter Settings	18-1
Using the CLI	18-1
Using the Web Management Interface	18-6
Chapter 19.	
Wireless Client Authentication	19-1
Configuring MAC Address Authentication	19-2
Using the CLI	19-2
Using the Web Management Interface	19-5
Configuring 802.1x Client Authentication	19-7
Using the CLI	19-7
Using the Web Management Interface	19-9
Configuring 802.1x Supplicant Authentication	19-11
Using the CLI	19-11
Using the Web Management Interface	19-12
Chapter 20.	
Ethernet Interface Configuration	20-1
Using the CLI	20-1
Using the Web Management Interface	20-4
Chapter 21.	
Radio Interface Configuration	21-1
Configuring Radio Settings (802.11a)	21-1
Using the CLI	21-2

Using the Web Management Interface	21-18
Configuring Radio Settings (802.11g)	21-23
Using the CLI	21-23
Using the Web Management Interface	21-26
Configuring Access Point Load Balancing	21-31
Using the CLI	21-31
Using the Web Management Interface	21-35
Chapter 22.	
Wireless Security Configuration	22-1
Configuring Static WEP	22-6
Using the CLI	22-6
Using the Web Management Interface	22-10
Configuring WPA or WPA2 Pre-Shared Key	22-13
Using the CLI	22-13
Using the Web Management Interface	22-15
Configuring WPA and WPA2 over 802.1x	22-16
Using the CLI	22-16
Using the Web Management Interface	22-18
Web Management Interface Advanced Security	22-20
Changing Encryption Types	22-23
Chapter 23.	
VLAN Support	23-1
Enabling VLAN Support	23-2
Using the CLI	23-2
Using the Web Management Interface	23-3
Setting Default VLAN IDs	23-4
Using the CLI	23-4
Using the Web Management Interface	23-5
Chapter 24.	
System Information	24-1
Displaying the Access Point Status	24-1
Using the CLI	24-1
Using the Web Management Interface	24-4
Displaying Wireless Client Information	24-5
Using the CLI	24-5
Using the Web Management Interface	24-9
Displaying the AP Inventory Report	24-10
Using the CLI	24-10
Chapter 25.	
QoS Support	25-1

Enabling QoS Support	25-2
Using the CLI	25-2
Using the Web Management Interface	25-6
Chapter 26.	
SSID Prioritization	26-1
How SSID Prioritization Works	26-1
Configuring SSID Prioritization for the IronPoint Access Point	26-2
Using the CLI	26-2
Using the Web Management Interface	26-5
Chapter 27.	
Miscellaneous Reports	27-1
AP Status	27-1
Neighbor APs	27-3
Chapter 27.	
RF Monitoring	27-1
Converting an Access Point to a Sensor	27-1
Viewing Sensor Data	27-2
Converting a Sensor Back to an Access Point	27-2
Appendix A.	
Troubleshooting	A-1
Appendix B.	
Syslog Messages	B-1
General System	B-1
802.1x	B-2
MAC Authentication	B-3
Radio Interface	B-3
Radio Security	B-5
Wireless Client	B-8
Access Point Management	B-10
SNMP	B-10
Syslog	B-11
DHCP	B-11
Appendix C.	
Country Channel Allocations	C-1
Channel Numbers	C-1
Channel Settings by Country	C-2
Glossary	
Index	

Chapter 1

About This Guide

The IronPoint™ 200 Access Point are devices that allow wireless clients to connect to your enterprise network. They are full-featured access points that can be managed as a single device. IronPoint 200 Access Point can be managed by IronView Network Manager, a network management tool that manages several Foundry devices on a network.

This guide presents the procedures for configuring and managing these access points using their command line interface and Web interface.

Audience

This guide is for system administrators with a working knowledge of network management for wired and wireless devices.

You should be familiar with switching and networking concepts.

Nomenclature

This guide uses the following typographical conventions to show information:

`Monospace font` – Enter text exactly as it appears in this guide.

bold font – Identifies a command line interface command when it is used in a sentence or paragraph.

<italics> – Words in *italics* inside a parenthesis indicate a value to be entered.

Note: emphasizes an important fact or calls your attention to a dependency.

Warranty Coverage

Contact Foundry Networks using any of the methods listed above for information about the standard and extended warranties.

Related Publications

Refer to the following installation guides for instructions on how to install the access point:

- ◆ *Foundry IronPoint 200 Installation Guide* – Contains details on how to install the IronPoint 200 Access Point, wireless network planning guidelines, troubleshooting guidelines, cabling, and

general operating specifications

- ◆ Foundry *IronPoint 250 Installation Guide* – Contains details on how to install the IronPoint 250 Access Point, wireless network planning guidelines, troubleshooting guidelines, cabling, and general operating specifications
- ◆ Foundry *IronPoint 200 Access Point User Guide* – Contains procedures for configuring the IronPoint 200 Access Point using the command line interface and the Web interface.
- ◆ Foundry *IronPoint 250 Access Point User Guide* – Contains procedures for configuring the IronPoint 250 Access Point using the command line interface and the Web interface.
- ◆ Foundry *IronPoint Wireless LAN Configuration Guide* – Contains information on how to configure the IronPoint FastIron Edge switch for wireless features.
- ◆ Foundry *IronView Network Manager User Guide* – Contains information on how to use IronView Network Manager to configure and manage the IronPoint access point.
- ◆ Release notes for the software release.

Updates to Manuals and Release Notes

Manuals and release notes for this product may be updated between releases. For the latest edition of manuals and release notes, check the Foundry Knowledge Portal at kp.foundrynet.com.

How to Get Help or Report Errors

Foundry Networks is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Foundry Networks using one of the following options.

Web Access

Go to kp.foundrynet.com and log in to the Knowledge Portal (KP) to obtain more information about a product, or to report documentation errors. To report errors, click on Cases > Create a New Ticket.

E-mail Access

Send an e-mail to: support@foundrynet.com

Telephone Access

1.877.TURBOCALL (887.2622) United States

1.408.207.1600 Outside the United States

Summary of Features

This manual contains the configuration and management commands for the IronPoint Access Point software release 02.02.02, which can be installed only on IronPoint 200 access points. software release 03.02.00.

Technical Specifications

The following table summarizes the technical specifications for the access point:

Properties	IronPoint 200
10/100 Base-T Ports	1
Wireless interfaces	802.11a 802.11b/g
Maximum clients	64 per VAP interface
Flash memory	8 MB
DRAM	32 MB
Physical Dimensions (HxWxD)	8.60 x 5.40 x 1.29 in (21.83 x 13.73 x 3.27 cm)
Weight	1.76 lbs (0.8 kg)
Power Consumption (Watt)	13.2 W maximum

List of Supported Features

The following table summarizes the features available in the access point. Refer to the appropriate sections in this manual for any feature limitations.

Category	Feature
IP Address Management	Automatic Discovery and Configuration (ADC)
	Static
	DHCP client
	DNS resolution
VLAN	802.1Q tagging
	64 VLAN IDs
	Management VLAN ID
	Default VLAN ID per radio
	802.1X dynamic VLAN assignments
System Software	Dual firmware image
	TFTP upgrade
	FTP upgrade
	HTTP upgrade
SNMP	SNMP v1 and v2c
	SNMPv3 users
	SNMPv3 groups
	SNMPv3 trap targets
	SNMPv3 trap filters

Category	Feature
Management Access	Console CLI
	HTTP
	HTTPS
	Telnet
	SSH v2.0
	PPPoE Management Tunnel
	ACLs to filter HTTP, HTTPS, Telnet, and SNMP access
	Banners
Logging	Event Logging
	Remote Syslog (4 servers)
	Console display and clear
	Web display and clear
System Clock	SNTP client
	Manual date and time setting
	Time zone
	Daylight saving
Bridge Filters	Wireless to wireless
	Ethernet protocols
	Management from wireless
Authentication	Management user name & password
	802.1x supplicant
	RADIUS Accounting
	TACACS+ AAA
	Intrusion Detection and Lockout
Status Information	System configuration
	Wireless configuration
	Wireless client status
QoS	IEEE 802.1p
	Source/Destination MAC address
	Ethernet protocol type
	SpectraLink Voice Priority (SVP)
Rate Limiting	Rate limiting of incoming broadcast or multicast traffic on Ethernet interfaces and wireless broadcast or multicast traffic
	Rate limiting of incoming wireless broadcast or multicast traffic on the IronPoint 200 (release 02.02.01 and later.)

Category	Feature
Radio Settings	Country Code setting
	External antenna
	Auto channel selection
	Selectable mode operation
	Selectable power setting
	Data rate settings
	Selectable beacon interval
	Selectable DTIM interval
	Adjustable RTS threshold
	Adjustable fragmentation threshold
	Maximum clients setting (64)
	802.11a Turbo mode
	IAPP support
	Load Balance
	SSID Prioritization
	Data rate based access control (release 02.02.04 and later)
	RSSI rate based access control (release 02.02.04 and later)
Wireless Security	Virtual access points per radio (4)
	Hidden SSID
	RADIUS MAC authentication
	Local MAC authentication
	802.1x client authentication
	WEP authentication
	WEP encryption (64, 128, 152 bit)
	Dynamic WEP keys with 802.1x
	WPA and WPA2 over 802.1x
	WPA and WPA2 Pre-shared Key
	WPA-WPA2 Mixed Mode
	WPA2 Pre-authentication
	TKIP encryption
	AES-CCMP encryption
RF Monitoring	Supported

What's New in This Edition

This section presents the enhancements in the IronPoint 200.

IronPoint 200 Release 02.2.04

Enhancement	Description	See ...
Data rate based access and RSSI rate based access	The datarate-based-access and the rssi-based-access CLI commands are introduced in this release. The datarate-based-access command prevents clients from transmitting data frames to the access point with low data rates, while the rssi-based-access command prevents clients with low RSSI values from connecting to an access point.	Chapter: Radio Interface Configuration Sections: “datarate-based-access” on page 21-7 and “rssi-based-access” on page 21-10

Chapter 2

Initial Configuration and Software Upgrades

Foundry IronPoint Access Point can be configured using the automatic discovery and configuration (ADC) feature or by manually defining each feature on an access point. The method you choose determines which procedure you need to use to configure or upgrade your access points.

ADC allows you to rapidly configure a number of access points, straight out of the box, by mapping an access point's MAC address to an IP address, subnet mask, and default gateway. This information is mapped on an IronPoint-FES interface. Once the access point is attached to the IronPoint-FES, the switch assigns the predefined IP address, subnet mask, and default gateway to the access point with the matching MAC address.

Foundry's IronView Network Manager, an SNMP-based network management software application, allows the IronPoint access point and the IronPoint-FES to be automatically discovered and configured by IronView Network Manager. Configuration definitions can be created in IronView Network Manager, then deployed to IronPoint-FES. Configuration definitions are then downloaded to the access points connected to an IronPoint-FES interface.

This chapter contains the following sections:

- “Initially Configuring an Access Point” allows you to choose one of the following methods to configure access points:
 - “Using ADC to Configure An IronPoint Access Point”
 - “Configuring an Access Point when ADC is not Used”
- “System Defaults”

Initially Configuring an Access Point

Before configuring a new access point, determine if you want to use ADC or not use ADC.

Using ADC to Configure An IronPoint Access Point

If ADC is enabled on the access point, TCP/IP address and default gateway information is configured using one of the following:

- IronView Network Manager application to configure TCP/IP information on an ADC-enabled IronPoint access point. Refer to the *IronView Network Manager User Guide*.

- IronPoint-FastIron Edge Switch to configure TCP/IP information on an ADC-enabled IronPoint Access Point. Refer to the *IronPoint Wireless LAN Configuration Guide for the IronPoint-FastIron Edge Switch*.

Configuring an Access Point when ADC is not Used

If you are not using ADC to configure an access point, follow the procedures presented in the sections below. You can manually configure an access point by using one of the following methods:

- A command line interface (CLI) that can be accessed through a direct connection to the access point's console port.
- A Web-browser interface that can be used through a network connection.
- Simple Network Management Protocol (SNMP) software that can be used through a network connection.

Required Connections

The IronPoint Access Point provides a console port that enables a connection to a PC or terminal for monitoring and configuration. Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the access point. You can use the console cable provided with this package, or use a cable that complies with the wiring assignments shown in "Console Port Pin Assignments" on page D-1.

To connect to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the serial port on the access point.
3. Make sure the terminal emulation software is set as follows:
 - Select the appropriate serial port (COM port 1 or 2).
 - Set the data rate to 9600 baud.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set flow control to none.
 - Set the emulation mode to VT100.
 - When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

4. Once you have set up the terminal correctly, press the [Enter] key to initiate the console connection. The console login screen displays.

For a description of how to use the CLI, see “Using the Command Line Interface” on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 5-1.

Logging In

Enter “admin” for the user name. Type the default password “admin” and press [Enter] at the password prompt. The CLI prompt appears as shown below.

```
Username: admin
Password:
Foundry AP#
```

Setting the IP Address

The access point has a default IP address of 169.254.1.1, which may not be compatible with your network. You will therefore have to use the CLI to assign a compatible IP address or configure the access point to obtain its IP settings from a DHCP server.

Type “configure” to enter configuration mode, then type “interface ethernet” to access the Ethernet interface-configuration mode.

```
Foundry AP#configure
Foundry AP(config)#interface ethernet
Foundry AP(if-ethernet)#
```

Type “ip address *ip-address netmask gateway*,” where “ip-address” is the access point’s IP address, “netmask” is the network mask for the network, and “gateway” is the default gateway router. Check with your system administrator to obtain an IP address that is compatible with your network.

```
Foundry AP(if-ethernet)#ip address 192.168.2.2 255.255.255.0 192.168.2.254
Foundry AP(if-ethernet)#
```

Alternatively, to configure the access point to obtain its IP settings from a DHCP server, type “ip dhcp.”

```
Foundry AP(if-ethernet)#ip dhcp
Foundry AP(if-ethernet)#
```

After configuring the access point’s IP parameters, you can access the management interface from anywhere within the attached network. The command line interface can also be accessed using Telnet from any computer attached to the network.

Note: Country regulations for wireless products differ from country to country. The access points may be shipped with the country code already preset, as required by the country, or set to the default setting of “99”. If your country code is pre-set (for example, for United States, Canada, Japan, and New Zealand), it is prohibited for you to change this setting. If country code on your

access point is set to "99", then you may set the country code, but you can set it only to the country in which the access point is to be used.

It is very important to follow these instructions carefully. Selection of the wrong country code for your device could result in the device operating outside of authorized frequency/power allocations and lead to possible legal action by the regulatory authority in your country

Although Foundry has attempted to provide accurate information in these materials, Foundry assumes no legal responsibility for the accuracy or completeness of the information. Please note that Foundry's product information does not constitute or contain any guarantee, warranty or legally binding representation, unless expressly identified as such in a duly signed writing.

Setting Passwords

Management access to the access point's CLI or Web interface is controlled through user names and passwords. Each user name has an associated access level; either Admin or Read-Only. A Read-Only user has only read access to the management interfaces. However, an Admin user has write access for all parameters. The first time you log into the CLI, you should define a new Admin user name and password, then delete the default user name.

User names and passwords can consist of between one and 64 alphanumeric characters and are case sensitive. To prevent unauthorized access to the access point, set a new Admin user name and password, then remove the default user name as follows:

1. Open the console interface with the default user name "admin" and password "admin."
2. Type "configure" and press <Enter>.
3. Type "user *username* *password* 0," where *username* is your new user name, *password* is your new password, and 0 indicates the Admin privilege level. Press <Enter>.
4. Type "no user admin," to delete the default Admin user from the system. Press <Enter>.

```
Username: admin
Password:
Foundry AP#configure
Foundry AP(config)#user [username] [password] 0
Foundry AP(config)#no user admin
Foundry AP(config)#
```

Enabling SNMP Management Access

The access point can be configured to accept management commands from Simple Network Management Protocol (SNMP v1, v2c, v3) applications. You can configure the access point to respond to SNMP requests and generate SNMP traps. By default, SNMP management is enabled on the access point.

Access to the access point using SNMP v1 and v2c is controlled by community strings. To communicate with the access point, a management station must first submit a valid community string for authentication. Access to the access point using SNMP v3 is controlled through defined users and groups that provide user authentication and data encryption for additional security.

When SNMP management stations send requests to the access point (either to return information or to set a parameter), the access point provides the requested data or sets the specified parameter. The access point can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP v1 and v2c stations, as well as to authorize these stations to receive trap messages from the access point. You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, it is recommended that you set SNMP management access to the access point to disabled.

To prevent unauthorized access to the access point via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>.
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Foundry AP(config)#snmp-server community ironpoint rw
Foundry AP(config)#snmp-server community foundry ro
Foundry AP(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the access point.

To configure a trap receiver, complete the following steps:

1. From the configuration mode prompt, type “snmp-server host *host-address community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host. Press <Enter>.

2. In order to configure the access point to send SNMP notifications, you must enable SNMP. Type "snmp-server enable server." Press <Enter>.

```
Foundry AP(config)#snmp-server host 1 10.1.19.23 ironpoint
Foundry AP(config)#snmp-server enable server
```

System Defaults

The following table lists some of the access point's basic system defaults. To reset the access point to factory defaults, use the CLI command "reset configuration" from the Exec level prompt.

Feature	Parameter	Default
Automatic Discovery and Configuration	adc enable	Depends on version of software image
Identification	System Name	IronPoint 200: Foundry AP
Administration	User Name	admin
	Password	admin
	FTP User Name	<i>null</i>
	FTP password	<i>null</i>
General	HTTP Server	Enabled
	HTTP Server Port	80
	HTTPS Server	Enabled
	HTTPS Server Port	443
	Telnet Server	Enabled
	SSH Server	Enabled
	SSH Server Port	22
IP	DHCP	Disabled
	IP Address	169.254.1.1
	Subnet Mask	255.255.0.0
	Default Gateway	169.254.1.254
	Primary DNS IP	0.0.0.0
	Secondary DNS IP	0.0.0.0
RADIUS (Primary and Secondary)	IP/Host Name	0.0.0.0
	Port	1812
	Key	DEFAULT
	Timeout	5 seconds
	Retransmit	3
MAC Authentication	MAC	Local MAC
	Authentication Session Timeout	0 minutes (disabled)
	Local MAC System Default	Allowed
	Local MAC Permission	Allowed

Feature	Parameter	Default
802.1x Authentication	802.1x Status	Disabled
	Broadcast Key Refresh	120 minutes
	RADIUS Session Timeout	0 minutes (disabled)
	802.1x Supplicant	Disabled
Intrusion Detection and Lockout	ids	Disabled
	Number of attempts (802.1X, pre-shared key, static WEP)	5 attempts per cycle
	Permanently Block Intruder	Enabled
	Block stations	(no default)
	Cycle timer	60 seconds during cycle 60 seconds between cycle
Filter Control	Local Bridge	Disabled
	Local Management	Enabled
	Ethernet Type	Disabled
VLAN	VLAN Tag Support	Disabled
	Management VLAN ID	1
SNMP	State	Enabled
	Location	<i>null</i>
	Contact	Contact
	Community (Read Only)	Public
	Community (Read/Write)	Private
	Traps	Enabled
	Trap Receiver IP/Host Name	<i>null</i>
	Trap Receiver Community	Public
	SNMP v3 Groups	RO RWAuth RWPriv
	SNMP v3 Users	<i>none</i>
System Logging	Syslog	Disabled
	Logging Host	Disabled
	Logging Console	Disabled
	IP Address / Host Name	0.0.0.0
	Logging Level	Informational
	Logging Facility Type	16
System Clock	SNTP Server Status	Disabled
	Date and Time	Jan 1 (if there is no time server)
	Daylight Saving Time	Disable
	Time Zone	(GMT-05) Eastern Time (US & Canada)
Ethernet Interface	Speed and Duplex	Auto

Feature	Parameter	Default
Wireless Interface 802.11b/g	SSID	IronPoint 200: Foundry AP (0 to 3)
	Radio Mode	802.11b+g
	IAPP	Disabled
	Channel	Auto
	Auto Channel Select	Enabled
	Transmit Power	Full
	Data Rate	54 Mbps
	Fragmentation Threshold	2346 bytes
	RTS Threshold	2347 bytes
	Beacon Interval	100 TUs
	DTIM Interval	1 beacon
	Maximum Association	64 stations
	Default VLAN ID	1
	Data rate based access	Disabled
	RSSI rate based access	Disabled
Wireless Security 802.11b/g	Hidden SSID	Disabled
	Authentication Type	Open System
	WPA Mode	Pre-Shared key
	WPA Client	Disabled
	Multicast Cipher	WEP
	WEP Encryption	Disabled
	WEP Key Length	None
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	<i>null</i>
	Data rate based access	Disabled
	RSSI rate based access	Disabled

Feature	Parameter	Default
Wireless Interface 802.11a	SSID	IronPoint 200: Foundry AP (0 to 3)
	Channel	Auto
	Auto Channel Select	Enabled
	Turbo Mode	Disabled
	Transmit Power	Full
	Data Rate	54 Mbps
	Fragmentation Threshold	2346 bytes
	RTS Threshold	2347 bytes
	Beacon Interval	100 TUs
	DTIM Interval	1 beacon
	Maximum Association	64 stations
	Default VLAN ID	1
	Data rate based access	Disabled
	RSSI rate based access	Disabled
Wireless Security 802.11a	Hidden SSID	Disabled
	Authentication Type	Open System
	WPA Mode	Pre-Shared key
	WPA Client	Disabled
	Multicast Cipher	WEP
	WEP Encryption	Disabled
	WEP Key Length	None
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	<i>null</i>
	Data rate based access	Disabled
	RSSI rate based access	Disabled

Chapter 3

Using the Web Management Interface

The Foundry IronPoint Access Point provides an embedded HTTP Web agent. Using a Web browser you can configure the access point and monitor wireless clients using the network. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 6.0 or above running on a Windows system).

You can also use the Command Line Interface (CLI) to manage the access point over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4, “Using the Command Line Interface.”

This chapter describes the configuration of the access point’s features based on its Web browser user interface.

Accessing the Web Browser Interface

Prior to accessing the access point from a Web browser, be sure you have first performed the initial configuration tasks described in Chapter 2, “Initial Configuration and Software Upgrades.”

To access the access point from a Web browser, perform the following steps:

1. Type the IP address of the access point into the address bar of your Web browser. The access point login page opens.
2. Type the user name and password in the appropriate text fields.

Note: Access to the access point’s Web interface is controlled by the same user name and password as the CLI. If you set a new user name and password during the initial configuration (see “Setting Passwords” on page 2-4), enter the new user name and password. Otherwise, enter the default user name “admin” and default password “admin.”

3. Click Login.

If the user name and password are accepted, the home page opens and you have access to access point configuration.

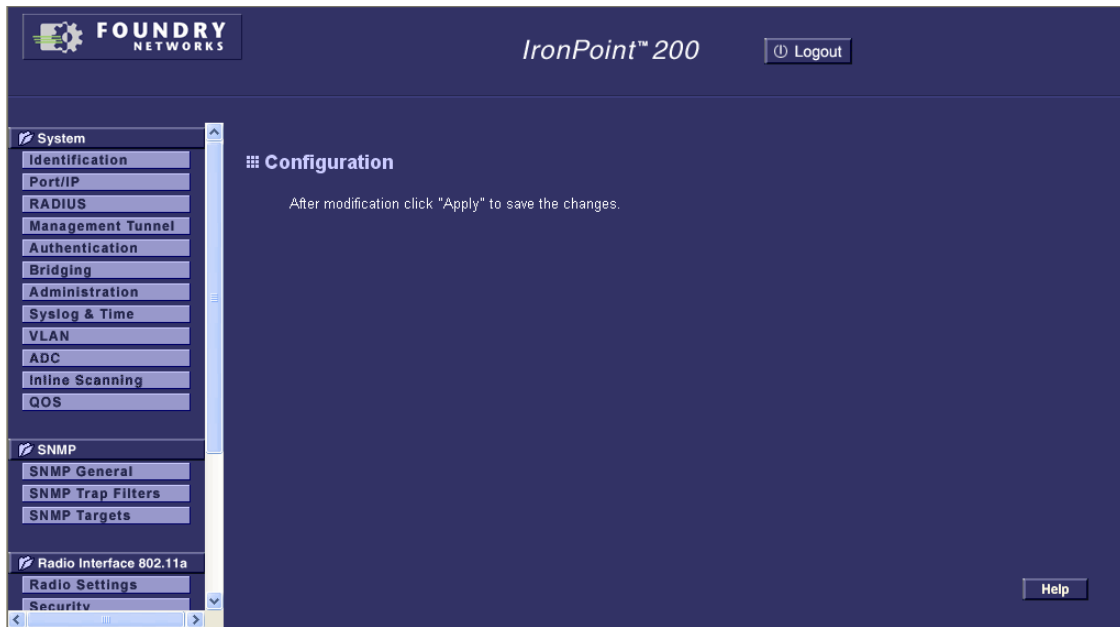


Navigating the Web Browser Interface

Home Page

When have successfully logged in to the access point's Web interface, the home page is displayed as shown below. The home page displays menus for System, SNMP, Radio Interface 802.11a, Radio

Interface 802.11g, and Status options on the left side of the screen. The menu links are used to display pages used to configure access point options and display access point status information.



Configuration Options

Configurable parameters have a text field box, drop-down list, check box, or radio button. Once a configuration change has been made on a page, be sure to click on the “Apply” button to confirm the new setting. The following table summarizes the common Web page configuration buttons.

Button	Action
Apply	Sets specified values to the system.
Cancel	Cancels specified values and restores current values prior to pressing “Apply.”
Help	Provides help information on access point configuration features.

Menus

The access point Web Management Interface menus include links to the pages specified in the following table.

Menu	Description	Page
<i>System</i>		
Identification	Specifies the name of the access point.	11-1
Port / IP	Configures the Ethernet port speed and duplex mode and the access point’s IP settings	8-4

Menu	Description	Page
RADIUS	Configures the RADIUS server for wireless client authentication	15-6
Management Tunnel		
Authentication	Configures 802.1x client authentication and MAC address authentication	19-2
Bridging	Filters communications between wireless clients, access to the management interface from wireless clients, traffic matching specific Ethernet protocol types, and IAPP setting	18-6
Administration	Configures user name and password for management access; enables the Telnet or SSH servers; upgrades software from local file, FTP or TFTP server; resets configuration settings to factory defaults; and resets the access point	9-1
Syslog & Time	Controls logging of error messages; sets the system clock via SNTP server or manual configuration	12-5
VLAN	Enables VLAN support and sets the management VLAN ID	23-3
ADC	Allows you to rapidly configure a number of access points, straight out of the box, by configuring access point information on an IronPoint-FES interface, which is deployed to the access point when an access point is attached to that interface.	6-10
Inline Scanning	Enables an access point to scan the current channel more frequently (once every ten minutes) to detect neighbor access points and report them to IronPoint Wireless Location	6-11
QoS	Specifies traffic priorities on the access point	25-1
SNMP		
SNMP General	Controls access to this access point from management stations using SNMP, as well as the hosts that will receive trap messages	10-6
SNMP Trap Filters	Defines trap filters for SNMPv3 users	10-14
SNMP Targets	Specifies SNMPv3 users that will receive trap messages	10-17
Radio Interface 802.11a		
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, beacon settings, and default VLAN ID	21-18
Security	Configures data encryption with Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	22-10
Radio Interface 802.11g		
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, beacon settings, and default VLAN ID	21-26
Security	Configures data encryption with Wired Equivalent Protection (WEP) or Wi-Fi Protected Access (WPA)	22-10

Menu	Description	Page
<i>Status</i>		
AP Status	Displays current system and wireless interface settings	24-4
Neighbor APs	Displays the neighbor access points that have been detected on the network	27-3
Stations	Displays the status of current associated clients	24-9
Event Log	Displays system log messages	12-6

Chapter 4

Using the Command Line Interface

This chapter describes how to use the Command Line Interface (CLI) for configuring and managing the IronPoint Access Point.

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the IronPoint Access Point over a direct connection to the console port, or via a Telnet connection, the access point can be managed by entering command keywords and parameters at the prompt. Using the access point's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the access point through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user name is "admin" and the default password is "admin.") When the password is entered, the CLI displays the "Foundry AP#" prompt.
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "exit" command. The access point saves all configurations settings as soon as they are made, so the configuration is always retained even after a reboot.

After connecting to the system through the console port, the login screen displays:

```
Username: admin
Password:
Foundry AP#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the default IP address used by the access point is 169.254.1.1, consisting of a network portion (169.254.1) and a host portion (1).

To access the access point through a Telnet session, you must first set the IP address for the access point, and set the default gateway if you are managing the access point from a different IP subnet. For example:

```
Foundry AP#configure
Foundry AP(config)#interface ethernet
Foundry AP(if-ethernet)#ip address 10.1.0.1 255.255.255.0 10.1.0.254
Foundry AP(if-ethernet)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the access point with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Foundry AP#” prompt to show that you are using executive access mode (i.e., Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “exit” command. The access point saves all configurations settings as soon as they are made, so the configuration is always retained even after a reboot.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:
Foundry AP#
```

Note: You can open up to four sessions to the access point via Telnet.

Entering Commands

This section describes how to enter CLI commands. Make sure an IP address and country code has been properly configured on the access point before using the CLI. Refer to Chapter 2, “Initial Configuration”.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces ethernet,” **show** and **interfaces** are keywords, and **ethernet** is an argument that specifies the interface type.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Foundry AP(config)#username smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “configure” example, typing **con** followed by a tab will result in printing the command up to “**configure**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by following a command with the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current configuration mode (Exec, Global Configuration, or Interface). You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Foundry AP#show ?
 authentication Show Authentication parameters
 bootfile        Show bootfile name
 filters         Show filters
 hardware        Show hardware version
 history         Display the session history
 interface       Show interface information
 line           TTY line information
 logging         Show the logging buffers
 pppoe          Show PPPoE parameters
 radius         Show radius server
 snmp           Show snmp statistics
 sntp           Show sntp statistics
 station        Show 802.11 station table
 system         Show system information
 tech-support    System snapshot for tech support
 version        Show system version
Foundry AP#show
```

The command “**show interface ?**” will display the following information:

```
Foundry AP#show interface ?
  ethernet  Show Ethernet interface
  wireless  Show wireless interface
  <cr>
Foundry AP#show interface
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Foundry AP#show s?
snmp      snmp      station  system
Foundry AP#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “**?**” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode
Exec	Privileged
Configuration	Global Interface-ethernet Interface-wireless interface-wireless-VAP

Exec Commands

When you open a new console session on access point, the system enters Exec command mode. Only a limited number of the commands are available in this mode. You can access all other commands only from the configuration mode. To access Exec mode, open a new console session with the user name “admin.” The command prompt displays as “Foundry AP#” by default for Exec mode.

```
Username: admin
Password: [system login password]
Foundry AP#
```

Configuration Commands

Configuration commands are used to modify access point settings. These commands modify the running configuration and are saved in memory.

The configuration commands are organized into four different modes:

- Global Configuration (GC) - These commands modify the system level configuration, and include commands such as **username** and **password**.
- Interface-Ethernet Configuration (IC-E) - These commands modify the Ethernet port configuration, and include commands such as **dns** and **ip**.
- Interface-Wireless Configuration (IC-W) - These commands modify the wireless port configuration of global parameters for the radio, and include commands such as **channel** and **transmit-power**.
- Interface-Wireless Virtual Access Point Configuration (IC-W-VAP) - These commands modify the wireless port configuration for each VAP, and include commands such as **ssid** and **authentication**.

To enter the Global Configuration mode, enter the command **configure** in Exec mode. The system prompt will change to “Foundry AP(config)#” which gives you access privilege to all Global Configuration commands.

```
Foundry AP#configure
Foundry AP(config)#
```

To enter Interface mode, you must enter the “**interface ethernet**,” or “**interface wireless a**,” or “**interface wireless g**” command while in Global Configuration mode. The system prompt will change to “Foundry AP(if-ethernet)#,” or “Foundry AP(if-wireless a)#,” or “Foundry AP(if-wireless g)#,” indicating that you have access privileges to the associated commands. Note that each wireless interface, for 802.11a and 802.11g, must be configured separately. You can use the **exit** command to return to the Exec mode.

```
Foundry AP(config)#interface ethernet
Foundry AP(if-ethernet)#
```

To enter VAP mode, you must enter the “**vap**” command while in Interface Wireless Configuration mode. The system prompt will change to “Foundry AP(if-wireless a: VAP[0])#,” or “Foundry AP(if-wireless g: VAP[0])#,” indicating that you have access privileges to the associated commands for the VAP (numbered 0, 1, 2, and 3). You can use the **end** command to return to the Interface-Wireless mode.

```
Foundry AP(config)#interface wireless a
Foundry AP(if-wireless a)#vap 0
Foundry AP(if-wireless a: VAP[0])#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates a task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes from cursor to the end of the command line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Shows the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor backward one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Chapter 5

Complete List of CLI Commands

This chapter provides a complete list of CLI commands separated into functional groups. Cross-reference page numbers are provided to the detailed description for each command.

Command Groups

The access point CLI commands can be broken down into the functional groups shown below.

Command Group	Description	Page
General System	Basic commands for entering configuration mode, restarting the system, quitting the CLI, and limiting broadcast or multicast traffic.	5-2
IP Configuration	Configures the access point's IP settings	5-3
Management Access	Configures user names and passwords, SSH, Telnet, and browser management options	5-3
System Information	Displays access point information and current status	5-3
System Identification	Specifies the host name for the access point	5-4
System Logging	Configures system logging parameters	5-4
System Clock	Configures SNTP and system clock settings	5-4
SNMP	Configures community access strings, trap receivers, and assigns SNMP v3 users to groups	5-4
Flash/File	Manages code image or access point configuration files	5-5
RADIUS Client	Configures the RADIUS client used with 802.1x authentication	5-6
802.1x Authentication	Configures 802.1x authentication	5-7
MAC Address Authentication	Configures MAC address authentication	5-6
Bridging and Traffic Filtering	Filters communications between wireless clients, controls access to the management interface from wireless clients, and filters traffic using specific Ethernet protocol types	5-8

Command Group	Description	Page
Ethernet Interface	Configures connection parameters for the Ethernet interface	5-8
Management Tunnel	Configures parameters for a PPPoE management tunnel on the Ethernet interface	5-8
Radio Interface	Configures radio interface settings	5-9
Wireless Security	Configures radio interface security and encryption settings	5-11
VLAN	Configures VLAN membership	5-11
QoS	Configures traffic priorities	5-11

The access mode shown in the following tables is indicated by these abbreviations: **GC** (Global Configuration), **IC-E** (Interface-Ethernet Configuration), **IC-W** (Interface-Wireless Configuration), and **IC-W-VAP** (Interface-Wireless VAP Configuration).

General System Commands

Command	Function	Mode	Page
configure	Activates global configuration mode	Exec	6-4
interface	Enters specified interface configuration mode	GC	6-4
end	Returns to Exec mode from any configuration mode	GC, IC	6-4
exit	Returns to the previous configuration mode or exits the CLI	any	6-5
help	Displays information on using the CLI	any	6-5
prompt	Customizes the command line prompt	GC	6-6
ping	Sends ICMP echo request packets to another node on the network	Exec	6-6
reset	Restarts the system	Exec	6-7
show history	Shows the command history buffer	Exec	6-7
show crashdump	Used by Foundry Technical Support	Exec	A-2
show line	Shows the configuration settings for the console port	Exec	6-8
trace show cpu-load	Show the CPU utilization during the last five minutes.	Exec	6-8
adc enable	Enables and disables the ADC feature on the access point	GC	6-9
inline-scanning	Provides support for IronPoint Wireless Location Manager	GC	6-10
wireless-rate-limit	Limits the number of wireless broadcast or multicast frames that an access point receives per second	GC	6-12

IP Configuration Commands

Command	Function	Mode	Page
ip address	Sets the IP address for the Ethernet interface	IC-E	8-2
ip dhcp	Submits a DHCP request for an IP address	IC-E	8-3
dns primary-server	Specifies the primary name server	IC-E	8-3
dns secondary-server	Specifies the secondary name server	IC-E	8-3

Management Access Commands

Command	Function	Mode	Page
user	Configures new user names and passwords for management access	GC	9-2
ip ssh-server enable	Enables the Secure Shell server	IC-E	9-4
ip ssh-server port	Sets the Secure Shell port	IC-E	9-5
ip telnet-server enable	Enables the Telnet server	IC-E	9-5
ip http port	Specifies the port to be used by the Web browser interface	GC	9-6
ip http server	Allows the access point to be monitored or configured from a browser	GC	9-7
ip https port	Specifies the UDP port number used for a secure HTTP connection to the access point's Web interface	GC	9-7
ip https server	Enables the secure HTTP server on the access point	GC	9-8

System Information Commands

Command	Function	Mode	Page
show system	Displays system information	Exec	24-1
show version	Displays version information for the system software	Exec	24-2
show hardware	Displays version information of the system hardware	Exec	24-3
show tech-support	Displays information from all CLI show commands	Exec	24-3
show station	Displays the wireless clients associated with the access point.	Exec	24-8
show inventory	Displays the status and configuration information for each VAP on an access point	Exec	24-10

System Identification Commands

Command	Function	Mode	Page
system name	Specifies the host name for the access point	GC	11-1

System Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	12-2
logging host	Adds a syslog server host IP address that will receive logging messages	GC	12-3
logging console	Initiates logging of error messages to the console	GC	12-3
logging level	Defines the minimum severity level for event logging	GC	12-3
logging facility-type	Sets the facility type for remote logging of syslog messages	GC	12-4
logging clear	Clears all log entries in access point memory	GC	12-6
show logging	Displays the state of logging	Exec	12-4
show event-log	Displays all log entries in access point memory	Exec	12-6

System Clock Commands

Command	Function	Mode	Page
sntp-server ip	Specifies one or more time servers	GC	13-3
sntp-server enable	Accepts time from the specified time servers	GC	13-3
sntp-server date-time	Manually sets the system date and time	GC	13-2
sntp-server daylight-saving	Sets the start and end dates for daylight savings time	GC	13-3
sntp-server timezone	Sets the time zone for the access point's internal clock	GC	13-4
show sntp	Shows current SNTP configuration settings	Exec	13-4

SNMP Commands

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	10-3

Command	Function	Mode	Page
snmp-server contact	Sets the system contact string	GC	10-4
snmp-server engine id	Sets the engine ID for SNMP v3	GC	10-10
snmp-server enable server	Enables SNMP service and traps	GC	10-2
snmp-server host	Specifies recipients of SNMP notifications	GC	10-4
snmp-server trap	Enables specific SNMP notifications	GC	10-5
snmp-server location	Sets the system location string	GC	10-3
snmp-server user	Sets the name of the SNMP v3 user	GC	10-11
snmp-server targets	Configures SNMP v3 notification targets	GC	10-16
snmp-server filter	Configures SNMP v3 notification filters	GC	10-13
snmp-server filter-assignment	Assigns SNMP v3 notification filters to targets	GC	10-16
show snmp groups	Displays the pre-defined SNMP v3 groups	Exec	10-12
show snmp users	Displays SNMP v3 user settings	Exec	10-12
show snmp group-assignments	Displays the assignment of users to SNMP v3 groups	Exec	10-12
show snmp target	Displays the SNMP v3 notification targets	Exec	10-17
show snmp filter	Displays the SNMP v3 notification filters	Exec	10-14
show snmp filter-assignments	Displays the SNMP v3 notification filter assignments	Exec	10-17
show snmp	Displays the status of SNMP communications	Exec	10-6

Flash/File Commands

Command	Function	Mode	Page
bootfile	Specifies the file or image used to start up the system	GC	7-3
show bootfile	Displays the name of the current operation code file that booted the system	GC	7-4
copy	Copies a code image or configuration between flash memory and a FTP/TFTP server	Exec	7-1
delete	Deletes a file or code image	Exec	7-4
dir	Displays a list of files in flash memory	Exec	7-3

RADIUS Client

Command	Function	Mode	Page
radius-server address	Specifies the RADIUS server	GC	15-2
radius-server port	Sets the RADIUS server network port	GC	15-3
radius-server key	Sets the RADIUS encryption key	GC	15-3
radius-server retransmit	Sets the number of retries	GC	15-3
radius-server timeout	Sets the interval between sending authentication requests	GC	15-4
radius-server port-accounting	Sets the RADIUS Accounting server network port	GC	15-4
radius-server timeout-interim	Sets the interval between transmitting accounting updates to the RADIUS server	GC	15-4
radius-server radius-mac-format	Sets the format for specifying MAC addresses on the RADIUS server	GC	15-5
radius-server vlan-format	Sets the format for specifying VLAN IDs on the RADIUS server	GC	15-5
show radius	Shows the current RADIUS settings	Exec	15-5

MAC Address Authentication

Command	Function	Mode	Page
address filter default	Sets filtering to allow or deny listed addresses	GC	19-3
address filter entry	Enters a MAC address in the filter table	GC	19-3
address filter delete	Removes a MAC address from the filter table	GC	19-4
mac- authentication server	Sets address filtering to be performed with local or remote options	GC	19-4
mac- authentication session-timeout	Sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database	GC	19-4
show authentication	Shows all 802.1x authentication settings, as well as the address filter table	Exec	19-5

802.1x Authentication

Command	Function	Mode	Page
802.1x	Configures 802.1x as disabled, supported, or required	IC-W-VAP	19-7
802.1x broadcast-key-refresh-rate	Sets the interval at which the primary broadcast keys are refreshed for stations using 802.1x dynamic keying	IC-W-VAP	19-8
802.1x session-key-refresh-rate	Sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying	IC-W-VAP	19-8
802.1x session-timeout	Sets the timeout after which a connected client must be re-authenticated	IC-W-VAP	19-8
802.1x supplicant user	Sets the supplicant user name and password for the access point	GC	19-11
802.1x supplicant	Enables the access point to operate as a 802.1x supplicant	GC	19-12

Intrusion Detection and Lockout

Command	Function	Mode	Page
ids enable	Enables the Intrusion Detection and Lockout feature.	GC	17-3
ids 802.1x	Defines the number of attempts for each Intrusion and Detection cycle when 802.1X authentication is used to authenticate wireless clients.	GC	17-3
ids permanently-block-intruder	Enables the ability to permanently block login attempts that failed all login cycles	GC	17-4
ids pre-shared	Defines the number of attempts for each Intrusion and Detection cycle when pre-shared key authentication is used to authenticate wireless clients.	GC	17-4
ids static	Defines the number of attempts for each Intrusion and Detection cycle when static WEP authentication is used to authenticate wireless clients.	GC	17-4
ids station block	Locks or unlocks a MAC address	GC	17-5
ids timer	Defines the timers for a login cycle (cycle time) and for the delay between cycles (block time)	GC	17-5
show ids	Displays the definition of the parameters for the Intrusion Detection and Lockout feature	GC	17-6
show station ids-block	Displays the MAC addresses that have been blocked from the network	GC	17-6

Bridging and Traffic Filtering Commands

Command	Function	Mode	Page
iapp	Enables the protocol signaling required to hand over wireless clients roaming between different 802.11f-compliant access points	GC	18-2
filter local-bridge	Disables communication between wireless clients	GC	18-3
filter ap-manage	Prevents wireless clients from accessing the management interface who are currently associated with the same access point	GC	18-3
filter ethernet-type enable	Checks the Ethernet type for all incoming and outgoing Ethernet packets against the protocol filtering table	GC	18-3
filter ethernet-type protocol	Sets a filter for a specific Ethernet type	GC	18-4
filter ethernet-type dynamic-protocol	Specifies a use-defined Ethernet type filter	GC	18-4
filter ethernet-type management-only	Sets Ethernet protocol filters to accept only management packets destined for the access point	GC	18-5
show filters	Shows the filter configuration	Exec	18-5

Ethernet Interface Commands

Command	Function	Mode	Page
rate-limit	Limits the rate at which broadcast or multicast packets are received on Ethernet interfaces	IC-E	20-2
shutdown	Disables the Ethernet interface	IC-E	20-2
speed-duplex	Configures speed and duplex operation	IC-E	20-3
show interface ethernet	Shows the status for the Ethernet interface	Exec	20-3

Management Tunnel (PPPoE) Commands

Command	Function	Mode	Page
ip pppoe	Enables PPPoE on the Ethernet interface	IC-E	14-2
pppoe ip allocation mode	Specifies how IP addresses for the PPPoE tunnel are configured on the interface	IC-E	14-3
pppoe ipcp dns	Negotiates DNS for the PPPoE tunnel	IC-E	14-3
pppoe lcp echo-interval	Sets LCP echo interval for the PPPoE tunnel	IC-E	14-3
pppoe lcp echo-failure	Sets LCP echo timeout for the PPPoE tunnel	IC-E	14-4

Command	Function	Mode	Page
pppoe local ip	Sets local IP address for the PPPoE tunnel	IC-E	14-4
pppoe remote ip	Sets remote IP address for the PPPoE tunnel	IC-E	14-5
pppoe username	Sets the user name for the PPPoE tunnel	IC-E	14-5
pppoe password	Sets the password for the PPPoE tunnel	IC-E	14-5
pppoe service-name	Sets the service name for the PPPoE tunnel	IC-E	14-6
pppoe restart	Restarts the PPPoE connection with updated parameters	IC-E	14-6
show pppoe	Shows information about the PPPoE configuration	PE	14-6

Radio Interface Commands

Command	Function	Mode	Page
antenna	Selects built-in antennas or an optional high-gain external antenna	IC-W	21-4
association-timeout-interval	Configures the idle time interval (when no frames are sent) after which a client is disassociated from the VAP interface	IC-W-VAP	21-4
authentication-timeout-interval	Configures the time interval after which clients must be re-authenticated	IC-W-VAP	21-5
auto-channel-selection-mode-overlap	Allows the 802.11b/g radio to select any valid channel available, including overlapping and non-overlapping channels	IC-W-VAP	21-24
auto-refresh-rate	Allows the access point radio to scan the air waves at the specified interval so it can automatically select a channel.	IC-W-VAP	21-5
beacon-interval	Configures the rate at which beacon signals are transmitted from the access point	IC-W	21-6
channel	Configures the radio channel	IC-W	21-6
closed-system	Prevents access from clients without a pre-configured SSID	IC-W-VAP	21-6
datarate-based-access	Prevents clients from transmitting data frames to the access point with low data rates.	IC-W	21-7
description	Adds a description to the wireless interface	IC-W-VAP	21-7

Command	Function	Mode	Page
dtim-period	Configures the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions	IC-W	21-8
fragmentation-length	Configures the minimum packet size that can be fragmented	IC-W	21-8
max-association	Configures the maximum number of clients that can be associated with the access point at the same time	IC-W-VAP	21-9
multicast-data-rate	Configures the maximum data rate at which the access point transmits multicast packets on the wireless interface	IC-W	21-9
preamble	Sets the length of the 802.11g signal preamble	IC-W	21-25
radio-mode	Forces the operating mode of the 802.11g radio	IC-W	21-25
rssi-based-access	Prevents clients with low RSSI values from connecting to an access point.	IC-W	21-10
rts-threshold	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications	IC-W	21-11
show auto	Displays the current access point configuration for automatic selection of channel and transmission power	Exec	21-14
show bssid	Displays the BSSID for each VAP interface	Exec	21-14
show interface wireless	Shows the status for the wireless interface	Exec	21-15
show neighbor-ap	Shows neighboring access points	Exec	21-17
show station	Shows the wireless clients associated with the access point	Exec	24-8
shutdown	Disables the wireless interface	IC-W-VAP	21-13
speed	Configures the maximum data rate at which a station can connect to the access point	IC-W	21-11
ssid	Configures the service set identifier	IC-W-VAP	21-12
transmit-power	Adjusts the power of the radio signals transmitted from the access point	IC-W	21-12
turbo	Configures turbo mode to use faster data rate	IC-W	21-13
vap	Provides access to the VAP interface configuration mode	IC-W	21-13

Wireless Security Commands

Command	Function	Mode	Page
authentication	Defines the authentication type allowed by the access point	IC-W-VAP	22-8
encryption	Defines whether or not data encryption is used to provide privacy for wireless communications	IC-W-VAP	22-9
key	Sets the keys used for WEP encryption	IC-W	22-9
transmit-key	Sets the index of the key to be used for encrypting data frames sent between the access point and wireless clients	IC-W-VAP	22-10
cipher-suite	Defines the WPA and WPA2 unicast and multicast cipher algorithms	IC-W-VAP	22-13
wpa-preshared-key	Defines a WPA pre-shared key value	IC-W-VAP	22-14
802.1x pre-authentication	Enables WPA2 pre-authentication for fast secure roaming	IC-W-VAP	22-17
pmksa-lifetime	Sets the time for aging out cached WPA2 Pairwise Master Key Security Association (PMKSA) information	IC-W-VAP	22-18

VLAN Commands

Command	Function	Mode	Page
vlan	Enables VLAN support for all traffic	GC	23-3
management-vlanid	Configures the management VLAN for the access point	GC	23-2
vlan-id	Configures the default VLAN for the VAP interface	IC-W-VAP	23-4

QoS Commands

Command	Function	Mode	Page
qos mode	Sets the QoS traffic priority mode used by the access point	GC	25-3
qos mac-addr	Maps source or destination MAC addresses to an 802.1p priority	GC	25-4
qos ether-type	Maps Ethernet protocol types to an 802.1p priority	GC	25-4

Command	Function	Mode	Page
svp	Enables SVP support	GC	25-5
show qos	Shows the current QoS configuration	Exec	25-5
show svp	Shows the current SVP setting	Exec	25-6

TACACS+ and AAA Commands

Command	Function	Mode	Page
tacacs address	Identifies the TACACS+ server that will supply AAA services.	GC	16-4
tacacs key	Defines the TACACS+ key.	GC	16-4
tacacs port	Defines the TCP port that TACACS+ will use for authentication and authorization.	GC	16-4
tacacs port accounting	Defines the TCP port that TACACS+ will use for accounting.	GC	16-5
tacacs retransmit	Specifies how many times the IronPoint access point will resend an authentication request when the TACACS+ server does not respond before considering the TACACS+ server to be unavailable.	GC	16-5
tacacs timeout	Specifies how many seconds the IronPoint access point waits for a response from a TACACS+ server before either retrying the authentication request or determining that the TACACS+ server is unavailable.	GC	16-6
show tacacs	Displays a list of users and their privilege level who have been authenticated and authorized by the TACACS server.	GC	16-6
aaa console enable	Enables the IronPoint access point to use the AAA services	GC	16-7
aaa authentication	Enables the IronPoint access point to use the authentication services of a server that provides AAA services.	GC	16-7
aaa authorization	Enables the IronPoint access point to use the authorization services of a server that provides AAA services.	GC	16-8
aaa accounting	Enables the IronPoint access point to use the accounting services of a server that provides AAA services.	GC	16-9

SSID Prioritization

Command	Function	Mode	Page
ssid-prioritization threshold	Sets the SSID Prioritization Threshold for an access point radio.	IC-W	26-5
ssid priority	Sets the SSID priority of a VAP to low, medium, high, or guaranteed.	IC-W-VAP	26-5

Chapter 6

General System and CLI Settings

This section presents the general system commands and the command to enable and disable the Automatic Discovery and Configuration (ADC) feature.

Using the General System Commands

The CLI commands described in this section set basic system parameters and configure general CLI settings.

There is no Web Management Interface equivalent for these commands, except for in-line scanning and ADC.

Using the CLI

The following table provides a summary of the CLI commands in this section.

Command	Function	Mode	Page
country	Sets the access point country code	Exec	6-2
configure	Activates global configuration mode	Exec	6-4
interface	Enters specified interface configuration mode	GC	6-4
end	Returns to Exec mode from any configuration mode	GC, IC	6-4
exit	Returns to the previous configuration mode or exits the CLI	any	6-5
help	Displays information on using the CLI	any	6-5
prompt	Customizes the command line prompt	GC	6-6
ping	Sends ICMP echo request packets to another node on the network	Exec	6-6
reset	Restarts the system	Exec	6-7
show history	Shows the command history buffer	Exec	6-7
show line	Shows the configuration settings for the console port	Exec	6-8

Command	Function	Mode	Page
trace show cpu-load	Shows CPU utilization in percent during the last five minutes (300 seconds)	Exec	6-8
adc enable	Enables and disables the ADC feature on the access point	GC	6-9
inline-scanning	Provides support for IronPoint Wireless Location Manager	GC	6-10
wireless-rate-limit	Limits the number of wireless broadcast or multicast frames received by the access point per second.	GC	6-12

country

This command configures the access point's country code, which identifies the country of operation and sets the authorized radio channels.

Note: Country regulations for wireless products differ from country to country. The access points may be shipped with the country code already preset, as required by the country, or set to the default setting of "99". If your country code is preset (for example, for United States, Canada, Japan, and New Zealand), you are prohibited from changing this setting. If country code on your access point is set to "99", then you may set the country code, but you can set it only to the country in which the access point is to be used.

It is very important to follow these instructions carefully. Selection of the wrong country code for your device could result in the device operating outside of authorized frequency/power allocations and lead to possible legal action by the regulatory authority in your country

Although Foundry has attempted to provide accurate information in these materials, Foundry assumes no legal responsibility for the accuracy or completeness of the information. Please note that Foundry's product information does not constitute or contain any guarantee, warranty or legally binding representation, unless expressly identified as such in a duly signed writing.

country <country_code>

country_code - A two character code that identifies the country of operation. See the following table for a full list of codes.

Country	Code	Country	Code	Country	Code	Country	Code
Albania	AL	Dominican Republic	DO	Kuwait	KW	Romania	RO
Algeria	DZ	Ecuador	EC	Latvia	LV	Russia	RU
Argentina	AR	Egypt	EG	Lebanon	LB	Saudi Arabia	SA
Armenia	AM	Estonia	EE	Liechtenstein	LI	Singapore	SG
Australia	AU	Finland	FI	Lithuania	LT	Slovak Republic	SK
Austria	AT	France	FR	Luxembourg	LU	Slovenia	SI

Country	Code	Country	Code	Country	Code	Country	Code
Azerbaijan	AZ	Georgia	GE	Macao	MO	South Africa	ZA
Bahrain	BH	Germany	DE	Macedonia	MK	Spain	ES
Belarus	BY	Greece	GR	Malaysia	MY	Sweden	SE
Belgium	BE	Guatemala	GT	Mexico	MX	Switzerland	CH
Belize	BZ	Hong Kong	HK	Monaco	MC	Syria	SY
Bolivia	BO	Hungary	HU	Morocco	MA	Taiwan	TW
Brazil	BR	Iceland	IS	Netherlands	NL	Thailand	TH
Brunei Darussalam	BN	India	IN	New Zealand	NZ	Turkey	TR
Bulgaria	BG	Indonesia	ID	Norway	NO	Ukraine	UA
Canada	CA	Iran	IR	Oman	OM	United Arab Emirates	AE
Chile	CL	Ireland	IE	Pakistan	PK	United Kingdom	GB
China	CN	Israel	IL	Panama	PA	United States	US
Colombia	CO	Italy	IT	Peru	PE	Uruguay	UY
Costa Rica	CR	Japan	JP	Philippines	PH	Venezuela	VE
Croatia	HR	Jordan	JO	Poland	PL	Vietnam	VN
Cyprus	CY	Kazakhstan	KZ	Portugal	PT		
Czech Republic	CZ	North Korea	KP	Puerto Rico	PR		
Denmark	DK	Korea Republic	KR	Qatar	QA		

Default Setting

Pre-set for some countries. If not pre-set, default is 99, no country setting.

Command Mode

Exec

Command Usage

- If your access point is configured by default without a country code (that is, set to "99"), you must set the country code before you can enable radio functions.
- The available Country Code settings can be displayed by using the **country ?** command.

Example

```
Foundry AP#country gb
Foundry AP#
```

configure

This command activates Global Configuration mode. You must enter this mode to modify most of the settings on the access point. You must also enter Global Configuration mode prior to enabling the context modes for Interface Configuration. See “Using the Command Line Interface” on page 4-1.

Default Setting

None

Command Mode

Exec

Example

```
Foundry AP#configure
Foundry AP(config)#
```

interface

This command configures an interface type and enters interface configuration mode.

Syntax

interface <ethernet | wireless <a | g>>

- **ethernet** - Interface for wired network.
- **wireless** - Interface for wireless clients.
- **a** - 802.11a radio interface.
- **g** - 802.11g radio interface.

Default Setting

None

Command Mode

Global Configuration

Example

```
Foundry AP(config)#interface ethernet
Foundry AP(if-ethernet)#
```

end

This command returns to the Exec mode from any configuration mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration

Example

This example shows how to return to the Exec mode from the Interface Configuration mode:

```
Foundry AP(if-ethernet)#end
Foundry AP#
```

exit

This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Exec mode from the Interface Configuration mode and then quit the CLI session:

```
Foundry AP(if-ethernet)#exit
Foundry AP(config)#exit
Foundry AP#exit
CLI session with the Access Point is now closed

Username:
```

help

This command displays information on using the CLI.

Default Setting

None

Command Mode

Any

Example

```

Foundry AP#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
Foundry AP#

```

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

```

prompt <string>
no prompt

```

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

IronPoint 200: Foundry AP

Command Mode

Global Configuration

Example

```

Foundry AP(config)#prompt RD2
RD2(config)#

```

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

```

ping <host_name / ip_address>

```

- *host_name* - Alias of the host.
- *ip_address* - IP address of the host.

Default Setting

None

Command Mode

Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Foundry AP#ping 10.1.0.19
192.168.1.19 is alive
Foundry AP#
```

reset

This command restarts the system or restores the factory default settings.

Syntax

reset <board | configuration>

- **board** - Reboots the system.
- **configuration** - Resets the configuration settings to the factory defaults, and then reboots the system.

Default Setting

None

Command Mode

Exec

Command Usage

When the system is restarted, it will always run the Power-On Self-Test.

Example

This example shows how to reset the system:

```
Foundry AP#reset board
Reboot system now? <y/n>: y
```

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Exec

Command Usage

- The history buffer size is fixed at 10 commands.
- Use the up or down arrow keys to scroll through the commands in the history buffer.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Foundry AP#show history
config
exit
show history
Foundry AP#
```

show line

This command displays the console port's configuration settings.

Command Mode

Exec

Example

The console port settings are fixed at the values shown below.

```
Foundry AP#show line
Console Line Information
=====
databits   : 8
parity     : none
speed      : 9600
stop bits  : 1
=====
Foundry AP#
```

trace show cpu-load

Shows CPU utilization in percent during the last five minutes (300 seconds). CPU utilization percentage is derived from the CPU busy time, divided by the total time. This data is captured every minute (60 seconds). The trace **show cpu-load** command displays the last five minutes of data available. This information is updated every 60 seconds.

Default Setting

None

Command Mode

Exec

Example

```
Foundry AP#trace show cpu-load

CPU Utilization (Updated every 60 Seconds):
 1.2%   1.5%   5.9%   2.3%   1.1%
Foundry AP#
```

Enabling and Disabling ADC

Automatic Discovery and Configuration (ADC) allows you to rapidly configure a number of access points, straight out of the box. You must enter the access point configuration on an IronPoint-FES interface using the CLI or IronView Network Manager. Once the access point is attached to that IronPoint-FES interface, the switch assigns the predefined configuration to the access point.

ADC is enabled by default. If you do not want to use the ADC feature, you must disable the feature.

Using the CLI

adc enable

This command enables or disables the ADC feature support on access points.

Syntax

adc enable
no adc enable

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

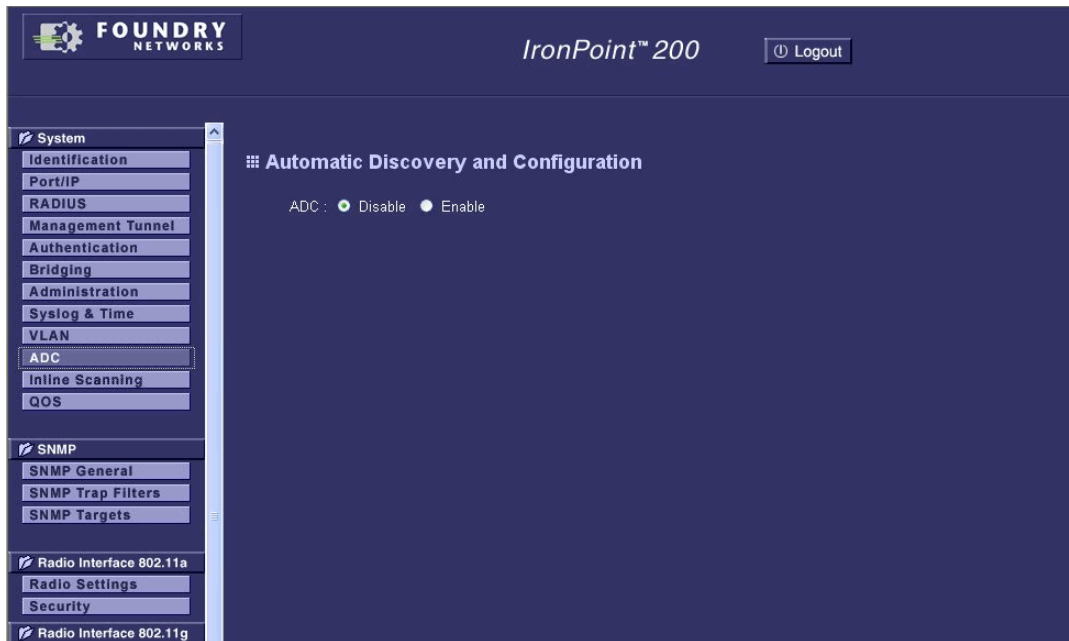
- Use **adc enable** to enable the ADC feature support on an IronPoint access point.
- Use the **no adc enable** command to disable the ADC feature support on an IronPoint access point.

Example

```
Foundry AP(config)#no adc enable
```

Using the Web Management Interface

You can enable or disable ADC using the Web Management Interface. Under the System menu, click ADC, then select Enable to enable ADC or Disable to disable it.



Support for IronPoint Wireless Location Manager

If you are using IronPoint Wireless Location Manager, use the inline scanning feature to allow IronPoint Access Point to scan for and report neighbor access points.

Using the CLI

inline-scanning

Enables the IronPoint Access Point to scan for and report neighbor access points.

Syntax

inline-scanning
no inline-scanning

Default Setting

By default, this feature is disabled.

Command Mode

Global Configuration

Command Usage

The purpose of this command is to enable access point to scan the current channel more frequently (once every ten minutes) to detect neighbor access points and report them to IronPoint Wireless Location Manager.

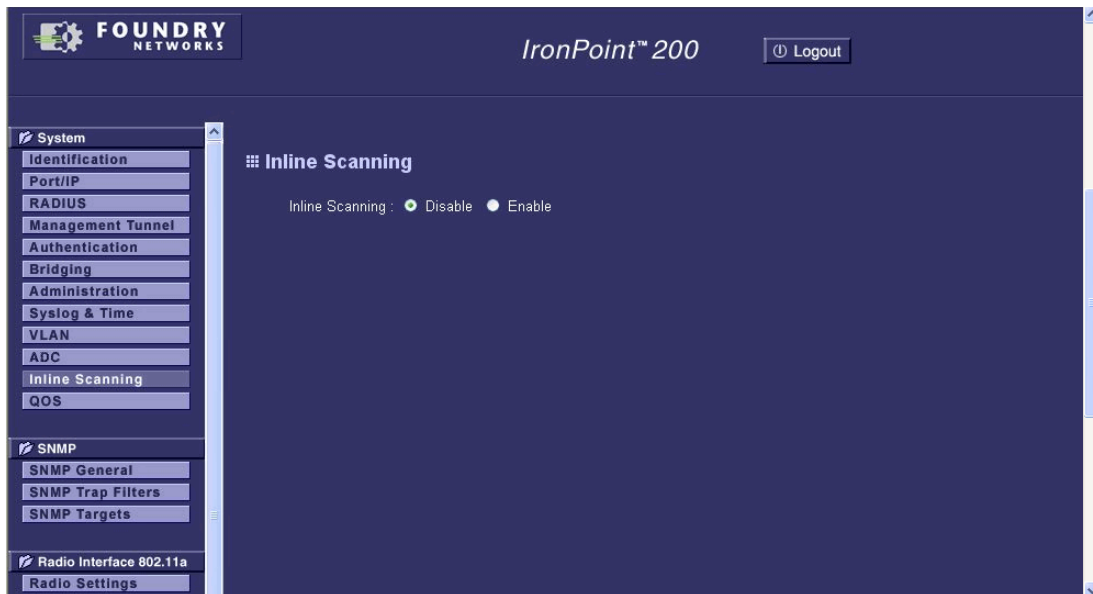
For networks without IronPoint Wireless Location Manager, inline-scanning can be disabled to eliminate unnecessary scanning of the access points. Use the **no** form of the command to disable it.

Example

```
Foundry AP(config)#inline-scanning
```

Using the Web Management Interface

Under the System Menu, click Inline Scanning.



Configurable Parameters

Inline scanning - Enables an access point to scan the current channel more frequently (once every ten minutes) to detect neighbor access points and report them to IronPoint Wireless Location Manager. Select Disable or Enable. (Default: Disable)

For networks without IronPoint Wireless Location Manager, inline-scanning can be disabled to eliminate unnecessary scanning of the access points.

Rate Limiting for Wireless Broadcast or Multicast Frames

Excessive wireless broadcast and multicast frames can cause the IronPoint access point to reboot. You can prevent this from happening by limiting the number of wireless frames received by the access point per second.

Note: This feature is available only on IronPoint 200 Access Points running software release 02.02.01 and later.

Using the CLI

wireless-rate-limit

Limits the number of wireless broadcast or multicast frames received by the access point per second.

Syntax

wireless-rate-limit broadcast *<frame-type>*

wireless-rate-limit multicast *<frame-type>*

no wireless-rate-limit broadcast

no wireless-rate-limit multicast

<frame-type> can be one of the following:

- aggressive - Allows up to 10 frames per second
- normal - Allows up to 25 frames per second
- conservative - Allows up to 50 frames per second

Default Setting

There is no default frame type when you issue this command. However, normal frame type is displayed for wireless broadcast or multicast multicast rate limit in a **show system** command if the command has not been configured, for example when the access point is set to factory defaults.

Command Mode

Global Configuration

Command Usage

- Configure separate rate limiting for wireless broadcast and wireless multicast frames.
- Use **wireless-rate-limit broadcast** *<frame-type>* to enable wireless rate limiting for broadcast traffic an IronPoint access point. Use **no wireless-rate-limit broadcast** to disable it.
- Use **wireless-rate-limit multicast** *<frame-type>* to enable wireless rate limiting for multicast traffic an IronPoint access point. Use **no wireless-rate-limit multicast** to disable it.
- You must enter a frame type when you issue this command; otherwise, the command will fail.
- Use the **show system** command to determine the current setting of the wireless-rate-limit commands. (See “show system” on page 24-1.)
- The access point generates a Syslog message if it receives more wireless broadcast or wireless multicast frames than what is configured for wireless-rate-limit. (See “General System” on page B-1.)

Example

```
Foundry AP(config)#wireless-rate-limit broadcast aggressive
Foundry AP(config)#wireless-rate-limit multicast normal
```


Chapter 7

Flash and File Commands

The commands in this section are used to manage files in the access point's flash.

Using the CLI

copy

This command copies a boot file, code image, or configuration file between the access point's flash memory and a FTP/TFTP server. When you save the configuration settings to a file on a FTP/TFTP server, that file can later be downloaded to the access point to restore system operation. Configuration files can be saved in a binary or readable XML format. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Syntax

copy <ftp | tftp> file

copy config <ftp | tftp>

- **ftp** - Keyword that allows you to copy to/from an FTP server.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **file** - Keyword that allows you to copy to/from a flash memory file.
- **config** - Keyword that allows you to upload the configuration file from flash memory.

Default Setting

None

Command Mode

Exec

Command Usage

- The system prompts for data required to complete the copy command.
- Only a configuration file can be uploaded to an FTP/TFTP server, but every type of file can be downloaded to the access point.
- A path on the server can be specified using "/" in the destination file name, providing the path already exists. Other than to indicate a path, the file name must not contain any slashes (\ or /), the leading letter cannot be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters or 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the access point supports only two operation code files.

- The download system configuration file must be named “syscfg” for binary format copy commands. For XML format configurations files, the name must end in a “.xml” extension, for example “syscfg.xml.”

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Foundry AP#copy config tftp
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
Foundry AP#
```

The following example shows how to download a configuration file:

```
Foundry AP#copy tftp file
1. Application Image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:2
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
Foundry AP#
```

The following example shows how to upgrade the application image:

```
Foundry AP#copy tftp file
1. Application Image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:1
TFTP Source file name: IPFR02202.bin
TFTP Server IP: 192.168.1.19
Current firmware version is 02.02.01Tv9. Copying new firmware version Run-Time
code v02.02.02. Please wait ...
Firmware copy complete. Reboot access point to complete firmware upgrade.
Foundry AP#reset board
```

The following example shows how to upgrade the boot code:

```

Foundry AP#copy tftp file
1. Application Image
2. Config file
3. Boot block image
TFTP Source file name: bootrom0400.bin
TFTP Server IP: 192.168.1.19
Select the type of download<1,2,3>: [1]:3
Updating Boot code v01.00.04 NOW!
Warning: You need to reboot the AP for the new boot image to take effect.
Do you want to reset the AP now? <y/n> [n]:y
Foundry AP#

```

dir

This command displays a list of files in flash memory.

Command Mode

Exec

Command Usage

File information is shown below:

Column Heading	Description
File Name	The name of the file.
Type	(2) Operation Code and (5) Configuration file
File Size	The length of the file in bytes.

Example

```

Foundry AP#dir
      File Name              Type File Size
      -----
      dflt-img.bin           2    1905806
      foundry-img.bin        2    1881274
      syscfg                  5      22624
      syscfg_bak              5      22624

                        3407872 byte(s) available

Foundry AP#

```

bootfile

This command specifies the image used to start up the system.

Syntax

bootfile <filename>

filename - Name of the image file.

Default Setting

None

Command Mode

Exec

Command Usage

- The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- If the file contains an error, it cannot be set as the default file.

Example

```
Foundry AP#foundry-img.bin
Foundry AP#
```

show bootfile

This command displays the name of the current operation code file that booted the system.

Command Mode

Exec

Example

```
Foundry AP#show bootfile

Bootfile Information
=====
Bootfile : foundry-img.bin
=====
Foundry AP#
```

delete

This command deletes a file or image.

Syntax

delete <*filename*>

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Exec

Caution: Beware of deleting application images from flash memory. At least one application image is required in order to boot the access point. If there are multiple image files in flash memory, and the

one used to boot the access point is deleted, be sure you first use the **bootfile** command to update the application image file booted at startup before you reboot the access point.

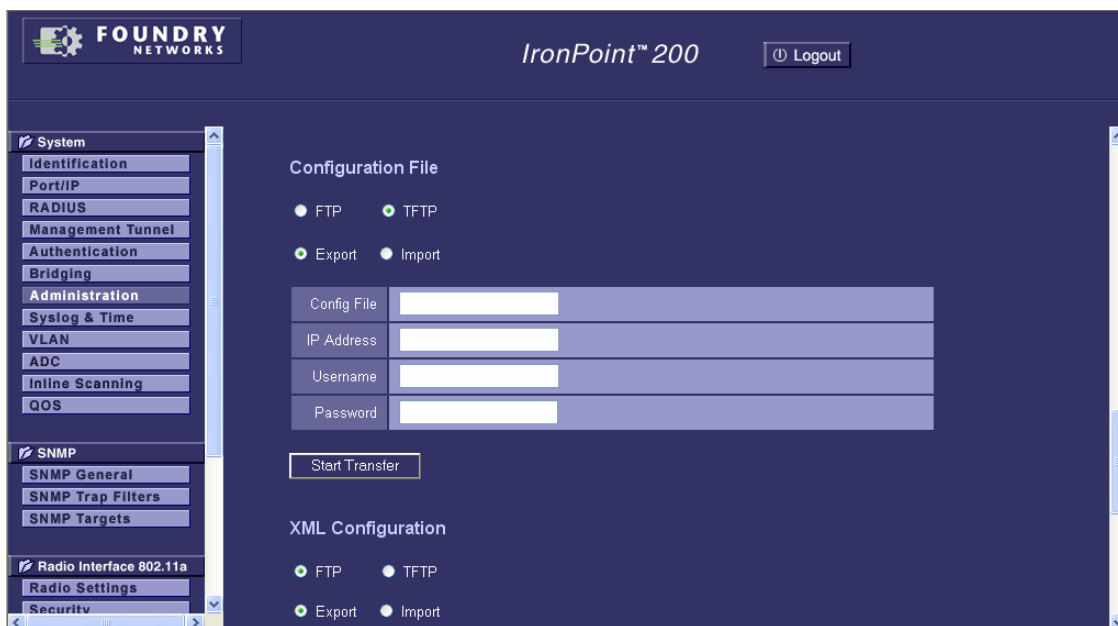
Example

This example shows how to delete the test.cfg configuration file from flash memory.

```
Foundry AP#delete test.cfg
Are you sure you wish to delete this file? <y/n>:
Foundry AP#
```

Using the Web Management Interface

From the System menu, click Administration. Scroll down to the Configuration File section.



Configurable Parameters

Configuration File – Uploads the current access point configuration file to a specified remote FTP or TFTP server. Downloads a configuration file from an FTP or TFTP server to restore a specific configuration. After filling in the following fields, click Start Transfer to proceed.

- **FTP/TFTP:** Selects either an FTP or TFTP server.
- **Export/Import:** Selects either an upload or download operation for the configuration file.

Note: If the country code on your access point is set to “99” and you export its configuration file, you will not be able to import that file back into the access point. Therefore, make sure the access point is configured with a country code other than “99”.

- **Config file:** Specifies the name of the configuration file on the server. A path on the server can be specified using “/” in the name, providing the path already exists; for example, “myfolder/syscfg.” Other than to indicate a path, the file name must not contain any slashes (\ or /), the leading letter cannot be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **IP Address:** IP address or host name of FTP or TFTP server.
- **Username:** The user ID used for login on an FTP server.
- **Password:** The password used for login on an FTP server.

The screenshot displays the Foundry IronPoint 200 web interface. The top header includes the Foundry Networks logo, the product name "IronPoint™ 200", and a "Logout" button. A left-hand navigation menu lists various system settings categories such as System, Identification, Port/IP, RADIUS, Management Tunnel, Authentication, Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP, Radio Interface 802.11a, Radio Settings, and Security. The main content area is titled "Configuration File" and features two sections: "Configuration File" and "XML Configuration". Both sections have radio buttons for "FTP" and "TFTP", and "Export" and "Import" options. The "Configuration File" section includes input fields for "Config File", "IP Address", "Username", and "Password", followed by a "Start Transfer" button. The "XML Configuration" section also has radio buttons for "FTP" and "TFTP", and "Export" and "Import" options.

To upload or download a readable text XML configuration file, scroll down to the XML Configuration section.

The screenshot shows the Foundry Networks IronPoint 200 web interface. On the left is a navigation menu with categories like System, SNMP, Radio Interface 802.11a, and Security. The main content area is titled 'XML Configuration'. It has two rows of radio buttons: the first row has 'FTP' selected and 'TFTP' unselected; the second row has 'Export' selected and 'Import' unselected. Below these are four input fields: 'New XML Configuration File', 'IP Address', 'Username', and 'Password'. At the bottom of this section is a button labeled 'Export/Import XML Config'. Further down, there is a 'Restore Factory Settings' button and a 'Restore' button.

Configurable Parameters

XML Configuration – Uploads or downloads an access point XML configuration file to or from a specified remote FTP or TFTP server. Note the following limitations

After filling in the following fields, click Export/Import XML Config to proceed.

- **FTP/TFTP:** Selects either an FTP or TFTP server.
- **Export/Import:** Selects either an upload or download operation for the XML configuration file.
- **New XML Configuration File:** Specifies the name of the configuration file on the server. The configuration file name must end with the file extension “.xml,” such as “syscfg.xml.” A path on the server can be specified using “/” in the name, providing the path already exists; for example, “myfolder/syscfg.xml.” Other than to indicate a path, the file name must not contain any slashes (\ or /), the leading letter cannot be a period (.), and the maximum length for file names on the FTP/TFTP server is 255 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **IP Address:** IP address or host name of FTP or TFTP server.
- **Username:** The user ID used for login on an FTP server.
- **Password:** The password used for login on an FTP server.

Viewing and Editing XML Configuration files

If you upload an XML format configuration file to an FTP or TFTP server, the file can be viewed and edited in any XML editor application.

```
<?xml version="1.0" ?>
- <config xmlns="http://www.foundry.com/rnd">
- <system>
  <system-country>TW</system-country>
  <system-name>Foundry AP</system-name>
- <user>
  <username>admin</username>
  <password>*****</password>
  <privilege>admin</privilege>
</user>
</system>
- <network>
  <dhcp>false</dhcp>
  <address>192.168.1.2</address>
  <netmask>255.255.255.0</netmask>
  <gateway>192.168.1.254</gateway>
  <speed-duplex>auto</speed-duplex>
- <dns>
  <index>1</index>
  <address>0.0.0.0</address>
</dns>
- <dns>
  <index>2</index>
  <address>0.0.0.0</address>
</dns>
  <vlan-enable>false</vlan-enable>
  <vlan-id>1</vlan-id>
- <qos>
  <qos-mode>qos-none</qos-mode>
  <svp-enable>false</svp-enable>
</qos>
</network>
+ <service>
- <server>
```


Chapter 8

Configuring IP Settings

Note: If ADC is enabled on the access point, TCP/IP address and default gateway information is configured using one of the following:

- IronView Network Manager application to configure TCP/IP information on an ADC-enabled IronPoint 200. Refer to the *IronView Network Manager* User Guide.

This section presents how to configure TCP/IP information when ADC is disabled.

Configuring the IronPoint Access Point with an IP address expands your ability to manage the access point. A number of access point features depend on IP addressing to operate.

Note: You can use the Web browser interface to access IP addressing only if the access point already has an IP address that is reachable through your network.

By default, the access point uses the default IP address of 169.254.1.1. You can configure the access point to be automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server on your network. However, if you are not using a DHCP server to configure IP addressing, use the CLI to manually configure the initial IP values. (See “Configuring an Access Point when ADC is not Used” on page 2-2.) After you have network access to the access point, you can use the Web browser interface to modify the initial IP configuration, if needed.

Note: If the access point is configured to use DHCP and there is no DHCP server on your network, or DHCP fails, the access point will automatically start up with the default IP address of 169.254.1.1.

Using the CLI

From the CLI configuration mode, use the **interface ethernet** command to access interface configuration mode. Use the **ip dhcp** command to enable the DHCP client, or **no ip dhcp** to disable it. Specify the new IP address, subnet mask, and default gateway using the **ip address** command.

To specify DNS server addresses use the **dns server** command. Use the **show interface ethernet** command from the Exec mode to display the current IP settings.

```

Foundry AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
Foundry AP(if-ethernet)#no ip dhcp
Foundry AP(if-ethernet)#ip address 192.168.1.2 255.255.255.0 192.168.1.253
Foundry AP(if-ethernet)#dns primary-server 192.168.1.55
Foundry AP(if-ethernet)#dns secondary-server 10.1.0.55
Foundry AP(config)#end
Foundry AP#show interface ethernet
Ethernet Interface Information
=====
MAC Address           : 00-0C-DB-81-40-93
IP Address            : 192.168.1.2
Subnet Mask           : 255.255.255.0
Default Gateway       : 192.168.1.253
Primary DNS           : 192.168.1.55
Secondary DNS         : 0.0.0.0
Speed-duplex Actual   : 100Base-TX Full Duplex
Speed-duplex Configured : Auto
Admin status          : Up
Operational status    : Up
=====
Foundry AP#

```

ip address

This command sets the IP address for the (10/100Base-TX) Ethernet interface. Use the **no** form to restore the default IP address.

Syntax

ip address <ip-address> <netmask> <gateway>
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- *gateway* - IP address of the default gateway

Default Setting

IP address: 169.254.1.1
 Netmask: 255.255.0.0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- DHCP is enabled by default. To manually configure a new IP address, you must first disable the DHCP client with the **no ip dhcp** command.
- You must assign an IP address to this device to gain management access over the network or to connect the access point to existing IP subnets. You can manually configure a specific IP address using this command, or direct the device to obtain an address from a DHCP server

using the **ip dhcp** command. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.

ip dhcp

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip dhcp
no ip dhcp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must assign an IP address to this device to gain management access over the network or to connect the access point to existing IP subnets. You can manually configure a specific IP address using the **ip address** command, or direct the device to obtain an address from a DHCP server using this command.
- When you use this command, the access point will begin broadcasting DHCP client requests. The current IP address (i.e., default or manually configured address) will continue to be effective until a DHCP reply is received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (DHCP values can include the IP address, subnet mask, and default gateway.)

dns server

This command specifies the address for the primary or secondary domain name server to be used for name-to-address resolution.

Syntax

dns primary-server <server-address>
dns secondary-server <server-address>

- **primary-server** - Primary server used for name resolution.
- **secondary-server** - Secondary server used for name resolution.
- *server-address* - IP address of domain-name server.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

The primary and secondary name servers are queried in sequence.

Using the Web Management Interface

From the System menu, click Port/IP. Select DHCP Client Enable if you are using a DHCP server, or select DHCP Client Disable and then specify the IP settings in the appropriate text fields. Click Apply.

Configurable Parameters

DHCP Client Enable – Select this option to obtain the IP settings for the access point from a DHCP (Dynamic Host Configuration Protocol) server. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) address are dynamically assigned to the access point by the network DHCP server. (Default: Disable)

DHCP Client Disable – Select this option to manually configure a static address for the access point.

IP Address – The IP address of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 169.254.1.1)

Subnet Mask – The mask that identifies the host address bits used for routing to specific subnets. (Default: 255.255.0.0)

Default Gateway – The default gateway is the IP address of the router for the access point, which is used if the requested destination address is not on the local subnet. If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided. (Default: 169.254.1.254)

Primary and Secondary DNS Address: The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. If you have one or more DNS servers located on the local network, type the IP addresses in the text fields provided. Otherwise, leave the addresses as all zeros (0.0.0.0).

Chapter 9

Management Access Settings

Configuring User Names and Passwords

Management access to the Web and CLI interface on the access point is controlled through user names and passwords. Each user account has an associated access level; either Admin or Read-Only. A Read-Only user has only read access to the management interfaces. However, an Admin user has write access for all parameters governing the access point. The default Admin user name is “admin” with the password “admin.” Up to 32 user accounts can be configured; 16 Admin users and 16 Read-Only users.

To protect access to the management interface, you need to configure a new Admin user name and password as soon as possible. If a new Admin user name and password is not configured, then anyone having access to the access point may be able to compromise access point and network security. Once a new Admin user has been configured, the default “admin” user name can be deleted from the system.

You can also gain additional access security by using control filters (see “Bridging and Traffic Filter Settings” on page 18-1).

Note: Pressing the Reset button on the back of the access point for more than five seconds resets user accounts to the factory defaults. For this reason, it is recommended that you protect the access point from physical access by unauthorized persons.

Using the CLI

To configure a new user account for the access point, use the **user** command from the CLI configuration mode. To delete a user account, use the **no user** command. To display all current configured users, use the **show user** command from the Normal Exec level.

```
Foundry AP(config)#user bob foundry 0
Foundry AP(config)#user chris guest 5
Foundry AP(config)#no user admin
Foundry AP(config)#exit
Foundry AP#show user

-----
User Name: bob
Password : *****
Privilege: Admin

User Name: chris
Password : *****
Privilege: Read-Only
-----
Foundry AP#
```

user

This command configures the name of the user who has management access to the access point.

Syntax

```
user <name> <password> <privilege>
no user <name>
```

- *name* - The name of the user.
(Length: 1-64 characters, case sensitive)
- *password* - The password of the user.
(Length: 1-64 characters, case sensitive)
- *privilege* - The access level for the user account: 0 (Admin) or 5 (Read-Only).

Default Setting

Name: admin
Password: admin
Privilege: 0 (Admin)

Command Mode

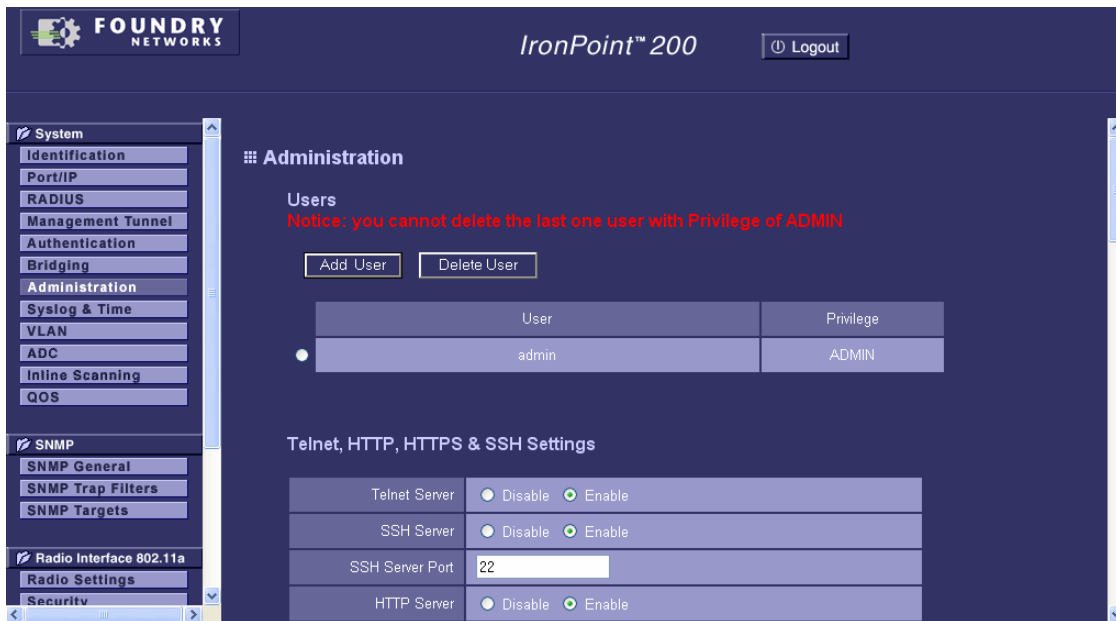
Global Configuration

Command Usage

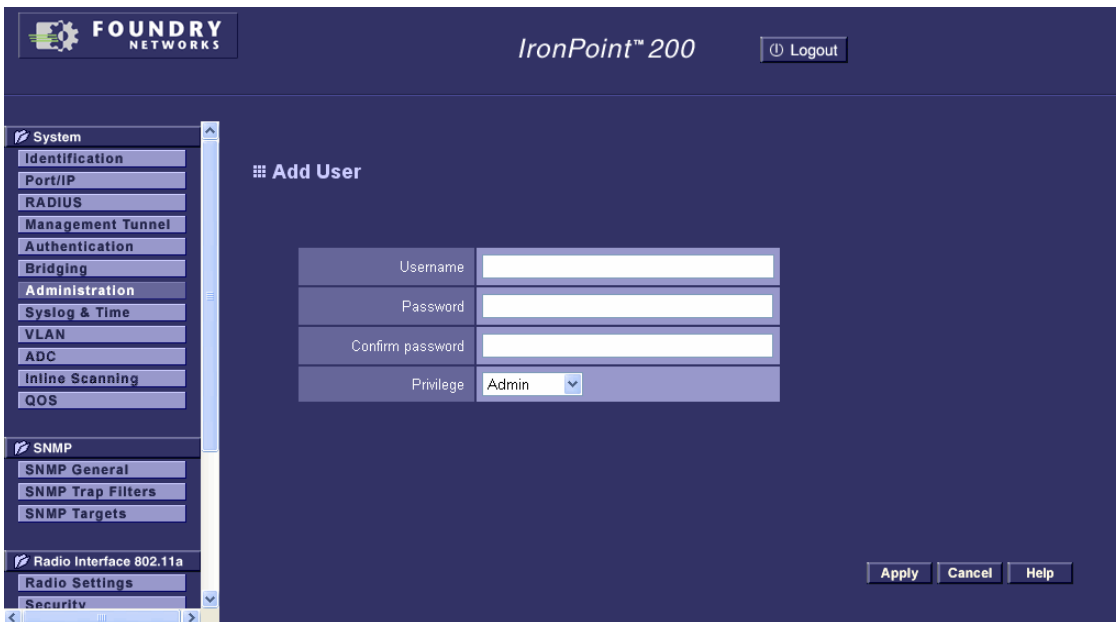
- Up to 32 user accounts can be configured; 16 Admin users and 16 Read-Only users.
- If there is only one Admin user account configured, it cannot be deleted. To delete the default “admin” user, first configure a new Admin user account before using the **no user** command to remove the “admin” user account.
- The password for an existing user cannot be changed without first deleting the account and then configuring it again with the new password.

Using the Web Management Interface

From the System menu, click Administration.



To configure a new user, click Add User, then set the user name and password, and select the access privilege level. Click Apply.



To remove a user, select the user name from the list and click Delete User.

Configurable Parameters

Add User – Adds a new user account for management access. A maximum of 32 users can be configured; 16 Admin users and 16 Read-Only users. (Default Username: admin; Default Password: admin)

- **Username:** The name of the user. (Length: 1-64 characters, case sensitive)
- **Password:** The password for the user. (Length: 1-64 characters, case sensitive)
- **Confirm Password:** Enter the password again for verification.
- **Privilege:** Select the access level for the user; Admin or Read-Only. An Admin user has read-write access for all management parameters. A Read-Only user has only read access to the management interfaces.

Delete User – Deletes the selected user from the Users list.

Telnet and SSH Settings

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, Telnet is not secure from hostile attacks. The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Note: The access point supports only SSH version 2.0.

Note: After boot up, the SSH server needs about two minutes to generate host encryption keys. The SSH server is disabled while the keys are being generated.

Using the CLI

To enable the Telnet and SSH servers, use the **ip telnet-server enable** or **ip ssh-server enable** commands from the CLI Ethernet interface configuration mode. To set the SSH server UDP port, use the **ip ssh-server port** command. To view the current settings, use the **show system** command from the CLI Exec mode (see “show system” on page 24-1.).

```
Foundry AP(if-ethernet)#ip telnet-server enable
Foundry AP(if-ethernet)#ip ssh-server enable
Foundry AP(if-ethernet)#ip ssh-server port 1124
Foundry AP#
```

ip ssh-server enable

This command enables the Secure Shell server. Use the **no** form to disable the server.

Syntax

ip ssh-server enable
no ip ssh-server

Default Setting

Interface enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The access point supports Secure Shell version 2.0 only.
- After boot up, the SSH server needs about two minutes to generate host encryption keys. The SSH server is disabled while the keys are being generated. The **show system** command displays the status of the SSH server.

ip ssh-server port

This command sets the Secure Shell server port. Use the **no** form to disable the server.

Syntax

ip ssh-server port <port-number>

- *port-number* - The UDP port used by the SSH server. (Range: 1-65535)

Default Setting

22

Command Mode

Interface Configuration (Ethernet)

ip telnet-server enable

This command enables the Telnet server. Use the **no** form to disable the server.

Syntax

ip telnet-server enable
no ip telnet-server

Default Setting

Interface enabled

Command Mode

Interface Configuration (Ethernet)

Using the Web Management Interface

From the System menu, click Administration. Enable or disable the Telnet and SSH servers and set the SSH server port as required. Click Apply.



Configurable Parameters

Telnet Server – Enables or disables the Telnet server. (Default: Enabled)

SSH Server – Enables or disables the SSH server. (Default: Enabled)

SSH Port Number – Sets the UDP port for the SSH server. (Range: 1-65535; Default: 22)

Configuring the Web Server

The access point allows the system Web server and secure Web server to be enabled or disabled, and the TCP port numbers to be set.

Using the CLI

Use the **ip http port** and the **ip https port** commands to set the Web server and secure Web server TCP ports. Use the **ip http server** and **ip https server** commands to enable the Web server and secure Web server.

```
Foundry AP(config)#ip http port 49154
Foundry AP(config)#ip http server
Foundry AP(config)#ip https port 49153
Foundry AP(config)#ip https server
Foundry AP(config)#
```

ip http port

This command specifies the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port <port-number>
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 80 or 1024-65535)

Default Setting

80

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- To avoid using common reserved TCP port numbers below 1024, the configurable range is restricted to between 1024 and 65535. However, the default port number is 80. To reset the default port number, use the **no ip http port** command, then enter the new HTTP port number.

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

ip https port

Use this command to specify the UDP port number used for HTTPS/SSL connection to the access point's Web interface. Use the **no** form to restore the default port.

Syntax

ip https port <port_number>
no ip https port

port_number – The UDP port used for HTTPS/SSL.
(Range: 443, 1024-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- To avoid using common reserved TCP port numbers below 1024, the configurable range is

restricted to 443 and between 1024 and 65535.

- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:
https://device:port_number

ip https server

Use this command to enable the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the access point's Web interface. Use the **no** form to disable this function.

Syntax

ip https server
no ip https server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently.
- If you enable HTTPS, you must indicate this in the URL:
https://device[port_number]
- When you start HTTPS, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
A padlock icon should appear in the status bar for Internet Explorer 6.x.
- IronPoint access point supports Internet Explorer version 6.0 and later, running on Windows platforms.

Using the Web Management Interface

From the System menu, click Administration. Enable or disable the HTTP and HTTPS Web servers and set the server port numbers as required. Click Apply.

Note: If you are using HTTP to configure the access point, your connection will be lost if you disable the HTTP server.

FOUNDRY NETWORKS *IronPoint™ 200* [Logout](#)

System

- Identification
- Port/IP
- RADIUS
- Management Tunnel
- Authentication
- Bridging
- Administration
- Syslog & Time
- VLAN
- ADC
- Inline Scanning
- QOS

SNMP

- SNMP General
- SNMP Trap Filters
- SNMP Targets

Radio Interface 802.11a

- Radio Settings
- Security

Telnet, HTTP, HTTPS & SSH Settings

Telnet Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SSH Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
SSH Server Port	<input type="text" value="22"/>
HTTP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
HTTP Server Port	<input type="text" value="80"/>
HTTP Secure Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
HTTP Secure Server Port	<input type="text" value="443"/>

Firmware Upgrade

Current version	02.02.00b10
-----------------	-------------

Local

Configurable Parameters

HTTP Server – Enables or disables management access through a Web browser interface. (Default: Enabled)

HTTP Server Port – Specifies the TCP port number used by the Web browser interface. (Range: 80 or 1024-65535; Default: 80)

HTTP Secure Server – Enables or disables management access through a secure Web browser interface. (Default: Enabled)

HTTP Secure Server Port – Specifies the TCP port number used by the secure Web browser interface. (Range: 443 or 1024-65535; Default: 443)

Using ACLs to Control Management Access

You can control management access to the access points by creating ACL policies to permit or deny access via Telnet, SSH, HTTP, HTTPS, or SNMP. The ACL policies permit or deny traffic from a specific IP address. You assign these policies to access groups for Telnet, SSH, Web access, and SNMP.

```

Foundry AP(config)#access-list 1
Foundry AP(access-list 1)#permit ip address 20.1.2.3 255.255.255.255
Foundry AP(access-list 1)#permit ip address 20.1.3.3 255.255.255.255
Foundry AP(access-list 1)#deny ip address 20.1.1.3 255.255.255.255
Foundry AP(access-list 1)#deny ip address 20.1.4.3 255.255.255.255
Foundry AP(access-list 1)#permit any
Foundry AP(access-list 1)#exit

Foundry AP#show access-list 1
access-list 1 (total number of entries:5)
=====
permit ip address 20.1.2.3 255.255.255.255
permit ip address 20.1.3.3 255.255.255.255
deny ip address 20.1.1.3 255.255.255.255
deny ip address 20.1.4.3 255.255.255.255
permit any
=====
Foundry AP(config)#access-list 1
Foundry AP(access-list 1)#no deny ip address 20.1.4.3 255.255.255.255
Foundry AP(access-list 1)#exit

Foundry AP#show access-list 1
access-list 1 (total number of entries:4)
=====
permit ip address 20.1.2.3 255.255.255.255
permit ip address 20.1.3.3 255.255.255.255
deny ip address 20.1.1.3 255.255.255.255
permit any
=====

Foundry AP#configure
Foundry AP(config)#telnet access-group 1
Foundry AP(config)#ssh access-group 1
Foundry AP(config)#web access-group 1
Foundry AP(config)#snmp-server access-group 1
Foundry AP(config)#end
Foundry AP#show filter
Protocol Filter Information
=====
Local Bridge          :DISABLED
AP Management         :ENABLED
Management: (Ethernet Port):ENABLED
                      ssh access-group 1
                      telnet access-group 1
                      web access-group 1
                      snmp-server access-group 1
Ethernet Type Filter  :DISABLED

Enabled Protocol Filters
-----
No protocol filters are enabled
=====

```

access-list

This command creates an ACL policy.

Syntax

access-list *<access-list-id>*

<access-list-id> – Enter a number for the ACL ID.
(Range: 1 - 10)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can configure up to 10 ACLs in an access point. Each ACL can have up to 10 entries.

The **access-list** command takes you to the ACL configuration level, where you can enter or delete permit and deny entries.

delete

description

Syntax

delete

Deletes all permit and deny statements from an ACL.

Default Setting

None.

Command Mode

ACL Configuration

deny

Disallows access to the access point from the specified IP address or from all IP addresses.

Syntax

deny *<ip-address>* *<subnet-mask>* | **any**
[no] deny *<ip-address>* *<subnet-mask>* | **any**

- **any** - Traffic from any IP address will be disallowed to access the access point.
- *<ip-address>* *<subnet-mask>* - Enter an IP address and subnet mask
- **no** - deletes a specific deny statement

Default Setting

None.

Command Mode

ACL Configuration

Command Usage

Use **any** to disallow management access to the access point from any IP address.

Enter an IP address and its subnet mask if you want to disallow access only from a specified IP address.

To remove a specific deny statement, you must enter **no** followed by the entire deny statement.

permit

Allows access to the access point from the specified IP address or from all IP addresses.

Syntax

```
permit <ip-address> <subnet-mask> | any  
[no] permit <ip-address> <subnet-mask> | any
```

- **any** - Traffic from any IP address will be allowed to access the access point.
- **<ip-address> <subnet-mask>** - Enter an IP address and subnet mask
- **no** - deletes a specific permit statement

Default Setting

None.

Command Mode

ACL Configuration

Command Usage

Use **any** to allow management access to the access point from any IP address.

To control management access, enter an IP address and its subnet mask. The access point allows management access only from the specified IP address.

To remove a specific permit statement, you must enter **no** followed by the entire deny statement.

show access-list all

Displays the ACLs configured on the access point.

Syntax

```
show access-list all | <access-list-id>
```

- Use **all** to display the entries in all ACLs configured on the access point.
- Enter an **<access-list-id>** to display a specific ACL's entries.

Default Setting

None.

Command Mode

Exec

snmp-server access-group

Applies an ACL to an access group to restrict management access to the access point via an SNMP server.

```
ssh access-group <access-list-id>  
no ssh access-group <access-list-id>
```

- Enter an ACL ID for **<access-list-id>**
- Use the **no** form of the command to delete the restriction on access from an SNMP server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Enter this command to restrict management access to the access point from an SNMP server (UDP Port 161).

ssh access-group

Applies an ACL to an access group to restrict management access to the access point via SSH.

ssh access-group *<access-list-id>*

no ssh access-group *<access-list-id>*

- Enter an ACL ID for *<access-list-id>*
- Use the **no** form of the command to delete the restriction on SSH access.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Enter this command to restrict management access to the access point via SSH. Use the **ip ssh-server** command, to enable an SSH server and to specify an SSH Server Port, if you do not want to use TCP Port 22, the default port, for SSH server.

telnet access-group

Applies an ACL to an access group to restrict management access to the access point via Telnet.

telnet access-group *<access-list-id>*

no telnet access-group *<access-list-id>*

- Enter an ACL ID for *<access-list-id>*
- Use the **no** form of the command to delete the restriction on Telnet access.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Enter this command to restrict management access to the access point via Telnet (TCP Port 23).

web access-group

Applies an ACL to an access group to restrict management access to the access point via HTTP and HTTPS.

web access-group *<access-list-id>*

no web access-group *<access-list-id>*

- Enter an ACL ID for *<access-list-id>*
- Use the **no** form of the command to delete the restriction on access using HTTP and HTTPS.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Enter this command to restrict management access to the access point via HTTP and HTTPS. Use the **ip http port** command to specify a port for HTTP, if you do not want to use TCP Port 80, the default port for HTTP. Likewise, use the **ip https port** command to specify a port for HTTPS, if you do not want to use TCP Port 443, the default port for HTTPS.

show filters

This command shows the filter options and protocol entries in the filter table, including the ACL filters that have been configured.

Syntax

show filters

Command Mode

Exec

Configuring Banners

Banners allow you to display messages when a user accesses a device using Telnet or Secure Shell (SSH).

Using the CLI**EXAMPLE:**

For example, you can configure a message that is displayed on the console and one that is displayed on the Telnet or SSH window.

```
Foundry AP(config)#banner incoming There is an Incoming Banner
Foundry AP(config)#banner motd Have a Great Holiday!
```

When an administrator access the access point using Telnet or SSH, the message created using the **banner incoming** command is displayed on the console as:

```
Telnet connected from 192.168.20.113
There is an Incoming Banner

or
```

```
SSH connected from 192.168.20.113
This is an Incoming Banner
```

The message created using the **banner motd** command is displayed on the Telnet or SSH window as:

```
Have a Great Holiday!
```

banner incoming

This command allows you to configure an incoming message which is displayed on the console when a user logs into the access point using Telnet or SSH.

Syntax

banner incoming <message>

[no] banner incoming

Default Setting

no banner

Command Mode

Global Configuration

Command Usage

Enter up to 255 characters for this message.

banner motd

This command allows you to enter a message of the day (motd), which is displayed on the Telnet or SSH window when a user logs into the access point using Telnet or SSH.

Syntax

banner motd <message>

[no] banner motd

Default Setting

none

Command Mode

Global Configuration.

Command Usage

Enter up to 255 characters for a message of the day.

Chapter 10

SNMP Configuration

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The access point includes an on-board agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the access point, as well as the traffic passing to and from wireless clients. A network management station can access this information using SNMP management software that is compliant with MIB II. To implement SNMP management, the access point must first have an IP address and subnet mask, configured either manually or dynamically. Access to the on-board agent using SNMP v1 and v2c is controlled by community strings. To communicate with the access point, the management station must first submit a valid community string for authentication.

Access to the access point using SNMP v3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling notifications that are sent to specified user targets.

Enabling SNMP and Setting v1 and v2c Parameters

The access point SNMP agent must be enabled for all versions (1, 2c, and 3) to function. Management access using SNMP v1 and v2c also requires community strings to be configured for authentication. Trap notifications can be enabled and sent to up to four management stations.

Using the CLI

To enable SNMP on the access point, use the **snmp-server enable server** command from the CLI configuration mode. To set read/write and read-only community names, use the **snmp-server community** command. Use the **snmp-server location** and **snmp-server contact** commands to indicate the physical location of the access point and define a system contact. The **snmp-server**

host command defines trap receiver hosts. To view the current SNMP settings, use the **show snmp** command.

```
Foundry AP(config)#snmp-server enable server
Foundry AP(config)#snmp-server community alpha rw
Foundry AP(config)#snmp-server community beta ro
Foundry AP(config)#snmp-server location WC-19
Foundry AP(config)#snmp-server contact Paul
Foundry AP(config)#snmp-server host 1 192.168.1.9 alpha
Foundry AP(config)#snmp-server trap dot11StationAssociation
Foundry AP(config)#exit
Foundry AP#show snmp

SNMP Information
=====
Service State           : Enable
Community (ro)          : *****
Community (rw)          : *****
Location                 : WC-19
Contact                  : Paul

EngineId      :80:00:07:e5:80:00:00:2e:62:00:00:00:18
EngineBoots:1

Trap Destinations:
1:      192.168.1.9, Community: *****, State: Enabled
2:      0.0.0.0, Community: *****, State: Disabled
3:      0.0.0.0, Community: *****, State: Disabled
4:      0.0.0.0, Community: *****, State: Disabled

dot11InterfaceAGFail Enabled      dot11InterfaceBFail Enabled
dot11StationAssociation Enabled    dot11StationAuthentication Enabled
dot11StationReAssociation Enabled  dot11StationRequestFail Enabled
dot1xAuthFail Enabled             dot1xAuthNotInitiated Enabled
dot1xAuthSuccess Enabled          dot1xMacAddrAuthFail Enabled
dot1xMacAddrAuthSuccess Enabled   iappContextDataSent Enabled
iappStationRoamedFrom Enabled     iappStationRoamedTo Enabled
localMacAddrAuthFail Enabled      localMacAddrAuthSuccess Enabled
pppLogonFail Enabled             snmpServerFail Enabled
configFileVersionChanged Enabled  radiusServerChanged Enabled
systemDown Enabled               systemUp Enabled
micFailure Enabled               tkipSequenceError Enabled

=====
Foundry AP#
```

snmp-server enable server

This command enables SNMP management access and also enables this device to send SNMP traps (i.e., notifications). Use the **no** form to disable SNMP service and trap messages.

Syntax

snmp-server enable server

no snmp-server enable server

Default Setting

None

Command Mode

Global Configuration

Command Usage

- This command enables all notifications.
- The **snmp-server host** command specifies host devices that will receive SNMP notifications.
- The **snmp-server trap** command enables specific SNMP notifications.

snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community <string> [ro | rw]

no snmp-server community <string>

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 23 characters, case sensitive)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

If you enable SNMP management but do not configure a community string, the following default community strings are available:

- **public** - for read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - for read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

If you enter a community string without the **ro** or **rw** option, the default is **rw** (read/write).

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*

no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact <string>
no snmp-server contact

string - String that describes the system contact. (Maximum length: 255 characters)

Default Setting

Contact

Command Mode

Global Configuration

snmp-server host

This command specifies the recipient of an SNMP notification. Use the **no** form to remove the specified host.

Syntax

snmp-server host <1 | 2 | 3 | 4> <host_ip_address | host_name> <community-string>
no snmp-server host

- **1** - First SNMP host.
- **2** - Second SNMP host.
- **3** - Third SNMP host.
- **4** - Fourth SNMP host.
- *host_ip_address* - IP of the host (the targeted recipient).
- *host_name* - Name of the host. (Range: 1-255 characters)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 23 characters)

Default Setting

Host Address: None
 Community String: public

Command Mode

Global Configuration

Command Usage

The **snmp-server host** command is used in conjunction with the **snmp-server enable server** command to enable SNMP notifications.

snmp-server trap

This command enables the access point to send specific SNMP traps (i.e., notifications). Use the **no** form to disable specific trap messages.

Syntax

snmp-server trap <trap>
no snmp-server trap <trap>

- *trap* - One of the following SNMP trap messages:
 - **dot11InterfaceAGFail** - The 802.11a or 802.11g interface has failed.
 - **dot11InterfaceBFail** - The 802.11b interface has failed.
 - **dot11StationAssociation** - A client station has successfully associated with the access point.
 - **dot11StationAuthentication** - A client station has been successfully authenticated.
 - **dot11StationReAssociation** - A client station has successfully re-associated with the access point.
 - **dot11StationRequestFail** - A client station has failed association, re-association, or authentication.
 - **dot1xAuthFail** - A 802.1x client station has failed RADIUS authentication.
 - **dot1xAuthNotInitiated** - A client station did not initiate 802.1x authentication.
 - **dot1xAuthSuccess** - A 802.1x client station has been successfully authenticated by the RADIUS server.
 - **dot1xMacAddrAuthFail** - A client station has failed MAC address authentication with the RADIUS server.
 - **dot1xMacAddrAuthSuccess** - A client station has successfully authenticated its MAC address with the RADIUS server.
 - **dot1xSupplicantAuthenticated** - The access point has been successfully authenticated with the RADIUS server.
 - **iappContextDataSent** - A client station's Context Data has been sent to another access point with which the station has associated.
 - **iappStationRoamedFrom** - A client station has roamed from another access point (identified by its IP address).
 - **iappStationRoamedTo** - A client station has roamed to another access point (identified by its IP address).
 - **localMacAddrAuthFail** - A client station has failed authentication with the local MAC address database on the access point.
 - **localMacAddrAuthSuccess** - A client station has successfully authenticated its MAC address with the local database on the access point.
 - **micFailure** - The TKIP message integrity check has detected an error.
 - **pppLogonFail** - The access point has failed to log onto the PPPoE server using the configured user name and password.
 - **sntpServerFail** - The access point has failed to set the time from the configured SNTP server.
 - **sysConfigFileVersionChanged** - The access point's configuration file has been changed.
 - **sysRadiusServerChanged** - The access point has changed from the primary RADIUS server to the secondary, or from the secondary to the primary.
 - **sysSystemDown** - The access point is about to shutdown and reboot.

- **sysSystemUp** - The access point is up and running.
- **tkipSequenceError** - The access point has detected replay attack.
- **wirelessExternalAntenna** - An external antenna has been attached or detached from the access point.

Default Setting

All traps enabled

Command Mode

Global Configuration

Command Usage

This command is used in conjunction with the **snmp-server host** and **snmp-server enable server** commands to enable SNMP notifications.

show snmp

This command displays the SNMP configuration settings.

Syntax

show snmp

Command Mode

Exec

Using the Web Management Interface

From the SNMP menu, click SNMP General. To configure the access point to support SNMP management, set SNMP to Enable, specify community names, and configure up to four host IP addresses to send trap messages to management stations. Click Apply.

The screenshot shows the Foundry Networks IronPoint 200 web management interface. The left sidebar contains a navigation menu with categories: System, SNMP, Radio Interface 802.11a, and Security. The main content area is titled "SNMP" and features a toggle switch for "SNMP" set to "Enable". Below this, there are configuration fields for two trap destinations. The first trap destination is configured with "Location", "Contact", "Community Name (Read Only)", "Community Name (Read/Write)", "Trap Destination 1" (set to "Enable"), "Trap Destination IP Address" (set to "100.0.0.201"), and "Trap Destination Community Name". The second trap destination is configured with "Trap Destination 2" (set to "Disable"), "Trap Destination IP Address" (set to "0.0.0.0"), and "Trap Destination Community Name".

Configurable Parameters

Status – Enables or disables SNMP management access and also enables the access point to send SNMP traps (notifications). (Default: Enabled)

Location – A text string that describes the system location. (Maximum length: 255 characters)

Contact – A text string that describes the system contact. (Maximum length: 255 characters)

Community Name (Read Only) – Defines the SNMP community access string that has read-only access. Authorized management stations are only able to retrieve MIB objects. (Maximum length: 23 characters, case sensitive; Default: Public)

Community Name (Read/Write) – Defines the SNMP community access string that has read/write access. Authorized management stations are able to both retrieve and modify MIB objects. (Maximum length: 23 characters, case sensitive; Default: Private)

Trap Destination IP Address (1 to 4) – Specifies recipients (up to four) of SNMP notifications. Enter the IP address or the host name. (Host Name: 1 to 255 characters)

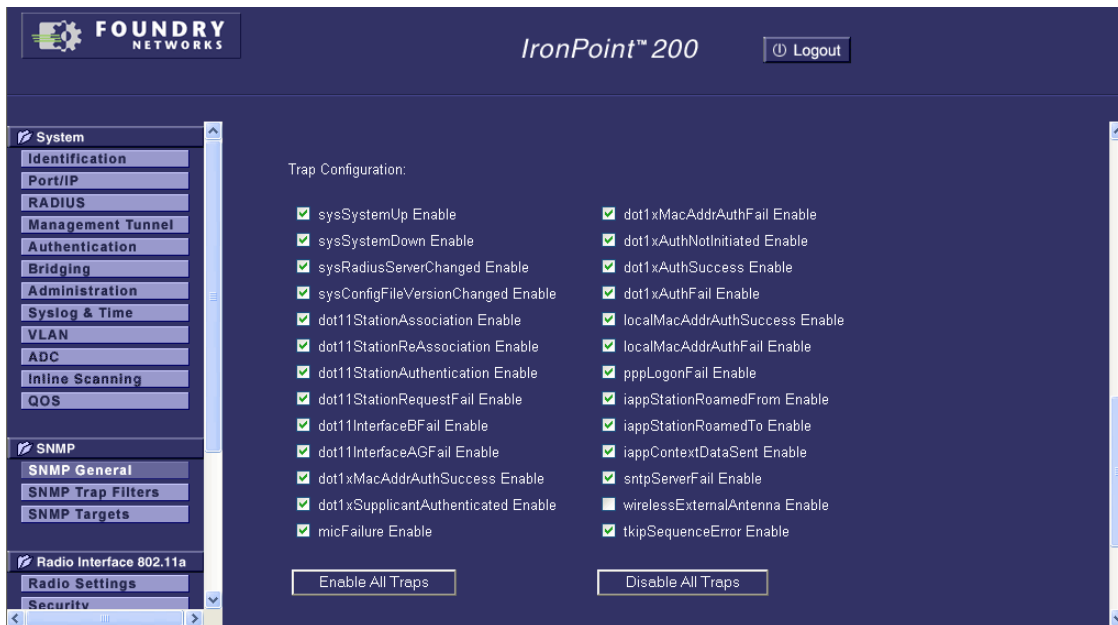
Trap Destination Community Name – The community string sent with the notification operation. (Maximum length: 23 characters; Default: Public)

Trap Configuration – Allows selection of specific SNMP notifications to send. The following are available:

- **sysSystemDown** - The access point is about to shutdown and reboot.
- **sysSystemUp** - The access point is up and running.
- **sysRadiusServerChanged** - The access point has changed from the primary RADIUS server to the secondary, or from the secondary to the primary.
- **sysConfigFileVersionChanged** - The access point's configuration file has been changed.
- **dot11StationAssociation** - A client station has successfully associated with the access point.
- **dot11StationReAssociation** - A client station has successfully re-associated with the access point.
- **dot11StationAuthentication** - A client station has been successfully authenticated.
- **dot11StationRequestFail** - A client station has failed association, re-association, or authentication.
- **dot11InterfaceBFail** - The 802.11b interface has failed.
- **dot11InterfaceAGFail** - The 802.11a or 802.11g interface has failed.
- **dot1xMacAddrAuthSuccess** - A client station has successfully authenticated its MAC address with the RADIUS server.
- **dot1xSupplicantAuthenticated** - The access point has been successfully authenticated with the RADIUS server.
- **dot1xMacAddrAuthFail** - A client station has failed MAC address authentication with the RADIUS server.

- **dot1xAuthNotInitiated** - A client station did not initiate 802.1x authentication.
- **dot1xAuthSuccess** - A 802.1x client station has been successfully authenticated by the RADIUS server.
- **dot1xAuthFail** - A 802.1x client station has failed RADIUS authentication.
- **localMacAddrAuthSuccess** - A client station has successfully authenticated its MAC address with the local database on the access point.
- **localMacAddrAuthFail** - A client station has failed authentication with the local MAC address database on the access point.
- **pppLogonFail** - The access point has failed to log onto the PPPoE server using the configured user name and password.
- **iappStationRoamedFrom** - A client station has roamed from another access point (identified by its IP address).
- **iappStationRoamedTo** - A client station has roamed to another access point (identified by its IP address).
- **iappContextDataSent** - A client station's Context Data has been sent to another access point with which the station has associated.
- **sntpServerFail** - The access point has failed to set the time from the configured SNTP server.
- **wirelessExternalAntenna** - An external antenna has been attached or detached from the access point.
- **micFailure** - The TKIP message integrity check has detected an error.
- **tkipSequenceError** - The access point has detected replay attack.

To configure the access point to send specific trap messages, select the traps from the list or use the Enable All Traps button. Click Apply.



Configuring SNMPv3 Users

The access point CLI also enables up to 10 SNMP v3 users to be assigned to one of three pre-defined groups. The **show snmp groups** command displays the group names (RO, RWAuth, or RWPriv) and the group security settings.

There is no Web Management Interface equivalent for configuring SNMPv3 users.

Note: Users must be assigned to groups that have the same security levels. If a user who has “AuthPriv” security (uses authentication and encryption) is assigned to a read-only (RO) group, the user will not be able to access the database. An AuthPriv user must be assigned to the RWPriv group with the AuthPriv security level.

Using the CLI

Use the **snmp-server engine-id** command to define the SNMP v3 engine before assigning users to groups. Use the **snmp-server user** command to assign users to one of the three groups and set the appropriate authentication and encryption types to be used. To view the current SNMP v3 engine ID,

use the **show snmp** command. To view SNMP users and group settings, use the **show snmp users** or **show snmp group-assignments** commands.

```

Foundry AP#show snmp groups

GroupName      :RO
SecurityModel  :USM
SecurityLevel  :NoAuthNoPriv

GroupName      :RWAuth
SecurityModel  :USM
SecurityLevel  :AuthNoPriv

GroupName      :RWPriv
SecurityModel  :USM
SecurityLevel  :AuthPriv
Foundry AP#configure
Foundry AP(config)#snmp-server engine-id 1a:2b:3c:4d:00:ff
Foundry AP(config)#snmp-server user chris RWPriv auth-protocol md5 auth-passphrase
a-good-pw priv-protocol des priv-passphrase a-v-good-pw
Foundry AP(config)#exit
Foundry AP#show snmp users

=====
UserName       :chris
GroupName      :RWPriv
AuthType       :MD5
    Passphrase:*****
PrivType       :DES
    Passphrase:*****
=====
Foundry AP#show snmp group-assignments

GroupName      :RWPriv
UserName       :chris
Foundry AP#

```

snmp-server engine-id

This command is used for SNMP v3. It is used to uniquely identify the access point among all access points in the network. Use the **no** form to delete the engine ID.

Syntax

snmp-server engine-id <engine-id>
no snmp-server engine-id

engine-id - Enter engine-id in hexadecimal (5 -32 characters).

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- This command is used in conjunction with the **snmp-server user** command.
- Entering this command invalidates all engine IDs that have been previously configured.
- If the engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users

snmp-server user

This command configures the SNMP v3 users that are allowed to manage the access point. Use the **no** form to delete an SNMP v3 user.

Syntax

```
snmp-server user <user-name> <group-name> [auth-proto {md5}] [auth-passphrase  
{<passphrase>}] [priv-proto {des}] [priv-passphrase {<passphrase>}]  
no snmp-server user <user-name>
```

- *user-name* - A user-defined string for the SNMP user. (32 characters maximum)
- *group-name* - The name of the SNMP group to which the user is assigned (32 characters maximum). There are three pre-defined groups: RO, RWAuth, or RWPriv.
- **auth-proto** - The authentication type used for user authentication: **md5** or none.
- **auth-passphrase** - The user password required when authentication is used (8 – 32 characters).
- **priv-proto** - The encryption type used for SNMP data encryption: **des** or none.
- **priv-passphrase** - The user password required when data encryption is used (8 – 32 characters).

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Up to 10 SNMPv3 users can be configured on the access point.
- The SNMP engine ID is used to compute the authentication/privacy digests from the pass phrase. You should therefore configure the engine ID with the **snmp-server engine-id** command before using this configuration command.
- The access point enables SNMP v3 users to be assigned to three pre-defined groups. Other groups cannot be defined. The available groups are:
 - RO - A read-only group using no authentication and no data encryption. Users in this group use no security, either authentication or encryption, in SNMP messages they send to the agent. This is the same as SNMP v1 or SNMP v2c.
 - RWAuth - A read/write group using authentication, but no data encryption. Users in this group send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.
 - RWPriv - A read/write group using authentication and data encryption. Users in this group send SNMP messages that use an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/passwords must be defined.
- Users must be assigned to groups that have the same security levels. If a user who has "AuthPriv" security (uses authentication and encryption) is assigned to a read-only (RO) group,

the user will not be able to access the database. An AuthPriv user must be assigned to the RWPriv group with the AuthPriv security level.

- To configure a user for the RWAAuth group, you must include the **auth-proto** and **auth-passphrase** keywords.
- To configure a user for the RWPriv group, you must include the **auth-proto**, **auth-passphrase**, **priv-proto**, and **priv-passphrase** keywords.

show snmp groups

This command displays the SNMP v3 pre-defined groups.

Syntax

show snmp groups

Command Mode

Exec

show snmp users

This command displays the SNMP v3 users and settings.

Syntax

show snmp users

Command Mode

Exec

show snmp group-assignments

This command displays the SNMP v3 user group assignments.

Syntax

show snmp group-assignments

Command Mode

Exec

Configuring SNMPv3 Trap Filters

SNMP v3 users can be configured to receive notification messages from the access point. An SNMP Target ID is created that specifies the SNMP v3 user, IP address, and UDP port. A user-defined notification filter can be created so that specific notifications can be prevented from being sent to particular targets.

The access point allows up to 10 notification filters to be created. Each filter can be defined by up to 20 MIB subtree ID entries.

Using the CLI

To create a notification filter, use the **snmp-server filter** command from the CLI configuration mode. Use the command more than once with the same filter ID to build a filter that includes or excludes

multiple MIB objects. To view the current SNMP filters, use the **show snmp filter** command from the CLI Exec mode.

```

Foundry AP(config)#snmp-server filter trapfilter include .1.3.6.1.2.1.2.2.1
Foundry AP(config)#snmp-server filter trapfilter exclude .1.3.6.1.2.1.2.2.1.1.23
Foundry AP(config)#exit
Foundry AP#show snmp filter

Filter: trapfilter
  Type: include
  Subtree: iso.3.6.1.2.1.2.2.1

  Type: exclude
  Subtree: iso.3.6.1.2.1.2.2.1.1.23
=====
Foundry AP#

```

snmp-server filter

This command configures SNMP v3 notification filters. Use the **no** form to delete an SNMP v3 filter or remove a subtree from a filter.

Syntax

snmp-server filter <filter-id> <include | exclude> <subtree> [mask {mask}]
no snmp-server filter <filter-id> [subtree]

- *filter-id* - A user-defined name that identifies an SNMP v3 notification filter. (Maximum length: 32 characters)
- **include** - Defines a filter type that includes objects in the MIB subtree.
- **exclude** - Defines a filter type that excludes objects in the MIB subtree.
- *subtree* - The part of the MIB subtree that is to be filtered.
- *mask* - An optional hexadecimal value bit mask to define objects in the MIB subtree.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The access point allows up to 10 notification filters to be created. Each filter can be defined by up to 20 MIB subtree ID entries.
- Use the command more than once with the same filter ID to build a filter that includes or excludes multiple MIB objects.
- The MIB subtree must be defined in the form “.1.2.3.4” and always start with a “.”.
- The mask is a hexadecimal value with each bit masking the corresponding ID in the MIB subtree. A “1” in the mask indicates an exact match and a “0” indicates a “wild card.” For example, a mask value of 0xFFBF provides a bit mask “1111 1111 1011 1111.” If applied to the subtree 1.3.6.1.2.1.2.2.1.1.23, the zero corresponds to the 10th subtree ID. When there are more subtree IDs than bits in the mask, the mask is padded with ones.

show snmp filter

This command displays the SNMP v3 notification filter settings.

Syntax

show snmp filter [*filter-id*]

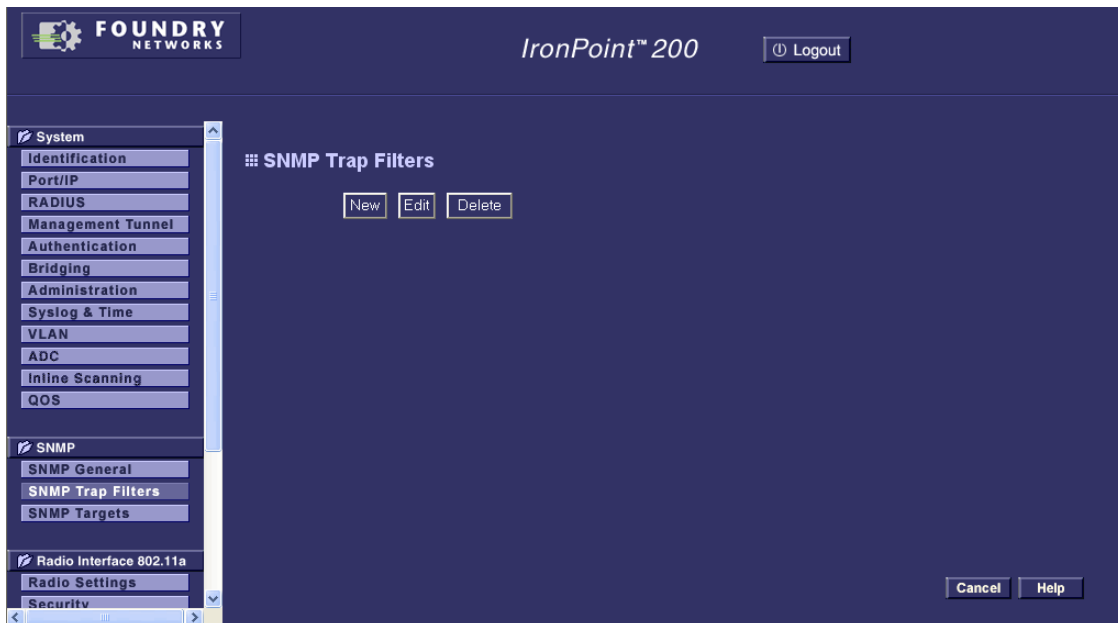
- *filter-id* - A user-defined name that identifies an SNMP v3 notification filter. (Maximum length: 32 characters)

Command Mode

Exec

Using the Web Management Interface

From the SNMP menu, click SNMP Trap Filters. To configure a new notification filter, click the New button.



A new page opens to configure the filter (see below).

The screenshot shows the Foundry Networks IronPoint 200 web interface. The top header includes the Foundry Networks logo, the product name 'IronPoint™ 200', and a 'Logout' button. The left sidebar is a navigation menu with the following items: System (expanded), Identification, Port/IP, RADIUS, Management Tunnel, Authentication, Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP (expanded), SNMP General, SNMP Trap Filters (selected), SNMP Targets, Radio Interface 802.11a, Radio Settings, and Security. The main content area is titled 'SNMP New Trap Filter' and contains three input fields: 'Filter ID' (text box), 'OID' (text box), and 'Filter Type' (dropdown menu set to 'Exclude'). At the bottom right of the main area are three buttons: 'Apply', 'Cancel', and 'Help'.

When you click on the New button in the SNMP Trap Filters page, a new page opens where the filter parameters are configured.

To edit an existing filter, select the radio button next to the entry in the table and then click the Edit button. To delete a filter, select the radio button next to the entry in the table and then click the Delete button.

Configurable Parameters

Filter ID – A user-defined name that identifies the filter. (Maximum length: 32 characters)

Subtree OID – Specifies MIB subtree to be filtered. The MIB subtree must be defined in the form “.1.2.3.4” and always start with a “.”.

Filter Type – Indicates if the filter is to “include” or “exclude” the MIB subtree objects from the filter. Note that MIB objects included in the filter are not sent to the receiving target and objects excluded are sent.

Configuring SNMPv3 Notification Targets

An SNMP v3 notification Target ID is specified by the SNMP v3 user, IP address, and UDP port. A user-defined filter can also be assigned to specific targets to limit the notifications received to specific MIB objects. (Note that the filter must first be configured. See “Configuring SNMPv3 Trap Filters” on page 10-12.)

Using the CLI

To create a notification target, use the **snmp-server targets** command from the CLI configuration mode. To assign a filter to a target, use the **snmp-server filter-assignment** command. To view the

current SNMP targets, use the **show snmp target** command from the CLI Exec mode. To view filter assignment to targets, use the **show snmp filter-assignments** command.

```
Foundry AP(config)#snmp-server targets mytraps 192.168.1.33 chris
Foundry AP(config)#snmp-server filter-assignment mytraps trapfilter
Foundry AP(config)#exit
Foundry AP#show snmp target

Host ID      : mytraps
User         : chris
IP Address   : 192.168.1.33
UDP Port     : 162
=====
Foundry AP#show snmp filter-assignments

                                HostID  FilterID
                                -----
                                mytraps  trapfilter

Foundry AP#
```

snmp-server targets

This command configures SNMP v3 notification targets. Use the **no** form to delete an SNMP v3 target.

Syntax

snmp-server targets <target-id> <ip-addr> <sec-name> [**version** {3}] [**udp-port** {port-number}] [**notification-type** {TRAP}]

no snmp-server targets <target-id>

- *target-id* - A user-defined name that identifies a receiver of SNMP notifications. (Maximum length: 32 characters)
- *ip-addr* - Specifies the IP address of the management station to receive notifications.
- *sec-name* - The defined SNMP v3 user name that is to receive notifications.
- **version** - The SNMP version of notifications. Currently only version **3** is supported in this command.
- **udp-port** - The UDP port that is used on the receiving management station for notifications.
- **notification-type** - The type of notification that is sent. Currently only **TRAP** is supported.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The SNMP v3 user name that is specified in the target must first be configured using the **snmp-server user** command.

snmp-server filter-assignment

This command assigns SNMP v3 notification filters to targets. Use the **no** form to remove an SNMP v3 filter assignment.

Syntax

snmp-server filter-assignment <target-id> <filter-id>
no snmp-server filter-assignment <target-id>

- *target-id* - A user-defined name that identifies a receiver of SNMP notifications. (Maximum length: 32 characters)
- *filter-id* - A user-defined name that identifies an SNMP v3 notification filter. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

show snmp target

This command displays the SNMP v3 notification target settings.

Syntax

show snmp target

Command Mode

Exec

show snmp filter-assignments

This command displays the SNMP v3 notification filter assignments.

Syntax

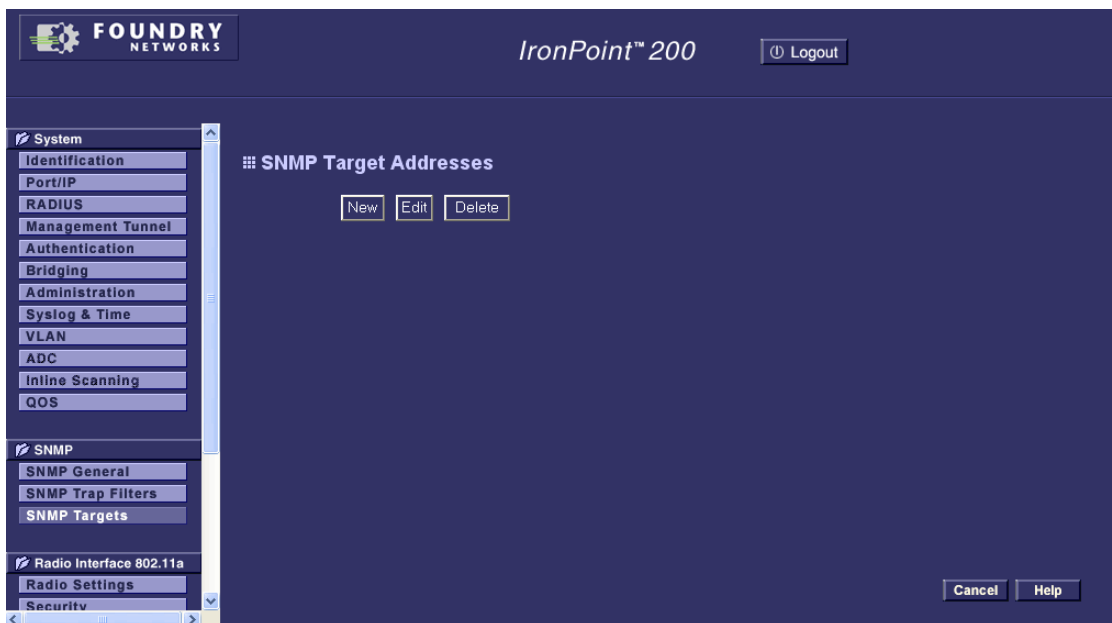
show snmp filter-assignments

Command Mode

Exec

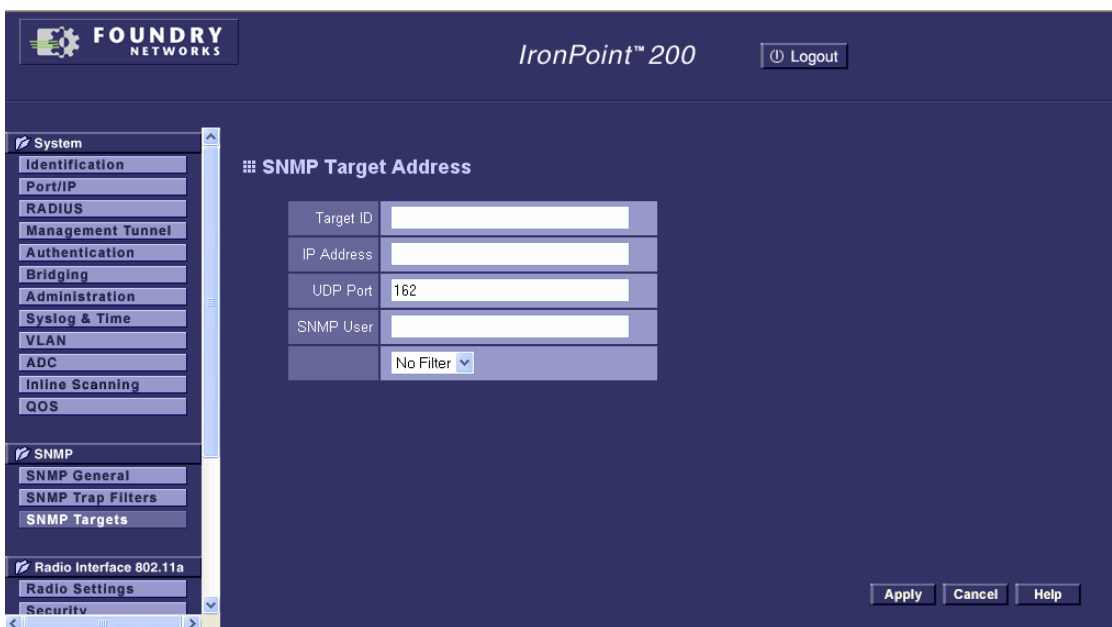
Using the Web Management Interface

From the SNMP menu, click SNMP Targets. To configure a new notification receiver target, click the New button. A new page opens to configure the settings (see below). To edit an existing target, select the radio button next to the entry in the table and then click the Edit button. To delete targets, select the radio button next to the entry in the table and then click the Delete button.



When you click on the New or Edit button in the SNMP Targets page, a new page opens where the target parameters are configured. Define the parameters and select a filter, if required. Note that the SNMP v3 user name must first be defined using the CLI. Click Apply.

Note: The Target ID cannot be changed in the Edit Target page. Only the New Target page allows the Target ID to be configured.



Configurable Parameters

Target ID – A user-defined name that identifies a receiver of notifications. (Maximum length: 32 characters)

IP Address – Specifies the IP address of the receiving management station.

UDP Port – The UDP port that is used on the receiving management station for notification messages.

SNMP User – The defined SNMP v3 user that is to receive notification messages. (Note that SNMP v3 users can only be defined using the CLI.)

Assigned Filter – The name of a user-defined notification filter that is applied to the target.

Chapter 11

System Identification

The system name for the access point can be left at its default setting. However, modifying this parameter can help you to more easily distinguish the access point from other devices in your network.

Using the CLI

In the CLI configuration mode, use the **system name** command to specify a new system name. Use the **show system** command from the Exec mode to display the current setting. (See “show system” on page 24-1.)

```
Foundry AP(config)#system name IronPoint-AP
```

system name

This command specifies or modifies the system name for this device. Use the **no** form to restore the default system name.

Syntax

system name <name>

no system name

name - The name of this host.
(Maximum length: 32 characters)

Default Setting

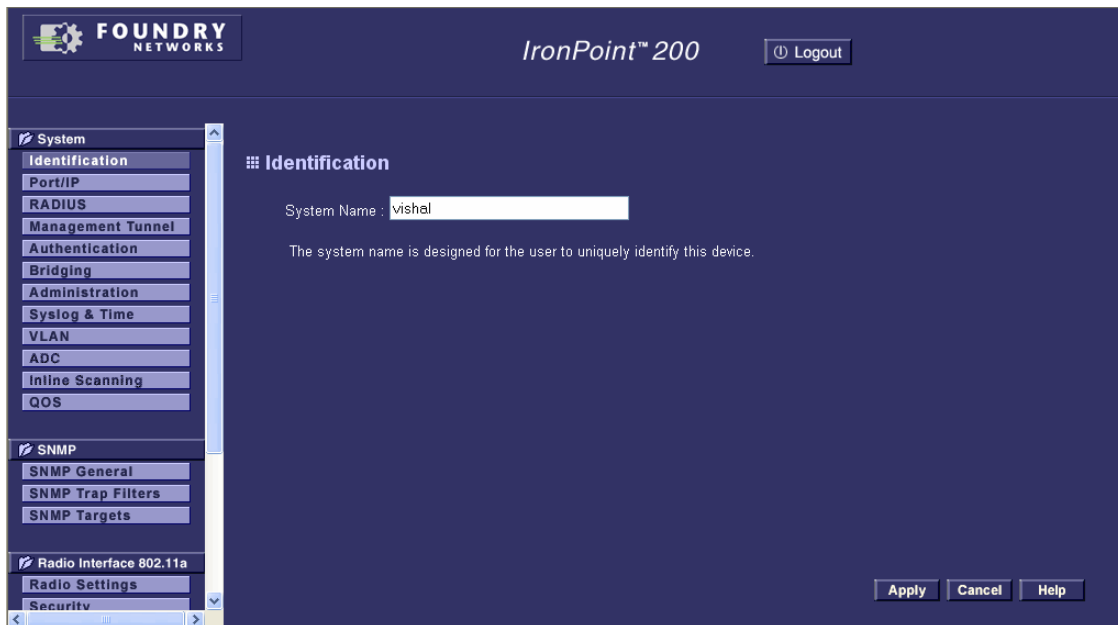
IronPoint 200: Foundry AP

Command Mode

Global Configuration

Using the Web Management Interface

From the System Menu, click Identification. Specify the system name in the text field, and then click Apply.



- **System Name** – An alias for the access point, enabling the device to be uniquely identified on the network. (Default: IronPoint 200 is Foundry AP, Range: 1-32 characters)

Chapter 12

System Logging

The access point supports a logging process that can control error messages saved to memory or sent to a System Log (Syslog) server. Connection details for up to four Syslog servers can be configured on the access point. The logged messages serve as a valuable tool for isolating access point and network problems.

The system allows you to limit the messages that are logged by specifying a minimum severity level. The following table lists the error message levels from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level.

Error Level	Description
Emergency	System unusable
Alert	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

Enabling System Logging

The access point's logging process must be enabled to save system messages to memory. Log messages saved in the access point's memory are erased when the device is rebooted. However, the access point can also be configured to send log messages to Syslog servers where they can be permanently stored.

The access point system clock should be set so that all the messages sent to Syslog servers are stamped with a meaningful time and date. See "System Clock" on page 13-1

Using the CLI

To enable logging on the access point, use the **logging on** command from the CLI configuration mode. The **logging level** command sets the minimum level of message to log. Use the **logging console** command to enable logging to the console. Use the **logging host** command to specify up to four Syslog servers. The CLI also allows the **logging facility-type** command to set the facility-

type number to use on the Syslog server. To view the current logging settings, use the **show logging** command.

```

Foundry AP(config)#logging on
Foundry AP(config)#logging level alert
Foundry AP(config)#logging console
Foundry AP(config)#logging host 1 10.1.0.3 514
Foundry AP(config)#logging facility-type 19
Foundry AP(config)#exit
Foundry AP#show logging

Logging Information
=====
Syslog State           : Disabled
Logging Console State  : Disabled
Logging Level          : Error
Logging Facility Type  : 16
Servers
  1: 0.0.0.0, UDP Port: 514, State: Disabled
  2: 0.0.0.0, UDP Port: 514, State: Disabled
  3: 0.0.0.0, UDP Port: 514, State: Disabled
  4: 0.0.0.0, UDP Port: 514, State: Disabled
=====

Foundry AP#

```

logging on

This command controls logging of error messages; i.e., sending debug or error messages to memory. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to memory. You can use the **logging level** command to control the type of error messages that are stored in memory.

logging level

This command sets the minimum severity level for event logging.

Syntax

logging level <Emergency | Alert | Critical | Error | Warning | Notice | Informational | Debug>

Default Setting

Informational

Command Mode

Global Configuration

Command Usage

Messages sent include the selected level down to the Emergency level.

Level Argument	Description
Emergency	System unusable
Alert	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

logging console

This command initiates logging of error messages to the console. Use the **no** form to disable logging to the console.

Syntax

logging console
no logging console

Default Setting

Disabled

Command Mode

Global Configuration

logging host

This command specifies a syslog server host that will receive logging messages. Use the **no** form to remove syslog server host.

Syntax

logging host <1 | 2 | 3 | 4> <*host_ip_address* | *host_name*> <*udp_port*>
no logging host

- **1** - First syslog server.
- **2** - Second syslog server.
- **3** - Third syslog server.
- **4** - Fourth syslog server.
- *host_ip_address* - The IP address of a syslog server.
- *host_name* - The name of a syslog server. (Range: 1-255 characters)
- *udp_port* - The UDP port used by the syslog server.

Default Setting

Disabled

Command Mode

Global Configuration

logging facility-type

This command sets the facility type for remote logging of syslog messages.

Syntax

logging facility-type <*type*>

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

16

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the access point. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

show logging

This command displays the logging configuration.

Syntax

show logging

Command Mode

Exec

Using the Web Management Interface

From the System menu, click Syslog & Time. Enable logging and specify a Syslog server or enable logging to the console interface. Set the Logging Level to restrict the number of messages that are logged. Click Apply.

Server	Enable/Disable	Name / IP	UDP Port
Server 1	<input checked="" type="radio"/> Enable	100.0.0.211	514
Server 2	<input checked="" type="radio"/> Enable	100.0.0.2	514
Server 3	<input checked="" type="radio"/> Disable		
Server 4	<input checked="" type="radio"/> Disable		

Logging Console: ☒ Enable

Logging Level:

SNTP Server: ☒ Disable

Configurable Parameters

System Log Setup – Enables the logging of error messages. (Default: Disable)

Logging Host – Enables the sending of log messages to a Syslog server host. Up to four Syslog servers are supported on the access point. (Default: Disable)

Server Name/IP – The IP address or name of a Syslog server. (Host Name: 1 to 255 characters)

UDP Port – The UDP port used by a Syslog server.

Logging Console – Enables the logging of error messages to the console. (Default: Disable)

Logging Level – Sets the minimum severity level for event logging. (Default: Informational)

Displaying Log Messages

The log messages generated by the access point and stored in memory can be viewed to check system events and errors. The access point also allows all the log messages to be cleared.

Using the CLI

To view the access point log entries, use the **show event-log** command from the Exec mode. To clear all log entries from the access point, use the **logging clear** command from the Global Configuration mode.

```

Foundry AP#show event-log
Mar 09 11:57:55 Information: 802.11g:11g Radio Interface Enabled
Mar 09 11:57:55 Information: 802.11g:Radio channel updated to 8
Mar 09 11:57:34 Information: 802.11g:11g Radio Interface Enabled
Mar 09 11:57:18 Information: 802.11g:11g Radio Interface Enabled
Mar 09 11:56:35 Information: 802.11a:11a Radio Interface Enabled
Mar 09 11:55:52 Information: SSH task: Set SSH server port to 22
Mar 09 11:55:52 Information: SSH task: Enable SSH server.
Mar 09 11:55:52 Information: Enable Telnet.
Mar 09 11:55:40 Information: 802.11a:11a Radio Interface Disabled
Mar 09 11:55:40 Information: 802.11a:Transmit Power set to QUARTER
Press <n> next. <p> previous. <a> abort. <y> continue to end :
Foundry AP#configure
Enter configuration commands, one per line. End with CTRL/Z
Foundry AP(config)#logging clear
Foundry AP#

```

show event-log

This command displays log messages stored in the access point's memory.

Syntax

show event-log

Command Mode

Exec

logging clear

This command clears all log messages stored in the access point's memory.

Syntax

logging clear

Command Mode

Global Configuration

Using the Web Management Interface

From the Status menu, click Event Log. The log entries can be deleted by clicking the Clear Log button.

FOUNDRY NETWORKS IronPoint™ 200 [Logout](#)

Event Logs

1	Jan 02 00:31:28 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
2	Jan 02 00:24:28 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
3	Jan 02 00:19:58 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
4	Jan 02 00:12:58 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
5	Jan 01 23:59:41 Information: DHCP Client : Receive Ack from 10.51.17.49, Lease time = 86400
6	Jan 01 23:59:41 Information: DHCP Client : Send Request, Request IP = 10.55.1.58
7	Jan 01 23:59:41 Information: DHCP Client : Send Request, Request IP = 10.55.1.58
8	Jan 01 23:59:16 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
9	Jan 01 23:30:08 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
10	Jan 01 23:18:58 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.
11	Jan 01 23:16:03 Warning: AP is receiving more than 10 multicast frames per second. Potential network overload condition exists.

Displayed Parameters

Log Time: The time the log message was generated.

Event Level: The logging level associated with this message. For a description of the various levels, see page 12-1.

Event Message: The content of the log message.

Note: The Event Logs window displays the last 128 messages logged in chronological order, from the newest to the oldest. Log messages saved in the access point's memory are erased when the device is rebooted.

Chapter 13

System Clock

Simple Network Time Protocol (SNTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an SNTP client, periodically sending time synchronization requests to specific time servers. You can configure up to two time server IP addresses. The access point will attempt to poll each server in the configured sequence.

If a time server is not used to set the system clock, the date and time can be set manually.

Using the CLI

To enable SNTP support on the access point, from the CLI configuration mode specify SNTP server IP addresses using the **sntp-server ip** command, then use the **sntp-server enable** command to enable the service. Use the **sntp-server timezone** command to set the location time zone and the

sntp-server daylight-saving command to set up a daylight saving. To view the current SNTP settings, use the **show sntp** command.

```

Foundry AP(config)#sntp-server ip 1 10.1.0.19
Foundry AP(config)#sntp-server enable
Foundry AP(config)#sntp-server timezone +8
Foundry AP(config)#sntp-server daylight-saving
Enter Daylight saving from which month<1-12>: 3
and which day<1-31>: 31
Enter Daylight saving end to which month<1-12>: 10
and which day<1-31>: 31
Foundry AP(config)#exit
Foundry AP#show sntp

SNTP Information
=====
Service State      : Enabled
SNTP (server 1) IP : 10.1.0.19
SNTP (server 2) IP : 0.0.0.0
Current Time       : 19 : 35, Nov 10, 2007
Time Zone          : +8 (TAIPEI, BEIJING)
Daylight Saving    : Enabled, from Mar, 31th to Oct, 31th
=====

Foundry AP#

```

The following CLI example shows how to manually set the system time when SNTP server support is disabled on the access point. This example sets the system clock to 17:37 June 19, 2007.

```

Foundry AP(config)#no sntp-server enable
Foundry AP(config)#sntp-server date-time
Enter Year<1970-2100>: 2007
Enter Month<1-12>: 6
Enter Day<1-31>: 19
Enter Hour<0-23>: 17
Enter Min<0-59>: 37
Foundry AP(config)#

```

sntp-server date-time

This command sets the system clock.

Syntax

sntp-server date-time

Default Setting

00 : 00, Jan 1, 1970

Command Mode

Global Configuration

sntp-server ip

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp-server ip <1 | 2> <*host_ip_address* | *host_name*>

- **1** - First time server.
- **2** - Second time server.
- *host_ip_address* - The IP address of a time server (NTP or SNTP).
- *host_name* - The name of a time server (NTP or SNTP). (Range: 1-255 characters)

Default Setting

0.0.0.0 for both time servers

Command Mode

Global Configuration

Command Usage

When SNTP client mode is enabled using the **sntp-server enable** command, the **sntp-server ip** command specifies the time servers from which the access point polls for time updates. The access point will poll the time servers in the order specified until a response is received.

sntp-server enable

This command enables SNTP client requests for time synchronization with NTP or SNTP time servers specified by the **sntp-server ip** command. Use the **no** form to disable SNTP client requests.

Syntax

sntp-server enable
no sntp-server enable

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the access point only records the time starting from the factory default set at the last bootup (i.e., 00 : 00, Jan 1, 1970).

sntp-server daylight-saving

This command sets the start and end dates for daylight savings time. Use the **no** form to disable daylight savings time.

Syntax

sntp-server daylight-saving
no sntp-server daylight-saving

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The command sets the system clock back one hour during the specified period.

sntp-server timezone

This command sets the time zone for the access point's internal clock.

Syntax

sntp-server timezone <hours>

hours - Number of hours before/after UTC.
(Range: -12 to +12 hours)

Default Setting

-5

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

show sntp

This command displays the current time and configuration settings for the SNTP client.

Syntax

show sntp

Command Mode

Exec

Using the Web Management Interface

From the System menu, click Syslog & Time. Enable logging and specify a Syslog server or enable logging to the console interface. Set the Logging Level to restrict the number of messages that are logged.

FOUNDRY NETWORKS IronPoint™ 200 [Logout](#)

System Log

System Log Setup ☐ Disable ☒ Enable

Server 1	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Name / IP	100.0.0.211	UDP Port	514
Server 2	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Name / IP	100.0.0.2	UDP Port	514
Server 3	<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
Server 4	<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
Logging Console	<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
Logging Level	Informational				

SNTP Server ☒ Disable ☐ Enable

If SNTP server support is enabled, set IP addresses for the primary and secondary servers. If SNTP server support is disabled, enter the time and date in the appropriate text fields. Set the Time Zone for your location and, if required, set the period for Daylight Saving. Click Apply.

FOUNDRY NETWORKS IronPoint™ 200 [Logout](#)

System Clock

Set Time ☐ Disable ☒ Enable

Logging Console ☐ Disable ☒ Enable

Logging Level: Informational

SNTP Server ☒ Disable ☐ Enable

Set Time: Year: 1970 Month: 1 Day: 2 Hour: 0 Min: 39

Set Time Zone

Enter Time Zone: (GMT-05) Eastern Time (US & Canada)

☐ Enable Daylight Saving

From: JAN 1 To: DEC 31

[Apply](#) [Cancel](#)

Configurable Parameters

System Log Setup – Enables the logging of error messages. (Default: Disable)

Logging Host – Enables the sending of log messages to a Syslog server host. Up to four Syslog servers are supported on the access point. (Default: Disable)

Server Name/IP – The IP address or name of a Syslog server.

UDP Port – The UDP port used by a Syslog server.

Logging Console – Enables the logging of error messages to the console. (Default: Disable)

Logging Level – Sets the minimum severity level for event logging. (Default: Informational)

SNTP Server – Configures the access point to operate as an SNTP client. When enabled, at least one time server IP address or name must be specified. When disabled, the system time can be entered manually in the text fields provided. (Default: Enable)

- **Primary Server:** The IP address or name of an SNTP or NTP time server that the access point attempts to poll for a time update. (Host Name: 1 to 255 characters)
- **Secondary Server:** The IP address or name of a secondary SNTP or NTP time server. The access point first attempts to update the time from the primary server; if this fails it attempts an update from the secondary server. (Host Name: 1 to 255 characters)

Set Time Zone – SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours your time zone is located before (east) or after (west) UTC. (Default: (GMT-05) Eastern Time (US & Canada))

Enable Daylight Saving – The access point provides a way to automatically adjust the system clock for Daylight Savings Time changes. To use this feature you must define the month and date to begin and to end the change from standard time. During this period the system clock is set back by one hour. (Default: Disable)

Chapter 14

Management Tunnel Settings

The access point uses a Point-to-Point Protocol over Ethernet (PPPoE) connection, or tunnel, only for management traffic between the access point and a remote PPPoE server (typically at an ISP). Examples of management traffic that may be initiated by the access point and carried over a PPPoE tunnel are RADIUS, Syslog, or DHCP traffic.

Using the CLI

From the CLI configuration mode, use the **interface ethernet** command to access interface configuration mode. Use the **ip pppoe** command to enable PPPoE on the Ethernet interface. Use the other PPPoE commands shown in the example below to set a user name and password, IP settings, and other PPPoE parameters as required by the service provider. The **pppoe restart**

command can then be used to start a new connection using the modified settings. To display the current PPPoE settings, use the **show pppoe** command from the Exec mode.

```
Foundry AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
Foundry AP(if-ethernet)#ip pppoe
Foundry AP(if-ethernet)#pppoe username mike
Foundry AP(if-ethernet)#pppoe password 12345
Foundry AP(if-ethernet)#pppoe service-name classA
Foundry AP(if-ethernet)#pppoe ip allocation mode static
Foundry AP(if-ethernet)#pppoe local ip 10.7.1.200
Foundry AP(if-ethernet)#pppoe remote ip 192.168.1.20
Foundry AP(if-ethernet)#pppoe ipcp dns
Foundry AP(if-ethernet)#pppoe lcp echo-interval 30
Foundry AP(if-ethernet)#pppoe lcp echo-failure 5
Foundry AP(if-ethernet)#pppoe restart
Foundry AP(if-ethernet)#end
Foundry AP#show pppoe
```

```
PPPoE Information
=====
State                : Link up
Username             : mike
Service Name         : classA
IP Allocation Mode    : Static
DNS Negotiation       : Enabled
Local IP             : 10.7.1.200
Echo Interval        : 30
Echo Failure         : 5
=====

Foundry AP#
```

ip pppoe

This command enables Point-to-Point Protocol over Ethernet (PPPoE) on the Ethernet interface. Use the **no** form to disable PPPoE on the Ethernet interface.

Syntax

ip pppoe
no ip pppoe

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

The access point uses a PPPoE connection, or tunnel, only for management traffic between the access point and a remote PPPoE server (typically at an ISP). Examples of management traffic that may be initiated by the access point and carried over a PPPoE tunnel are RADIUS, Syslog, or DHCP traffic.

pppoe ip allocation mode

This command specifies how IP addresses for the PPPoE tunnel are configured on this interface.

Syntax

pppoe ip allocation mode {automatic | static}

- **automatic** - IP addresses are dynamically assigned by the ISP during PPPoE session initialization.
- **static** - Fixed addresses are assigned by the ISP for both the local and remote IP addresses.

Default Setting

automatic

Command Mode

Interface Configuration (Ethernet)

Command Usage

The IP address allocation mode depends on the type of service provided by the ISP. If automatic mode is selected, DHCP is used to allocate the IP addresses for the PPPoE connection. If static addresses have been assigned to by the ISP, these must be entered using the **pppoe local ip** and **pppoe remote ip** commands.

pppoe ipcp dns

This command requests allocation of IP addresses for Dynamic Naming System (DNS) servers from the device at the remote end of the PPPoE tunnel.

Syntax

pppoe ipcp dns
no pppoe ipcp dns

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

DNS servers are used to translate host computer names into IP addresses. PPPoE clients can request a primary and secondary DNS server from the network connection device at the remote end of the PPPoE tunnel. This request is passed to the remote end during the IP Control Protocol (IPCP) negotiation phase during session initialization.

pppoe lcp echo-interval

This command sets the Link Control Protocol (LCP) echo interval for the PPPoE tunnel.

Syntax

pppoe lcp echo-interval <interval>

interval - The interval between sending echo requests. (Range: 1-60 seconds)

Default Setting

10

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Echo requests are used to verify the integrity of the link through the PPPoE tunnel. Devices at either end of the link can issue an echo-request. Devices receiving an echo-request must return an echo-reply.
- If a link is busy with large data transfers, the echo-reply may not be issued in a timely manner causing the link to timeout. If you experience this kind of problem, try extending the echo interval or timeout.

pppoe lcp echo-failure

This command sets the Link Control Protocol (LCP) echo timeout for the PPPoE tunnel.

Syntax

pppoe lcp echo-failure *<timeout>*

timeout - The number of timeouts allowed. (Range: 1-10)

Default Setting

3

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Echo requests are used to verify the integrity of the link through the PPPoE tunnel. Devices at either end of the link can issue an echo-request. Devices receiving an echo-request must return an echo-reply.
- If a link is busy with large data transfers, the echo-reply may not be issued in a timely manner causing the link to timeout. If you experience this kind of problem, try extending the echo interval or timeout.

pppoe local ip

This command sets the local IP address for the PPPoE tunnel.

Syntax

pppoe local ip *<ip-address>*

ip-address - IP address of the local end of the PPPoE tunnel.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If the **pppoe ip allocation mode** is set to static, the local IP address must be entered with this command, and the remote IP address must be entered with the **pppoe remote ip** command.

pppoe remote ip

This command sets the remote IP address for the PPPoE tunnel.

Syntax

pppoe remote ip <*ip-address*>

ip-address - IP address of the remote end of the PPPoE tunnel.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If the **pppoe ip allocation mode** is set to static, the remote IP address must be entered with this command, and the local IP address must be entered with the **pppoe local ip** command.

pppoe username

This command sets the user name for the PPPoE tunnel.

Syntax

pppoe username <*username*>

username - User name assigned by the service provider. (Range: 1-32 alphanumeric characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

You must enter a user name with this command, and a password with the **pppoe password** command.

pppoe password

This command sets the password for the PPPoE tunnel.

Syntax

pppoe password <*string*>

string - Password assigned by the service provider. (Range: 1-32 alphanumeric characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

You must enter a password with this command, and a user name with the **pppoe username** command.

pppoe service-name

This command sets the service name for the PPPoE tunnel.

Syntax

pppoe service-name <*string*>

string - Service name assigned by the service provider. (Range: 1-32 alphanumeric characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

The service name is normally optional, but may be required by some service providers.

pppoe restart

This command restarts the PPPoE connection with updated parameters.

Syntax

pppoe restart

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command restarts PPPoE service using the most recently configured parameters.

show pppoe

This command shows information about the PPPoE configuration.

Syntax

show pppoe

Command Mode

Privileged Exec

Using the Web Management Interface

From the System menu, click Management Tunnel. Enable PPPoE and enter the assigned user name and password, service name, and IP settings as provided by the service provider. Click Apply.

The screenshot shows the Foundry Networks IronPoint 200 web management interface. The left sidebar contains a navigation menu with the following items: System, Identification, Port/IP, RADIUS, Management Tunnel (selected), Authentication, Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QoS, SNMP, SNMP General, SNMP Trap Filters, SNMP Targets, Radio Interface 802.11a, Radio Settings, and Security. The main content area is titled 'PPPoE Settings' and contains the following configuration fields:

PPP over Ethernet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PPPoE Username	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm Password	<input type="password"/>
PPPoE Service Name	<input type="text"/>
PPPoE DNS Negotiation	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PPPoE Echo Failure	<input type="text" value="3"/>
PPPoE Echo Interval	<input type="text" value="10"/>
IP Allocation Mode	<input checked="" type="radio"/> Automatically allocated <input type="radio"/> Static assigned

Below the fields is a 'PPPoE Restart' button. At the bottom right are 'Apply', 'Cancel', and 'Help' buttons.

Configurable Parameters

PPP over Ethernet – Enable PPPoE on the RJ-45 Ethernet interface to pass management traffic between the access point and a remote PPPoE server. (Default: Disable)

PPPoE Username – The user name assigned for the PPPoE tunnel. (Range: 1-32 alphanumeric characters)

PPPoE Password – The password assigned for the PPPoE tunnel. (Range: 1-32 alphanumeric characters)

Confirm Password – Use this field to confirm the PPPoE password.

PPPoE Service Name – The service name assigned for the PPPoE tunnel. The service name is normally optional, but may be required by some service providers. (Range: 1-32 alphanumeric characters)

PPPoE DNS Negotiation – DNS servers are used to translate host computer names into IP addresses. PPPoE clients can request a primary and secondary DNS server from the network connection device at the remote end of the PPPoE tunnel. This request is passed to the remote end during the IP Control Protocol (IPCP) negotiation phase during session initialization.

PPPoE Echo Failure – Echo requests are used to verify the integrity of the link through the PPPoE tunnel. Devices at either end of the link can issue an echo-request. Devices receiving an echo-request must return an echo-reply. If a link is busy with large data transfers, the echo-reply may not

be issued in a timely manner causing the link to timeout. If you experience this kind of problem, try extending the echo failure count or the echo interval.

PPPoE Echo Interval – Sets the interval between sending echo requests for the PPPoE tunnel.

IP Allocation Mode – This field specifies how IP addresses for the PPPoE tunnel are configured on the RJ-45 interface. The allocation mode depends on the type of service provided by the PPPoE server. If automatic mode is selected, DHCP is used to allocate the IP addresses for the PPPoE connection. If static addresses have been assigned by the service provider, you must manually enter the assigned addresses. (Default: Automatic)

- **Automatically allocated:** IP addresses are dynamically assigned by the service provider during PPPoE session initialization.
- **Static assigned:** Fixed addresses are assigned by the service provider for both the local and remote IP addresses.

Local IP Address – IP address of the local end of the PPPoE tunnel. (Must be entered for static IP allocation mode.)

Remote IP Address – IP address of the remote end of the PPPoE tunnel. (Must be entered for static IP allocation mode.)

Chapter 15

RADIUS Client Settings

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network.

A primary RADIUS server must be specified for the access point to implement IEEE 802.1x network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible.

In addition, the configured RADIUS server can also act as a RADIUS Accounting server and receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured a RADIUS server to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

Using the CLI

From the CLI configuration mode, use the **radius-server address** command to specify the IP address or host name of a primary and, if required, secondary RADIUS server. Specify the UDP port used by the RADIUS server using the **radius-server port** command. Using the **radius-server key** command, enter the same “secret key” that is also configured on the RADIUS server. If necessary, adjust the re-transmit and timeout parameters using the **radius-server retransmit** and **radius-server timeout** commands. If you are using RADIUS Accounting, you must specify the server port using the **radius-server port-accounting** command and set the timeout for accounting updates using the **radius-server timeout-interim** command. You can also specify the format of MAC addresses and VLAN IDs configured on the RADIUS server using the **radius-server radius-mac-**

format and **radius-server vlan-format** commands. To display the current RADIUS server settings, use the **show radius** command from the Exec mode.

```

Foundry AP(config)#radius-server address 192.168.1.25
Foundry AP(config)#radius-server port 1234
Foundry AP(config)#radius-server key green
Foundry AP(config)#radius-server retransmit 5
Foundry AP(config)#radius-server timeout 10
Foundry AP(config)#radius-server port-accounting 1813
Foundry AP(config)#radius-server timeout-interim 500
Foundry AP(config)#radius-server radius-mac-format multi-dash
Foundry AP(config)#radius-server vlan-format ascii
Foundry AP(config)#end
Foundry AP#show radius

Radius Server Information
=====
IP                : 192.168.1.25
Port              : 1234
Key               : *****
Retransmit        : 5
Timeout           : 10
Accounting Port   : 1813
InterimUpdate     : 500
=====

Radius Secondary Server Information
=====
IP                : 0.0.0.0
Port              : 1812
Key               : *****
Retransmit        : 3
Timeout           : 5
Accounting Port   : 0
InterimUpdate     : 3600
=====
Foundry AP#

```

radius-server address

This command specifies the primary and secondary RADIUS servers.

Syntax

radius-server address [secondary] <host_ip_address | host_name>

- **secondary** - Secondary server.
- *host_ip_address* - IP address of server.
- *host_name* - Host name of server. (Range: 1-255 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

If the **secondary** argument is not specified in the command, the CLI configures the primary RADIUS server.

radius-server port

This command sets the RADIUS server network port.

Syntax

radius-server [**secondary**] **port** <port_number>

- **secondary** - Secondary server. If **secondary** is not specified, then the access point assumes you are configuring the primary RADIUS server.
- *port_number* - RADIUS server UDP port used for authentication messages. (Range: 1024-65535)

Default Setting

1812

Command Mode

Global Configuration

radius-server key

This command sets the RADIUS “secret key” that is used to encrypt messages between the access point and the RADIUS server. The key must be configured the same on both the access point and the RADIUS server.

Syntax

radius-server [**secondary**] **key** <key_string>

- **secondary** - Secondary server. If **secondary** is not specified, then the access point assumes you are configuring the primary RADIUS server.
- *key_string* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 64 characters)

Default Setting

DEFAULT

Command Mode

Global Configuration

radius-server retransmit

This command sets the number of retries for sending authentication requests to the RADIUS server.

Syntax

radius-server [**secondary**] **retransmit** <number_of_retries>

- **secondary** - Secondary server.
- *number_of_retries* - Number of times the access point tries to send an authentication request to the RADIUS server. (Range: 1 - 30)

Default Setting

3

Command Mode

Global Configuration

Command Usage

The access point sends client authentication requests to the RADIUS server and waits for a reply. If no reply is received within the configured timeout period, the access point continues to resend the authentication request for the number of times set by the retransmit parameter. When the number of retransmit attempts has expired without a reply, client authentication fails.

radius-server timeout

This command sets the interval between each retransmit attempt when sending authentication requests to the RADIUS server.

Syntax

radius-server [**secondary**] **timeout** *<number_of_seconds>*

- **secondary** - Secondary server.
- *number_of_seconds* - Number of seconds the access point waits for a reply before resending a request. (Range: 1-60)

Default Setting

5

Command Mode

Global Configuration

radius-server port-accounting

This command sets the RADIUS Accounting server network port.

Syntax

radius-server [**secondary**] **port-accounting** *<port_number>*

- **secondary** - Secondary server. If **secondary** is not specified, then the access point assumes you are configuring the primary RADIUS server.
- *port_number* - RADIUS Accounting server UDP port used for accounting messages. (Range: 0 or 1024-65535)

Default Setting

0 (disabled)

Command Mode

Global Configuration

Command Usage

- When the RADIUS Accounting server UDP port is specified, a RADIUS accounting session is automatically started for each user that is successfully authenticated to the access point.

radius-server timeout-interim

This command sets the interval between transmitting accounting updates to the RADIUS server.

Syntax

radius-server [**secondary**] **timeout-interim** <*number_of_seconds*>

- **secondary** - Secondary server.
- *number_of_seconds* - Number of seconds the access point waits between transmitting accounting updates. (Range: 60-86400)

Default Setting

3600

Command Mode

Global Configuration

Command Usage

- The access point sends periodic accounting updates after every interim period until the user logs off and a “stop” message is sent.

radius-server radius-mac-format

This command sets the format for specifying MAC addresses on the RADIUS server.

Syntax

radius-server radius-mac-format <**multi-colon** | **multi-dash** | **no-delimiter** | **single-dash**>

- **multi-colon** - Enter MAC addresses in the form aa:bb:cc:dd:ee:ff.
- **multi-dash** - Enter MAC addresses in the form aa-bb-cc-dd-ee-ff.
- **no-delimiter** - Enter MAC addresses in the form aabbccddeeff.
- **single-dash** - Enter MAC addresses in the form aabbcc-ddeeff.

Default Setting

No delimiter

Command Mode

Global Configuration

radius-server vlan-format

This command sets the format for specifying VLAN IDs on the RADIUS server.

Syntax

radius-server vlan-format <**hex** | **ascii**>

- **hex** - Enter VLAN IDs as a hexadecimal number.
- **ascii** - Enter VLAN IDs as an ASCII string.

Default Setting

ASCII

Command Mode

Global Configuration

show radius

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Exec

Using the Web Management Interface

From the System menu, click RADIUS. Specify the Primary RADIUS server settings in the appropriate text fields. If you are using a secondary RADIUS server, specify the details. You can also specify the ID of VLANs configured on the RADIUS server. Click Apply.

Primary RADIUS Server Setup	
IP Address	0.0.0.0
Port	1812
Secret Key	•••••
Timeout (seconds)	5
Retransmit attempts	3
Accounting Port	0
Interim Update Timeout	3600

Secondary RADIUS Server Setup	
IP Address	0.0.0.0
Port	1812
Secret Key	•••••

Configurable Parameters

Primary Radius Server Setup – Configure the following settings to use RADIUS authentication on the access point.

- **IP Address:** Specifies the IP address or host name of the RADIUS server. (Host Name: 1 to 255 characters)
- **Port:** The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Key:** A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 64 characters)
- **Timeout:** Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 5)

- **Retransmit attempts:** The number of times the access point tries to resend a request to the RADIUS server before authentication fails. (Range: 1-30; Default: 3)
- **Accounting Port:** The RADIUS Accounting server UDP port used for accounting messages. (Range: 0 or 1024-65535; Default: 0, disabled)
- **Interim Update Timeout:** The interval between transmitting accounting updates to the RADIUS server. (Range: 60-86400; Default: 3600 seconds)

Note: For the Timeout and Retransmit attempts fields, accept the default values unless you experience problems connecting to the RADIUS server over the network.

Secondary Radius Server Setup – Configure a secondary RADIUS server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role.

Radius VLAN ID Format Setup – Sets the format for specifying VLAN IDs on the RADIUS server. VLAN IDs can be entered as a hexadecimal number or an ASCII string. (Default: ASCII)

Chapter 16

TACACS+ AAA

You can use TACACS+ (Terminal Access Controller Access Control System Plus) to perform authentication, authorization, and accounting of Telnet or console access to the IronPoint access point. The TACACS+ protocol defines how authentication, authorization, and accounting (AAA) information is sent between the IronPoint access point and an authentication database on a TACACS+ server. TACACS+ services are maintained in a database, typically on a UNIX workstation or PC with a TACACS+ server running.

TACACS+ Authentication

When you configure an IronPoint access point to use a TACACS+ server for authentication, the device prompts users who are trying to access the CLI for a user name and password, then verifies the password with the TACACS+ server.

If you are using TACACS+, Foundry recommends that you also configure **authorization**, in which the IronPoint device consults a TACACS+ server to determine which management privilege level (and which associated set of commands) an authenticated user is allowed to use. You can also optionally configure **accounting**, which causes the Foundry device to log information on the TACACS+ server when certain events occur on the access point.

TACACS+ Authorization

Once a user is authenticated after login, he or she is placed at the appropriate privilege levels as follows:

- If authorization is not configured, the user is placed into the “admin” privilege level of the CLI. At this level the user has full read and write access to the CLI.
- If authorization is configured, the user is placed at either the “admin” privilege level or “read-only” privilege level, depending on the privilege level defined for that user.

When TACACS+ exec authorization takes place, the following events occur:

1. A user logs into the IronPoint access point using Telnet or console.
2. The user is authenticated.
3. The IronPoint access point consults the TACACS+ server to determine the privilege level of the user.

4. The TACACS+ server sends back a response containing an A-V (Attribute-Value) pair with the privilege level of the user.
5. The user is granted the specified privilege level.

TACACS+ Accounting

TACACS+ accounting works as follows:

1. A user logs into the access point using Telnet or console and is authenticated and is authorized with a certain privilege level.
2. If the user's privilege level requires TACACS+ accounting, IronPoint access point sends a TACACS+ accounting start packet to the TACACS+ accounting server, containing information about the commands the user enters.
3. The TACACS+ accounting server acknowledges the accounting start packet.
4. The TACACS+ accounting server records information about the commands.
5. When the user logs out, the IronPoint access point sends an accounting stop packet to the TACACS+ accounting server.
6. The TACACS+ accounting server acknowledges the accounting stop packet and stops recording.

Configuration Note

When using TACACS+ for AAA services:

- The configured system name is used as the default CLI prompt during a TACACS+ Telnet or console session.
- If the CLI prompt is customized during a TACACS+ Telnet session, the prompt will revert to the system name once the user logs out.
- You cannot use the **no prompt** command to remove the customized CLI prompt during a TACACS+ Telnet session.
- There can be only one console TACACS+ user and only one Telnet TACACS+ user logged in at the same time. If a second user tries to connect to the IronPoint access point, the access point will close the connection of the new user.

Defining TACACS+ Servers

Before you can define TACACS+ AAA options, you must first identify the TACACS+ servers on the IronPoint access point. The TACACS+ server provides the authentication, authorization, and accounting services when a user logs in.

You can define up to two TACACS+ server on the access point. The first is the primary server. The second is the secondary, which will provide AAA services if the primary TACACS+ server is not available.

Also, you must identify the IP addresses of the IronPoint access points in the TACACS+ server as AAA clients; otherwise, the IronPoint access points will hang when you a user attempts to login on the IronPoint access point as a TACACS user.

```

Foundry AP(config)#tacacs address 192.168.20.255
Foundry AP(config)#tacacs key 12sdjdiimsksn
Foundry AP(config)#tacacs port 49
Foundry AP(config)#tacacs port-accounting 49
Foundry AP(config)#tacacs retransmit 5
Foundry AP(config)#tacacs timeout 5
Foundry AP(config)#tacacs secondary address 20.1.1.2
Foundry AP(config)#tacacs secondary key maryhadalittlelamb
Foundry AP(config)#tacacs secondary port 49
Foundry AP(config)#tacacs secondary port-accounting 49
Foundry AP(config)#show tacacs
Tacacs+ Server Information
=====
IP           : 192.168.20.255
Port         : 49
Key          : *****
Retransmit   : 5
Timeout      : 5
Accounting Port : 49
=====

Tacacs+ Secondary Server Information
=====
IP           : 20.1.1.2
Port         : 49
Key          : *****
Retransmit   : 5
Timeout      : 5
Accounting Port : 49
=====

Foundry AP(config)#show user

-----
User Name: admin
Password : *****
Privilege: Admin

-----
Console Login Users (TACACS+):
-----
User Name: fdry
Privilege: Admin
-----

Telnet Login Users (TACACS+):
      Total number of users: 1
-----
User Name: fdry
Privilege: Admin
-----

```

tacacs address

This command identifies the TACACS+ server that will be used for TACACS+ AAA services. You can define a primary and a secondary TACACS+ server. The secondary TACACS+ server will be used for AAA services if the primary one is unavailable. Use the **no** form of the command to remove a TACACS+ server from the configuration.

Syntax

tacacs [secondary] address <ip-address>

no tacacs [secondary] address

secondary - Use this keyword to define a secondary TACACS+ server. You can define a secondary TACACS+ server without defining a primary one.

ip-address - IP address of the TACACS+ server.

hostname - Hostname of the TACACS+ server. Enter up to 255 characters.

Default Setting

0.0.0.0

Command Mode

Global Configuration

Command Usage

See above.

tacacs key

This command defines the TACACS+ key used to encrypt TACACS+ packets before they are sent over the network. This key parameter must match the one configured on the TACACS+ server. Use the **no** form of the command to remove the TACACS+ key from the configuration.

Syntax

tacacs [secondary] key <string>

no tacacs [secondary] key

secondary - Use this keyword to define a key for the secondary TACACS+ server.

string - 1 to 32 characters long

Default Setting

DEFAULT

Command Mode

Global Configuration

Command Usage

See above.

tacacs port

This command defines the TCP port that TACACS+ will use for authentication and authorization. Use the **no** form of the command to remove port from the configuration.

Syntax**tacacs [secondary] port <number>****[no] tacacs [secondary] port**

secondary - Use this keyword to define the authentication and authorization port for the secondary TACACS+ server.

number - Enter the TCP port number. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Command Usage

See above.

tacacs port-accounting

This command defines the TCP port that TACACS+ will use for accounting. Use the **no** form of the command to remove a accounting port from the configuration.

Syntax**tacacs [secondary] port-accounting <number>****no tacacs [secondary] port-accounting**

secondary - Use this keyword to define the accounting port for the secondary TACACS+ server.

number - Enter the TCP port number. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Command Usage

See above.

tacacs retransmit

This parameter specifies how many times the IronPoint access point will resend an authentication request when the TACACS+ server does not respond before considering the TACACS+ server to be unavailable. If there are two TACACS+ servers, the IronPoint access point checks the primary server first. If the primary server is unavailable, it checks the secondary TACACS+ server. If none of the TACACS+ server is available, the authentication, authorization, or accounting request is dropped and user's access to the network is not granted.

Syntax**tacacs retransmit <number>****no tacacs retransmit**

number - Number of transmission retries (Range: 1 - 30)

Default Setting

3

Command Mode

Global Configuration

Command Usage

See above.

tacacs timeout

This command specifies how many seconds the IronPoint access point waits for a response from a TACACS+ server before either retrying the authentication request or determining that the TACACS+ server is unavailable. If there are two TACACS+ servers, the IronPoint access point checks the primary server first. If the primary server is unavailable, it checks the secondary TACACS+ server. If none of the TACACS+ server is available, the authentication, authorization, or accounting request is dropped and user's access to the network is not granted.

Syntax

tacacs timeout <seconds>
no tacacs timeout

seconds - Number of seconds between retries. (Range 1 - 15 seconds)

Default Setting

3 seconds

Command Mode

Global Configuration

Command Usage

See above.

show tacacs

Syntax

show tacacs

Default Setting

None.

Command Mode

Global Command

Command Usage

See above.

Related Command

If TACACS+ users are logged in, the **show user** command list the user names and privilege level.

Configuring TACACS+ Authentication

The commands below are used to enable the IronPoint access point to use the AAA services via the TACACS+ server and to enable TACACS+ authentication.

```
Foundry AP(config)#aaa authentication login default tacacs+ local
Foundry AP(config)#aaa console enable
```

aaa authentication

This command enables the IronPoint access point to use the authentication service of a server that provides AAA services. When users connect to the IronPoint access point using Telnet or console, they will be required to enter a user name and password. The IronPoint access point consults the server to authenticate the user name and password.

Currently, authentication will be performed by the TACACS+ server. If no TACACS+ server is defined, the login will fail.

Syntax

```
aaa authentication login default tacacs+ local | null
no aaa authentication login default tacacs+ local | null
```

Default Setting

Disable.

Command Mode

Global Configuration

Command Usage

The TACACS+ server that provides AAA services must be identified in the IronPoint access point, and that server must have the name and passwords of users who are allowed to log into the IronPoint access point.

AAA authentication must be configured if you want to use authorization and accounting.

You also need to specify a rollover method by entering **local** or **null**. The **local** rollover method allows the access point to authenticate a user if the TACACS+ server is not available. If **null** is used, then a user is authenticated only by a TACACS+ server that is reachable in the network. You must indicate **local** or **null**.

aaa console enable

This command is optional. It enables the AAA services for console login on the IronPoint access Point. Currently, the TACACS+ server, if one is configured, provides AAA services for console logins. Use the **no** form of the command to disable TACACS+ AAA services.

Syntax

```
aaa console enable
no aaa console enable
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Ensure that at least one server that provides AAA services has been defined in the IronPoint access point. Also, before you can enter this command, make sure AAA services have been configured on the access point using the **aaa authentication** command.

Configuring TACACS+ Authorization

The commands below are used to enable AAA authorization on the IronPoint access point.

```
Foundry AP(config)#aaa authentication login default tacacs+ local
Foundry AP(config)#aaa console enable
Foundry AP(config)#aaa authorization exec default tacacs+
```

If you want to configure authorization, make sure you configure authorization on the server that provides AAA services. During TACACS+ authorization, the IronPoint access point expects the server to send a response containing an A-V (Attribute-Value) pair that specifies the privilege level of the user. When the IronPoint access point receives the response, it extracts an A-V pair configured for the Exec service and uses it to determine the user's privilege level.

To set a user's privilege level, you can configure the "foundry-privlvl" A-V pair for the Exec service on the TACACS+ server. For example:

```
user=bob {
  default service = permit
  member admin
  # Global password
  global = cleartext "cat"
  service = exec {
    foundry-privlvl = 0
  }
}
```

In this example, the A-V pair foundry-privlvl = 15 grants the user full read-write access. The value in the foundry-privlvl A-V pair is an integer that indicates the privilege level of the user. Possible values are 0- 14 for read-only privilege and 15 for admin, full read-write, privilege. The foundry-privlvl A-V pair can also be embedded in the group configuration for the user. See your TACACS+ documentation for the configuration syntax relevant to your server.

aaa authorization

This commands instructs the IronPoint access point to consult an AAA server to determine the privilege level of the authenticated user.

Syntax

```
aaa authorization exec default tacacs+
no aaa authorization exec default tacacs+
```

Default Setting

Disabled.

Command Mode

Global Configuration

Command Usage

- A server that provides AAA services must be identified in the IronPoint access point. That server must have the name and passwords of users who are allowed to log into the IronPoint access point, along with their privilege level.
- Authentication must be enabled. (See “Configuring TACACS+ Authentication” on page 16-7.)
- If authorization is not configured on the IronPoint access point, the user is placed into the “admin” privilege level of the CLI once the user’s login is authenticated. At the admin level, the user has full read and write access to the CLI.

If authorization is configured, the user is placed at either the “admin” privilege level or “read-only” privilege level, depending on the privilege level defined for that user.

Configuring TACACS+ Accounting

The commands below are used to enable AAA accounting on the IronPoint access point.

```
Foundry AP(config)#aaa authentication login default tacacs+ local
Foundry AP(config)#aaa console enable
Foundry AP(config)#aaa authorization exec default tacacs+
Foundry AP(config)#aaa accounting commands admin default start-stop tacacs+
```

aaa accounting

This command identifies which privilege level requires accounting services. When commands are entered at that privilege level, the IronPoint access point sends an accounting start packet that contains information about the commands entered by the user to the server that is providing the accounting service. When the accounting server acknowledges the accounting start packet, it records information about the commands.

When the user logs out, the IronPoint access point sends an accounting stop packet to the server that provides the accounting service. That server acknowledges the accounting stop packet and stops recording.

Syntax

aaa accounting commands admin | read-only default start-stop tacacs+
no aaa accounting commands admin | read-only default start-stop tacacs+

admin | read-only - Identify which privilege level requires accounting. Enter **admin** if all commands entered at the full, read-write privilege level are to be recorded in the accounting server. Enter **read-only** if commands entered at the read-only privilege level are to be recorded.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- A server that provides AAA services must be identified in the IronPoint access point.
- Authentication must be enabled on the access point if you want to use accounting.

show aaa

Use this command to display AAA information.

Syntax

show aaa

Default Setting

N/A

Command Mode

Global Configuration

Command Usage

See above.

Chapter 17

Intrusion Detection and Lockout

The Intrusion Detection and Lockout feature helps prevent unauthorized access to the network through the access point. This feature can be used if static WEP, pre-shared key, or 802.1X authentication types are used on the access point.

When the feature is enabled, wireless clients are given three cycles of login attempts to access the network. Each cycle has a number of login attempts that a client is allowed. There is a duration of time between each login cycle before the next cycle begins. If the client cannot log in during these login cycles, the login attempts return to the first cycle after a duration of time, or if the **permanently-block-intruder** feature is enabled, the wireless client's MAC address is permanently locked out from accessing the network. A network administrator must unlock the wireless client's MAC address in order for the wireless client to attempt any more logins.

NOTE: Intrusion Detection does not support WEP with open authentication.

This section presents the CLI commands to configure the Intrusion Detection and Lockout feature. There is no Web Management Interface equivalent for these commands.

Using the CLI

The following table lists the CLI commands used for the Intrusion Detection and Lockout feature.

Command	Function	Mode	Page
ids enable	Enables the Intrusion Detection and Lockout feature.	GC	17-3
ids 802.1x	Defines the number of attempts for each Intrusion and Detection cycle when 802.1X authentication is used to authenticate wireless clients.	GC	17-3
ids permanently-block-intruder	Enables the ability to permanently block login attempts that failed all login cycles	GC	17-4
ids pre-shared	Defines the number of attempts for each Intrusion and Detection cycle when pre-shared key authentication is used to authenticate wireless clients.	GC	17-4
ids static	Defines the number of attempts for each Intrusion and Detection cycle when static WEP authentication is used to authenticate wireless clients.	GC	17-4
ids station block	Locks or unlocks a MAC address	GC	17-5
ids timer	Defines the timers for a login cycle (cycle time) and for the delay between cycles (block time)	GC	17-5
show ids	Displays the definition of the parameters for the Intrusion Detection and Lockout feature	GC	17-6
show station ids-block	Displays the MAC addresses that have been blocked from the network	GC	17-6

The following example shows how to configure the Intrusion Detection and Lockout feature. The access point is configured to allow five login attempts in each of the three login cycles. The **ids cycle time** is configured for 60 seconds and **ids block time** is configured for 300 seconds. Each cycle lasts 60 seconds. There is a 300 second delay before the next cycle begins. Also the **permanently-block-intruder** feature is enabled on the access point.

Example

```
Foundry AP# configure
Foundry AP(config)# ids enable
Foundry AP(config)# ids 802.1x 1 5
Foundry AP(config)# ids 802.1x 2 5
Foundry AP(config)# ids 802.1x 3 5
Foundry AP(config)# ids pre-shared-key 1 5
Foundry AP(config)# ids pre-shared-key 2 5
Foundry AP(config)# ids pre-shared-key 3 5
Foundry AP(config)# ids static 1 5
Foundry AP(config)# ids static 2 5
Foundry AP(config)# ids static 3 5
Foundry AP(config)# ids permanently-block-intruder
Foundry AP(config)# ids station block 00e0.5201.0c72
Foundry AP(config)# ids timer block 300
Foundry AP(config)# ids timer cycle 60
```

A wireless client attempts to log in but his login fails. He tries to log in five times, but all his logins are unsuccessful. His MAC address is blocked from any further attempts for 300 seconds.

If the client tries to log in again after 300 seconds, the next login cycle starts. He has five additional login attempts during the second 60-second login cycle. If all these logins fail, his MAC address is blocked when his login attempts exceed five times, this time for another 300 seconds.

If after 300 seconds the client tries to log in again, the third cycle starts. He has another five attempts to log in during the third 60-second login cycle. If all of these attempts fail, his MAC address is permanently locked out when his login attempts exceed five times.

ids enable

This command enables the Intrusion Detection and Lockout feature.

Syntax

ids enable
no ids enable

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Use this command to enable the Intrusion Detection and Lockout feature. You can define intrusion detection parameters before you enable the feature on an access point.
- This feature works with static WEP, pre-shared key, and 802.1X authentication. Make sure one or more of the appropriate authentication method is configured on the access point.

ids 802.1x

This command sets the maximum number of login attempts for each login cycle if 802.1X authentication is used.

Syntax

ids 802.1x *<cycle-number>* *<number-attempts>*
no ids 802.1x

- *cycle-number* – The login number of the cycle you are configuring. Enter 1, 2, 3. There is no default cycle number.
- *number-attempts* – Enter a number for the maximum number of login attempts in the cycle being defined. Enter a number from 1 – 65535. However, if this value is set below 4, some client supplicants may say that this feature is not working, even though it is. To avoid this behavior, set the number of attempts per cycle to 4 or more.

Default Setting

5 attempts per cycle

Command Mode

Global Configuration

Command Usage

This command sets the maximum number of attempts for a login cycle on this access point, if 802.1X authentication is used. If you do not define a value for a cycle, then the default is used. Also, entering a **no ids 802.1x** resets the number of attempts to the default value.

Note: When a client is permanently blocked, then unblocked via the CLI, the CLI still sees the

client as permanently blocked until Cycle 1 of the next set of attempts expires.

ids permanently-block-intruder

Enables the ability to permanently block login attempts that failed all login cycles.

Syntax

ids permanently-block-intruder
no ids permanently-block-intruder

Default

Enabled

Command Mode

Global Configuration

Command Usage

Enable this command to permanently block MAC addresses that fail all login attempts in all the login cycles. Use the **no** form of the command to disable this feature.

ids pre-shared-key

This command sets the maximum number of login attempts for each login cycle if the pre-shared key authentication method is used.

Syntax

ids pre-shared-key *<cycle-number>* *<number-attempts>*
no ids pre-shared-key

- *cycle-number* – The login number of the cycle you are configuring. Enter 1, 2, 3. There is no default cycle number.
- *number-attempts* – Enter a number for the maximum number of login attempts in the cycle being defined. Enter a number from 1 – 65535. However, if this value is set below 4, some client supplicants may say that this feature is not working, even though it is. To avoid this behavior, set the number of attempts per cycle to 4 or more.

Default Setting

5 attempts per cycle

Command Mode

Global Configuration

Command Usage

This command sets the maximum number of attempts for a login cycle on this access point, if the pre-shared key authentication type is used. If you do not define a value for a cycle, the default is used. Also, entering a **no ids pre-shared-key** resets the number of attempts to the default value.

ids static

This command sets the maximum number of login attempts for each login cycle if the static WEP key authentication method is used.

Syntax

ids static *<cycle-number>* *<number-attempts>*
no ids static

- *cycle-number* – The login number of the cycle you are configuring. Enter 1, 2, 3. There is no default cycle number.

- *number-attempts* – Enter a number for the maximum number of login attempts in the cycle being defined. Enter a number from 1 – 65535. However, if this value is set below 4, some client supplicants may say that this feature is not working, even though it is. To avoid this behavior, set the number of attempts per cycle to 4 or more.

Default Setting

5 attempts per cycle

Command Mode

Global Configuration

Command Usage

This command sets the maximum number of attempts for a login cycle on this access point, if the static WEP key authentication method is used. If you do not define a value for a cycle, the default is used. Also, entering a **no ids static** resets the number of attempts to the default value.

ids station block

This command prevents wireless clients with the specified MAC addresses from logging into the access point. It also unlocks MAC addresses that have been permanently blocked from the access point because of failed login attempts.

Syntax

ids station block <mac-address>
no ids station

Enter the MAC address of the wireless client you want to block from this access point.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the **no** form of the command to unlock MAC addresses that have been permanently blocked from the access point due to failed login attempts.
- Use the command to block a MAC address from accessing the networking through the access point.

ids timer

This command defines the duration of time for a cycle and between cycles.

Syntax

ids timer cycle | block <seconds>
no ids timer cycle | block

- **cycle** – Specify *cycle* to define how long a login cycle last, then enter a number from 1 – 65535 seconds. The value you enter applies to all login cycles.
- **block** – Specify *block* to define the duration between cycles. Enter a number from 1 – 65535 seconds. The value you enter applies to all durations between login cycles.

Default Setting

- **cycle** – 60 seconds during the cycle
- **block** – 60 seconds between cycles

Command Mode

Global Configuration

Command Usage

If you do not enter a value for **cycle** or **block**, the default values are used. Also, entering a **no ids timer cycle** or **no ids timer block** command resets the parameter to the default value.

show ids

Shows the configuration for the Intrusion Detection and Lockout feature on the access point.

Syntax

show ids

Default Setting

Not applicable

Command Mode

Global Configuration

Command Usage

Use this command to display the definition of the Intrusion Detection and Lockout feature on this access point.

Example

```
Foundry AP# show ids

IDS Configuration:
=====
IDS: Disable
IDS: System Block Time: 30
IDS: System Cycle Time: 120
IDS: System Cycle Number: 3
IDS: System Max Number of Attempts for Key Type of 802.1X in Cycle 1: 5
IDS: System Max Number of Attempts for Key Type of 802.1X in Cycle 2: 5
IDS: System Max Number of Attempts for Key Type of 802.1X in Cycle 3: 5
IDS: System Max Number of Attempts for Key Type of Pre-Shared Key in Cycle 1: 3
IDS: System Max Number of Attempts for Key Type of Pre-Shared Key in Cycle 2: 3
IDS: System Max Number of Attempts for Key Type of Pre-Shared Key in Cycle 3: 3
IDS: System Max Number of Attempts for Key Type of Static WEP Key in Cycle 1: 2
IDS: System Max Number of Attempts for Key Type of Static WEP Key in Cycle 2: 2
IDS: System Max Number of Attempts for Key Type of Static WEP Key in Cycle 3: 2
IDS: System Permanently Block Intruder: False
Foundry AP
```

show station ids-block

This command displays the clients' ID and authentication related information for all traffic types. This information is captured as the client begins the login and before the client is granted access to the network. Once the client is granted access to the network, his or her information no longer appears in the report.

Syntax

show station ids-block

Default Setting

None

Command Mode

Global Configuration

Command Usage

Use this command to display which wireless clients have been blocked from accessing the network.

Example

```
Foundry AP#show station ids-block
Station Information:
=====
Station Address : 00-09-5B-94-2A-4C
Last Key Type : STATIC WEP
Ids Block (Manual): FALSE
Ids Block (Dynamic): TRUE
Remaining Ids Blocking Time after Cycle 3 : 4 seconds
Traps/syslogs:

Level: Information

IDS: real-time intrusion detection: enable
IDS: real-time intrusion detection: disable
IDS: real-time intrusion detection: STA: 00-09-5B-94-2A-4C last key type:
Static WEP/Pre-shared Key/802.1x is unlocked due to block timer expiring and moves
to Cycle 3.
"IDS: real-time intrusion detection: STA: 00-09-5B-94-2A-4C last key type:
Static WEP/Pre-shared Key/802.1x is locked due to the max #: 20 of attempts
in Cycle 2.
IDS: real-time intrusion detection: STA: 00-09-5B-94-2A-4C last key type:
Static WEP/Pre-shared Key/802.1x is unlocked manually and moves to Cycle 3.
```


Chapter 18

Bridging and Traffic Filter Settings

The access point can employ network traffic frame filtering to control access to network resources and increase security. You can prevent communications between wireless clients and prevent access point management from wireless clients. Also, you can block specific Ethernet traffic from being forwarded by the access point or specify an Ethernet type as management traffic.

Using the CLI

IAPP provides the protocol signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points. To enable IAPP for the access point, use the **iapp** command.

```
Foundry AP(config)#iapp
Foundry AP(config)#
```

Use the **filter local-bridge** command from the CLI configuration mode to prevent wireless-to-wireless communications through the access point. Use the **filter ap-manage** command to restrict management access from wireless clients.

```
Foundry AP(config)#filter local-bridge
Foundry AP(config)#filter ap-manage
Foundry AP(config)#
```

To configure Ethernet protocol filtering, use the **filter ethernet-type enable** command to enable filtering and the **filter ethernet-type protocol** command to specify defined protocols that you want to filter. To add a user-defined filter, use the **filter ethernet-type dynamic-protocol** command. To

filter an Ethernet protocol as management traffic, use the **filter ethernet-type management-only** command. To display the current settings, use the **show filters** command from the Exec mode.

```

Foundry AP(config)#filter ethernet-type protocol ARP
Foundry AP(config)#filter ethernet-type dynamic-protocol ipv6 86dd
Foundry AP(config)#filter ethernet-type management-only protocol airfortress
Foundry AP(config)#filter ethernet-type enable
Foundry AP(config)#exit
Foundry AP#show filters

Protocol Filter Information
=====
Local Bridge           :ENABLED
AP Management          :ENABLED
Ethernet Type Filter   :ENABLED

Enabled Protocol Filters
-----
Protocol: Airfortress           ISO: 0x8895 (Management-Only)
Protocol: ARP                   ISO: 0x0806
Protocol: ipv6                  ISO: 0x86dd (Dynamic)
=====
Foundry AP#

```

iapp

This command enables the protocol signaling required to hand over wireless clients roaming between different 802.11f-compliant access points. Use the **no** form to disable 802.11f signaling.

Syntax

iapp
no iapp

Default

Enabled

Command Mode

Global Configuration

Command Usage

The current 802.11 standard does not specify the signaling required between access points in order to support clients roaming from one access point to another. In particular, this can create a problem for clients roaming between access points from different vendors. This command is used to enable or disable 802.11f handover signaling between different access points.

Also, if you are using Layer 3 roaming, IAPP must be disabled on the access points.

filter local-bridge

If two or more clients are associated with an access point at the same time, this command determines if they are allowed to communicate with each other through the access point. Use the **no** form to disable this filtering.

Syntax

filter local-bridge
no filter local-bridge

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command can disable wireless-to-wireless communications between clients via the access point. However, it does not affect communications between wireless clients and the wired network.

filter ap-manage

This command prevents wireless clients from accessing the management interface on the access point. Use the **no** form to disable this filtering.

Syntax

filter ap-manage
no filter ap-manage

Default

Enabled

Command Mode

Global Configuration

filter ethernet-type enable

This command enables the checking of the Ethernet type on all incoming and outgoing Ethernet packets against the protocol filtering table. Use the **no** form to disable this feature.

If the Ethernet type is in the protocol filtering table and has been set to “filter” using the **filter ethernet-type protocol** command, the traffic is not allowed in or out of the access point. Other Ethernet types, either in the protocol filtering table or not, are allowed in or out of the access point.

Syntax

filter ethernet-type enable
no filter ethernet-type enable

Default

Disabled

Command Mode

Global Configuration

Command Usage

- This command is used in conjunction with the **filter ethernet-type protocol** command to determine which Ethernet protocol types are to be filtered.
- Ethernet protocol types not specified in the filtering table are always forwarded by the access point.

filter ethernet-type protocol

This command sets a specific Ethernet protocol type that is listed in the protocol table to be filtered from the access point. Use the **no** form to disable filtering for a specific Ethernet type.

Any traffic that matches the protocol types in the table that have been set to “filter” by this command are not forwarded by the access point. Other protocol types, either defined in the table or not, are allowed in and out the access point.

Syntax

filter ethernet-type protocol <protocol>
no filter ethernet-type protocol <protocol>

protocol - An Ethernet protocol type. (Options: Airfortress, Aironet-DDP, Appletalk-ARP, ARP, Banyan, Berkeley-Trailer-Neg, CDP, Cranite, DEC-LAT, DEC-MOP, DEC-MOP-Dump-Load, DEC-XNS, EAPOL, Enet-Config-Test, Ethertalk, IP, LAN-Test, NetBEUI, Novell-IPX(new), Novell-IPX(old), RARP, Telxon-TXP, X25-Level-3)

Default

None

Command Mode

Global Configuration

Command Usage

- Use the **filter ethernet-type enable** command to enable filtering for Ethernet types specified in the filtering table, or the **no filter ethernet-type enable** command to disable all filtering based on the filtering table.
- Ethernet protocol types not specified in the filtering table are always forwarded by the access point.

filter ethernet-type dynamic-protocol

This command defines a specific Ethernet protocol type that is not listed in the protocol table to be filtered from the access point. Use the **no** form to delete a specific Ethernet type.

Syntax

filter ethernet-type dynamic-protocol <filter-name><protocol-type>
no filter ethernet-type dynamic-protocol <filter-name>

- *filter-name* - A text name that identifies the filter. (Up to 31 alphanumeric characters.)
- *protocol-type* - A defined Ethernet protocol type to be filtered from the access point. (Range: 0x0000 - 0xFFFF)

Default

None

Command Mode

Global Configuration

Command Usage

- Up to four user-defined Ethernet type filters can be specified.
- Entering duplicate dynamic protocol names replaces the existing configuration.

filter ethernet-type management-only

This command sets Ethernet protocol filters to accept only management packets destined for the access point.

Syntax

filter ethernet-type management-only <**protocol** *protocol* | **dynamic-protocol** *filter-name* *protocol-type*>

- *protocol* - An Ethernet protocol type. (Options: Airtoss, Aironet-DDP, Appletalk-ARP, ARP, Banyan, Berkeley-Trailer-Neg, CDP, Cranite, DEC-LAT, DEC-MOP, DEC-MOP-Dump-Load, DEC-XNS, EAPOL, Enet-Config-Test, Ethertalk, IP, LAN-Test, NetBEUI, Novell-IPX(new), Novell-IPX(old), RARP, Telxon-TXP, X25-Level-3)
- *filter-name* - A text name that identifies the filter. (Up to 32 alphanumeric characters.)
- *protocol-type* - A defined Ethernet protocol type to be filtered from the access point. (Range: 0x0000 - 0xFFFF)

Default

None

Command Mode

Global Configuration

Command Usage

- When an Ethernet type filter is set as “management only,” received frames with a matching protocol type that are also destined for the access point are forwarded, otherwise the frames are discarded.
- The **filter ethernet-type management-only dynamic-protocol** command creates a user-defined filter and sets it as management only. Up to four user-defined Ethernet type filters can be specified.
- To disable an Ethernet protocol filter set to management only, use the **no filter ethernet-type protocol** or **no filter ethernet-type dynamic-protocol** commands.

show filters

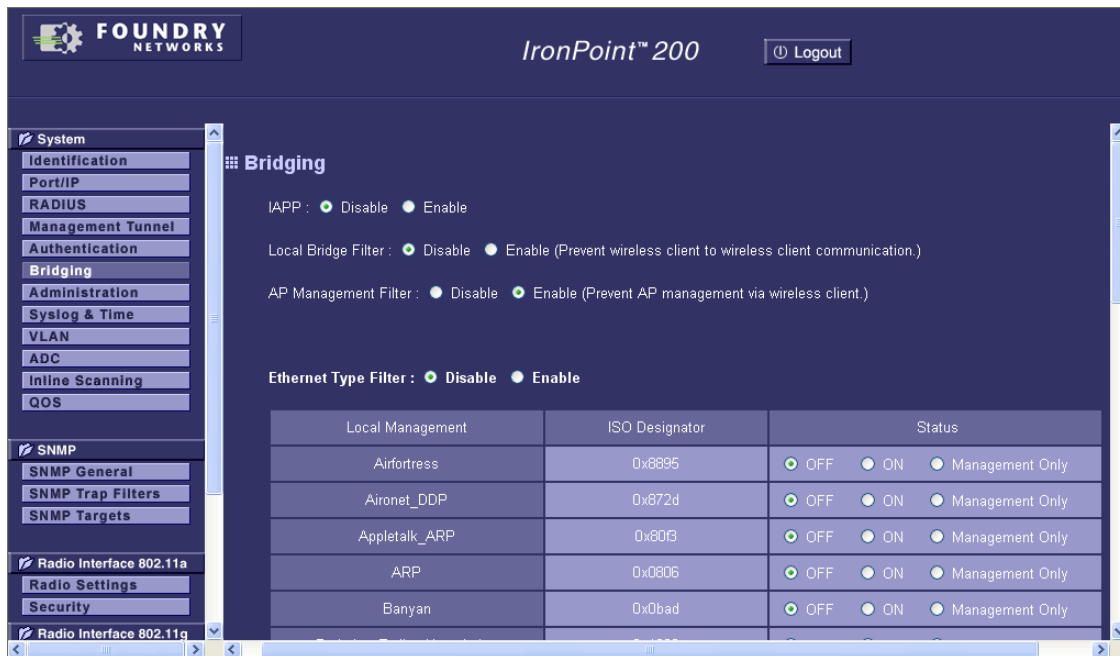
This command shows the filter options and protocol entries in the filter table.

Syntax**show filters****Command Mode**

Exec

Using the Web Management Interface

From the System menu, click Bridging. Enable local bridge or management filtering as required. If you want to filter certain types of Ethernet traffic, set Ethernet Type Filter to Enable and select the protocol types to filter from the Local Management list. If an Ethernet type is not included in the list, it can be defined as a dynamic protocol. Ethernet type filters can also be set as Management Only to accept only matching frames that are destined for the access point. Click Apply.



Configurable Parameters

IAPP – Enables or disables the Inter Access Point Protocol (IAPP) support on the access point. IAPP, or IEEE 802.11f, is a protocol that defines the required signaling to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points. (Default: Enable)

Note: IAPP must be set to Disable if you are using Wireless Mobility (Layer 3 roaming).

Local Bridge Filter – Controls wireless-to-wireless communications between clients through the access point. However, it does not affect communications between wireless clients and the wired network. (Default: Disable)

- **Disable:** Allows wireless-to-wireless communications between clients through the access point.
- **Enable:** Blocks wireless-to-wireless communications between clients through the access point.

AP Management Filter – Controls management access to the access point from wireless clients. Management interfaces include the Web, Telnet, or SNMP. (Default: Enable)

- **Disable:** Allows management access from wireless clients.
- **Enable:** Blocks management access from wireless clients.

Ethernet Type Filter – Controls checks on the Ethernet type of all incoming and outgoing Ethernet packets against the protocol filtering table. (Default: Disable)

- **Disable:** Access point does not filter Ethernet protocol types.
- **Enable:** Access point filters Ethernet protocol types based on the configuration of protocol types in the filter table. If a protocol has its status set to “ON,” the protocol is filtered from the access point. If a protocol is set to “Management Only,” the protocol filter accepts only matching frames that are destined for the access point.

Dynamic Protocol :
 Notice: If you choose the status to be OFF, the filter will be deleted from the table

Local Management	ISO Designator	Status
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> OFF <input type="radio"/> ON <input type="radio"/> Management Only
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> OFF <input type="radio"/> ON <input type="radio"/> Management Only
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> OFF <input type="radio"/> ON <input type="radio"/> Management Only
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> OFF <input type="radio"/> ON <input type="radio"/> Management Only

Buttons: Apply, Cancel, Help

Dynamic Protocol – Adds user-defined Ethernet-type filters to the protocol filtering table. Up to four user-defined Ethernet type filters can be specified.

- **Local Management:** A user-defined name that identifies the protocol. (Up to 32 alphanumeric characters.)
- **ISO Designator:** A defined Ethernet protocol type to be filtered from the access point. (Range: 0x0000 - 0xFFFF)
- **Status:** If a protocol has its status set to “ON,” the protocol is filtered from the access point. If a protocol is set to “Management Only,” the protocol filter accepts only matching frames that are destined for the access point. If the protocol status is set to “OFF,” the protocol type is deleted from the table.

Note: Ethernet protocol types not listed in the filtering table are always forwarded by the access point.

Chapter 19

Wireless Client Authentication

Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point (local authentication using MAC addresses), or by using a database configured on a central RADIUS server (remote authentication).

A client's MAC address provides relatively weak user authentication, since MAC addresses can be easily captured and used by another station to break into the network. Use MAC address authentication for a small network with a limited number of users.

Alternatively, authentication can be implemented using the IEEE 802.1x network access control protocol. Using 802.1x provides more robust user authentication using user names and passwords or digital certificates.

It is possible to configure the access point to use both local MAC addresses, remote MAC addresses, and 802.1x authentication, with client station authentication of MAC addresses occurring prior to 802.1x authentication. Before implementing authentication of MAC addresses or 802.1x authentication, consider the following guidelines:

- Local MAC addresses can be manually configured on the access point itself without the need to set up a RADIUS server. The access point supports up to 1000 MAC addresses in its filtering table, but managing a large number of MAC addresses across many access points is very cumbersome, since each access point must be configured with the same MAC address database.
- A RADIUS server can be used to centrally manage a larger database of user MAC addresses, however this requires more resources and knowledge to maintain and a RADIUS server would provide more security options supporting an 802.1x implementation.
- Use IEEE 802.1x authentication for networks with a larger number of users and where security is the most important issue. A RADIUS server is required in the wired network to control the user credentials (digital certificates, smart cards, passwords, or other) of wireless clients. The 802.1x authentication approach provides a standards-based, flexible, and scalable solution that can be centrally managed. Using 802.1x also provides a mechanism for enhanced network security using dynamic encryption key rotation or Wi-Fi Protected Access (WPA). However, implementing 802.1x requires more resources and skills to operate and maintain a RADIUS server and manage a large database of user credentials.

Note: If you choose to configure RADIUS MAC authentication together with 802.1x, the RADIUS MAC address authentication occurs prior to 802.1x authentication. Only when RADIUS MAC authentication succeeds is 802.1x authentication performed. When RADIUS MAC authentication

fails, 802.1x authentication is not performed.

Configuring MAC Address Authentication

To implement MAC address authentication, you must set up a database of client MAC addresses either locally on the access point or centrally on a configured RADIUS server.

Using the CLI

To configure local MAC authentication on the access point, use the **mac-authentication server** command from the CLI configuration mode to enable local MAC authentication. Set the default for MAC addresses not in the local table using the **address filter default** command, then enter MAC addresses in the local table using the **address filter entry** command. To remove an entry from the table, use the **address filter delete** command. To display the current settings, use the **show authentication** command from the Exec mode.

```

Foundry AP(config)#mac-authentication server local
Foundry AP(config)#address filter default denied
Foundry AP(config)#address filter entry 00-70-50-cc-99-1a denied
Foundry AP(config)#address filter entry 00-70-50-cc-99-1b allowed
Foundry AP(config)#address filter entry 00-70-50-cc-99-1c allowed
Foundry AP(config)#address filter delete 00-70-50-cc-99-1c
Foundry AP(config)#exit
Foundry AP#show authentication

Authentication Information
=====
MAC Authentication Server      : LOCAL
MAC Auth Session Timeout Value : 5 min
802.1x supplicant             : DISABLED
802.1x supplicant user        : ****
802.1x supplicant password    : ****
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address      Status
-----
00-70-50-cc-99-1a  DENIED
00-70-50-cc-99-1b  ALLOWED
=====
Foundry AP#

```

To configure RADIUS MAC authentication on the access point, use the **mac-authentication server** command from the CLI configuration mode to enable remote MAC authentication. Set the timeout value for re-authentication using the **mac-authentication session-timeout** command. Be sure to

also configure connection settings for the RADIUS server (not shown in the following example). To display the current settings, use the **show authentication** command from the Exec mode.

```

Foundry AP(config)#mac-authentication server remote
Foundry AP(config)#mac-authentication session-timeout 5
Foundry AP(config)#exit
Foundry AP#show authentication

Authentication Information
=====
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 5 min
802.1x supplicant             : DISABLED
802.1x supplicant user        : ****
802.1x supplicant password    : ****
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address      Status
-----
00-70-50-cc-99-1a  DENIED
00-70-50-cc-99-1b  ALLOWED
=====
Foundry AP#

```

address filter default

This command sets filtering to allow or deny listed MAC addresses.

Syntax

address filter default <allowed | denied>

- **allowed** - Only MAC addresses entered as “allowed” in the address filtering table are denied.
- **denied** - Only MAC addresses entered as “denied” in the address filtering table are allowed.

Default

allowed

Command Mode

Global Configuration

address filter entry

This command enters a MAC address in the filter table.

Syntax

address filter entry <mac-address> <allowed | denied>

- *mac-address* - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens; e.g., 00-90-D1-12-AB-89.)
- **allowed** - Entry is allowed access.
- **denied** - Entry is denied access.

Default

None

Command Mode

Global Configuration

Command Mode

- The access point supports up to 1000 MAC addresses.
- An entry in the address table may be allowed or denied access, depending on the global setting configured for the **address entry default** command.

address filter delete

This command deletes a MAC address from the filter table.

Syntax

address filter delete <mac-address> | all

mac-address - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens.)

all - use this keyword to delete all MAC addresses from the filter table.

Default

None

Command Mode

Global Configuration

mac-authentication server

This command sets address filtering to be performed using the local MAC address database or using a database configured on a central RADIUS server. Use the **no** form to disable MAC address authentication.

Syntax

mac-authentication server [local | remote]

- **local** - Authenticate the MAC address of wireless clients with the local MAC address database during 802.11 association. If this argument is entered, all access points in the wireless realm must be configured with the same MAC addresses to be filtered.
- **remote** - Authenticate the MAC address of wireless clients with a MAC address database on a RADIUS server. If this argument is entered, the list of MAC addresses must be defined in the RADIUS server.

Default

local

Command Mode

Global Configuration

mac-authentication session-timeout

This command sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database. Use the **no** form to disable reauthentication.

Syntax

mac-authentication session-timeout <minutes>

minutes - Re-authentication interval. (Range: 0-1440)

Default

0 (disabled)

Command Mode

Global Configuration

show authentication

This command shows all 802.1x authentication settings, as well as the address filter table.

Syntax

show authentication

Command Mode

Exec

Using the Web Management Interface

From the System menu, click Authentication. If you want to use MAC Authentication, select Local MAC or Radius MAC from the drop-down list. For Local MAC authentication, enter the MAC addresses in the provided text field and set the appropriate permission. For Radius MAC authentication, a configured RADIUS server must be available on the network and the connection settings entered on the RADIUS page of the Web interface. Click Apply.

The screenshot displays the Foundry Networks IronPoint 200 web management interface. The left sidebar contains a navigation menu with the following items: System, Identification, Port/IP, RADIUS, Management Tunnel, Authentication (selected), Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP, SNMP General, SNMP Trap Filters, SNMP Targets, Radio Interface 802.11a, Radio Settings, Security, and Radio Interface 802.11g. The main content area is titled 'Authentication' and includes the following sections:

- 802.1x Supplicant:** A section with a 'Supplicant' label and an 'Enable' checkbox.
- Local MAC Selection:** A section with a 'MAC Authentication' dropdown menu set to 'Local MAC' and a 'MAC Authentication Session Timeout (0-1440)' field set to '0' minutes.
- Local MAC Authentication:** A section with a 'System Default' radio button group showing 'Deny' and 'Allow' (selected).
- MAC Authentication Settings:** A table with three columns: 'MAC Address', 'Permission', and 'Update'. The 'Permission' column has radio buttons for 'Deny', 'Allow' (selected), and 'Delete'. An 'Update' button is located at the bottom right of the table.

Below the table, the text 'MAC Authentication Table:' is visible.

Configurable Parameters

MAC Authentication – You can configure a list of the MAC addresses for wireless clients that are authorized to access the network. This provides a basic level of authentication for wireless clients attempting to gain access to the network. A database of authorized MAC addresses can be stored locally on the access point or remotely on a central RADIUS server.

(Default: Local MAC)

- **Disable:** No checks are performed on an associating station's MAC address.
- **Local MAC:** The MAC address of the associating station is compared against the local database stored on the access point. The Local MAC Authentication section enables the local database to be set up. If this option is selected, all access points in the wireless network service area must be configured with the same MAC address database.
- **Radius MAC:** The MAC address of the associating station is sent to a configured RADIUS server for authentication. When using a RADIUS authentication server for MAC address authentication, the server must first be configured in the RADIUS Web page (See "RADIUS Client Settings" on page 15-1.). If this option is selected, the database of MAC addresses and filtering policy must be defined in the RADIUS server.

MAC Authentication Session Timeout – sets the interval at which associated clients will be re-authenticated with the RADIUS server. (Range: 0-1440 minutes; Default: 0, disabled)

Local MAC Authentication – Configures the local MAC authentication database. The MAC database provides a mechanism to take certain actions based on a wireless client's MAC address. The MAC list can be configured to allow or deny network access to specific clients.

- **System Default:** Specifies a default action for all unknown MAC addresses (that is, those not listed in the local MAC database).
 - **Deny:** Blocks access for all MAC addresses except those listed in the local database as "allowed."
 - **Allow:** Permits access for all MAC addresses except those listed in the local database as "denied."
- **MAC Authentication Settings:** Enters specified MAC addresses and permissions into the local MAC database.
 - **MAC Address:** Physical address of a client. Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-D1-12-AB-89.
 - **Permission:** Select Allow to permit access or Deny to block access. If Delete is selected, the specified MAC address entry is removed from the database.
 - **Update:** Enters the specified MAC address and permission setting into the local database.
- **MAC Authentication Table:** Displays current entries in the local MAC database.

Note: The access point supports up to 1000 MAC addresses.

Configuring 802.1x Client Authentication

The 802.1x standard provides a framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1x client application to submit user credentials for authentication. The 802.1x standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the access point grants client access to the network.

The 802.1x EAP packets are also used to pass dynamic unicast session keys and static broadcast keys to wireless clients. Session keys are unique to each client and are used to encrypt and correlate traffic passing between a specific client and the access point. You can also enable broadcast key rotation, so the access point provides a dynamic broadcast key and changes it at a specified interval.

Using the CLI

Client authentication using 802.1x is configurable separately for each VAP interface. To configure 802.1x authentication on a VAP interface, from the CLI wireless interface configuration mode, first use the **vap** command to access VAP interface configuration. Use the **802.1x supported** command to enable 802.1x authentication. Set the session and broadcast key refresh rate, and the re-authentication timeout. To display the current settings, use the **show interface wireless** command from the Exec mode (not shown in the following example).

```
Foundry AP(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless g: VAP[0])#802.1x supported
Foundry AP(if-wireless g: VAP[0])#802.1x broadcast-key-refresh-rate 100
Foundry AP(if-wireless g: VAP[0])#802.1x session-timeout 5
Foundry AP(if-wireless g: VAP[0])#
```

802.1x

This command configures 802.1x as optionally supported or as required for wireless clients. Use the **no** form to disable 802.1x support.

Syntax

802.1x <supported | required>

no 802.1x

- **supported** - Authenticates clients that initiate the 802.1x authentication process. Uses standard 802.11 authentication for all others.
- **required** - Requires 802.1x authentication for all clients.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- When 802.1x is disabled, the VAP interface does not support 802.1x authentication for any station. After successful 802.11 association, each client is allowed to access the network.
- When 802.1x is supported, the VAP interface supports 802.1x authentication only for clients initiating the 802.1x authentication process (i.e., the access point does NOT initiate 802.1x authentication). For stations initiating 802.1x, only those stations successfully authenticated are allowed to access the network. For those stations not initiating 802.1x, access to the network is allowed after successful 802.11 association.
- When 802.1x is required, the VAP interface enforces 802.1x authentication for all 802.11 associated stations. If 802.1x authentication is not initiated by the station, the access point will initiate authentication. Only those stations successfully authenticated with 802.1x are allowed to access the network.
- 802.1x does not apply to the 10/100Base-TX port.
- When Layer 3 roaming is configured on an IronPoint-FES and static WEP clients are allowed to connect to an IronPoint access point using DHCP, make sure 802.1X is configured as "disabled" on each VAP of the access point.

802.1x broadcast-key-refresh-rate

This command sets the interval at which the broadcast keys are refreshed for stations using 802.1x dynamic keying.

Syntax

802.1x broadcast-key-refresh-rate <rate>

rate - The interval at which broadcast encryption keys are changed for the VAP interface.
(Range: 0 (disabled), 60 - 1440 minutes)

Default Setting

120 minutes

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- The access point uses EAPOL (Extensible Authentication Protocol Over LANs) packets to pass dynamic unicast session and broadcast keys to wireless clients. The 802.1x **broadcast-key-refresh-rate** command specifies the interval after which the broadcast keys are changed. The **802.1x session-key-refresh-rate** command specifies the interval after which unicast session keys are changed.
- Dynamic broadcast key rotation allows the access point to generate a random group key and periodically update all key-management capable wireless clients.

802.1x session-timeout

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form to disable 802.1x re-authentication.

Syntax

802.1x session-timeout <minutes>

no 802.1x session-timeout

minutes - The number of minutes. (Range: 0 (disabled), 60 - 1440 minutes)

Default

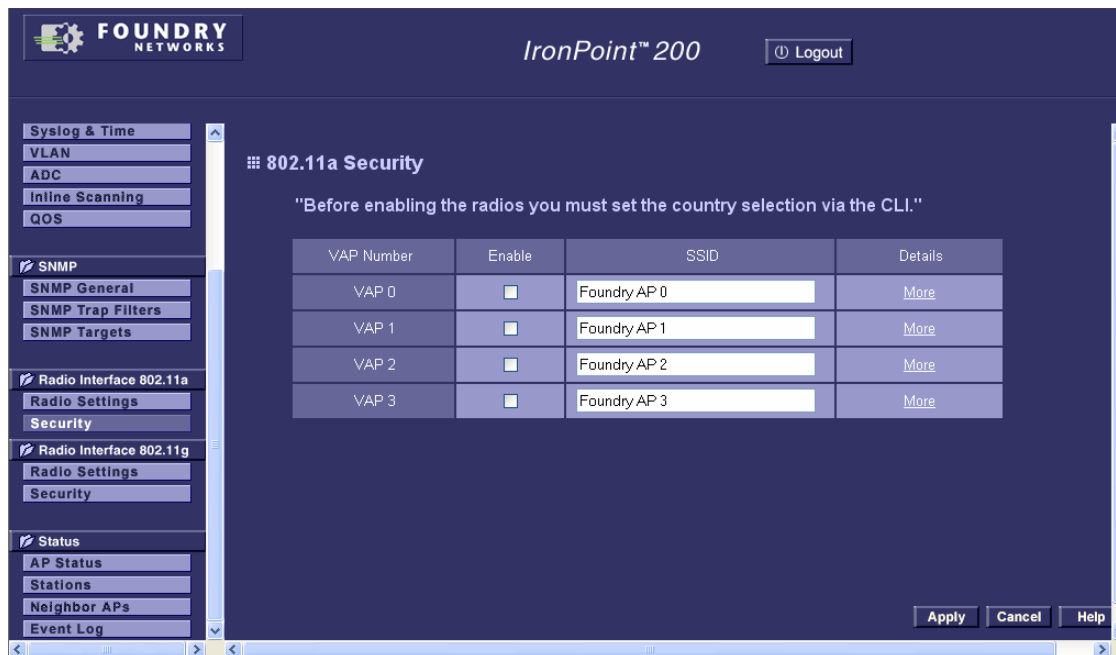
0 (Disabled)

Command Mode

Interface Configuration (Wireless-VAP)

Using the Web Management Interface

From the Radio Interface 802.11a menu or the Radio 802.11g menu, click Security.



For the VAP interface using 802.1x, click More.



Under 802.1x Setup, select Supported or Required and enter appropriate refresh rates for broadcast and session keys, and for re-authentication. Click Apply.

A RADIUS server is required for 802.1x implementation, make sure to enter the connection settings on the RADIUS page of the Web interface.

Configurable Parameters

802.1x Setup – You can enable 802.1x as optionally supported or as required to enhance the security of the wireless network. When 802.1x is enabled, the broadcast and session key rotation intervals can also be configured for the VAP interface. (Default: Disable)

- **Disable:** The VAP interface does not support 802.1x authentication for any wireless client. After successful wireless association with the access point, each client is allowed to access the network.
- **Supported:** The VAP interface supports 802.1x authentication only for clients initiating the 802.1x authentication process (the access point does not initiate 802.1x authentication). For clients initiating 802.1x, only those successfully authenticated are allowed to access the network. For those clients not initiating 802.1x, access to the network is allowed after successful wireless association with the access point.
- **Required:** The VAP interface enforces 802.1x authentication for all associated wireless clients. If 802.1x authentication is not initiated by a client, the access point will initiate authentication. Only those clients successfully authenticated with 802.1x are allowed to access the network.
- **Broadcast Key Refresh Rate:** If 802.1x is set to Supported or Required, sets the interval at which the broadcast keys are refreshed for stations using 802.1x dynamic keying. (Range: 0, 60-1440 minutes; 0 means disabled. Default: 120 minutes)

- **802.1x Re-authentication Refresh Rate:** If 802.1x is set to Supported or Required, sets the time period after which a connected client must be re-authenticated. During the re-authentication process of verifying the client's credentials on the RADIUS server, the client remains connected the network. Only if re-authentication fails is network access blocked. (Range: 0, 60-1440 minutes; Default: 0 means disabled)

Configuring 802.1x Supplicant Authentication

The access point can also operate in a 802.1x supplicant mode. This enables the access point itself to be authenticated with a RADIUS server using a configured MD5 user name and password. This prevents rogue access points from gaining access to the network.

Using the CLI

To configure the access point to operate as a 802.1x supplicant, first use the **802.1x supplicant user** command to set a user name and password for the access point, then use the **802.1x supplicant** command to enable the feature. To display the current settings, use the **show authentication** command from the Exec mode (not shown in the following example).

```
Foundry AP(config)#802.1x supplicant user ip200 ironpoint
Foundry AP(config)#802.1x supplicant
Foundry AP(config)#
```

802.1x supplicant user

This command sets the user name and password used for authentication of the access point when operating as a 802.1x supplicant. Use the **no** form to clear the supplicant user name and password.

Syntax

802.1x supplicant user <username> <password>

no 802.1x supplicant user

- *username* - The access point name used for authentication to the network. (Range: 1-32 alphanumeric characters)
- *password* - The MD5 password used for access point authentication. (Range: 1-32 alphanumeric characters)

Default

None

Command Mode

Global Configuration

Command Usage

The access point currently only supports EAP-MD5 CHAP for 802.1x authentication.

802.1x supplicant

This command enables the access point to operate as an 802.1x supplicant for authentication. Use the **no** form to disable 802.1x authentication of the access point.

Syntax

802.1x supplicant
no 802.1x supplicant

Default

Disabled

Command Mode

Global Configuration

Command Usage

A user name and password must be configured first before the 802.1x supplicant feature can be enabled.

Using the Web Management Interface

If you want the access point to be authenticated, click Authentication on the System menu. Enable the 802.1x Supplicant feature and configure a user name and password. Click Apply.

The screenshot shows the Foundry IronPoint 200 Web Management Interface. The left sidebar contains a menu with the following items: System, Identification, Port/IP, RADIUS, Management Tunnel, Authentication (selected), Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP, SNMP General, SNMP Trap Filters, SNMP Targets, Radio Interface 802.11a, Radio Settings, Security, and Radio Interface 802.11g. The main content area is titled 'Authentication' and contains the following sections:

- 802.1x Supplicant**: A table with four rows: 'Supplicant' with a checked 'Enable' checkbox, 'Username' with a text input field, 'Password' with a text input field, and 'Confirm password' with a text input field.
- Local MAC Selection**: A section with 'MAC Authentication' set to 'Local MAC' (via a dropdown), 'MAC Authentication Session Timeout (0-1440)' set to '0' minutes, and 'Local MAC Authentication' with 'System Default' set to 'Allow' (radio buttons for Deny and Allow).
- MAC Authentication Settings**: A section with a label 'MAC Authentication Settings:' followed by a list of settings (not fully visible).

Configurable Parameters

802.1x Supplicant – Enables the access point to be authenticated with a RADIUS server. If enabled, a user name and password must be configured. (Default: Disable)

- **Username:** The authentication name used for the access point, as configured on the RADIUS server. (Range: 1-32 alphanumeric characters)

- **Password:** The MD5 password used in the authentication process. (Range: 1-32 alphanumeric characters)

Chapter 20

Ethernet Interface Configuration

The CLI commands described in this section configure connection parameters for the access point's Ethernet interface.

Using the CLI

The following table provides a summary of the CLI commands in this section.

Command	Function	Mode	Page
rate-limit	Limits the rate at which broadcast or multicast packets are received on Ethernet interfaces	IC-E	20-2
shutdown	Disables the Ethernet interface	IC-E	20-2
speed-duplex	Configures speed and duplex operation	IC-E	20-3
show interface ethernet	Shows the status for the Ethernet interface	Exec	20-3

The following example shows how to enable the 10/100Base-TX network interface, set the port to 100 Mbps and half-duplex operation.

```
Foundry AP(config)#interface ethernet
Foundry AP(if-ethernet)#no shutdown
Foundry AP(if-ethernet)#speed-duplex 100-half
Foundry AP(if-ethernet)#rate-limit broadcast
aggressive
Foundry AP(if-ethernet)#end
```

Use the **show interface ethernet** command to display the current status of the interface.

On an IronPoint 200, the **show interface ethernet** displays the following information.

```

Foundry AP#show interface ethernet

Ethernet Interface Information
=====
MAC Address           : 00-0C-DB-81-40-93
IP Address            : 192.168.1.2
Subnet Mask           : 255.255.255.0
Default Gateway       : 192.168.1.254
Primary DNS           : 192.168.1.55
Secondary DNS         : 10.1.0.55
Speed-duplex Actual   : 100Base-TX Half Duplex
Speed-duplex Configured : 100Base-TX Half Duplex
Admin status          : Up
Operational status    : Up
Broadcast Rate Limit   : Aggressive
Multicast Rate Limit   : Conservative
=====
Foundry AP#

```

rate-limit

This command allows you to limit the rate at which broadcast or multicast frames are accepted by the access point from the Ethernet interface. When this command is configured, the access point monitors the rate at which the specified frame type is received. If the rate is less than the specified rate, frames are accepted. Once the specified frame rate is reached, subsequent frames received during that second are dropped.

Syntax

```

rate-limit <broadcast | multicast> <aggressive | normal | conservative>
no rate-limit <broadcast | multicast>

```

- **aggressive** - Allow only 10 frames per second
- **normal** - Allow only 25 frames per second
- **conservative** - Allow only 50 frames per second

Default Setting

broadcast: conservative

multicast: normal

Command Mode

Interface Configuration (Ethernet)

Command Usage

Configure separate rate limiting for broadcast and multicast packets.

shutdown

This command disables the Ethernet interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

Interface enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command allows you to disable the Ethernet port due to abnormal behavior (e.g., excessive collisions), and reenables it after the problem has been resolved. You may also want to disable the Ethernet port for security reasons.

speed-duplex

This command configures the speed and duplex mode of the access point's Ethernet port. Use the **no** form to restore the default.

Syntax

speed-duplex <auto | 10-half | 10-full | 100-half | 100-full>

- **auto** - Enables autonegotiation to set the speed and duplex mode
- **10-half** - Forces 10 Mbps, half-duplex operation
- **10-full** - Forces 10 Mbps, full-duplex operation
- **100-half** - Forces 100 Mbps, half-duplex operation
- **100-full** - Forces 100 Mbps, full-duplex operation

Default Setting

Autonegotiation

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When the Ethernet port is set to **auto** (the default), autonegotiation is enabled and the speed and duplex mode are automatically set to match the connected device.
- If the device connected to the Ethernet port does not support autonegotiation or is forced to a specific speed and duplex mode, the access point's Ethernet port must be manually configured to match the settings.
- When the Ethernet port is forced to a specific speed and duplex mode, autonegotiation is disabled.

show interface ethernet

This command displays the status for the Ethernet interface.

Syntax

show interface [ethernet]

Default Setting

Ethernet interface

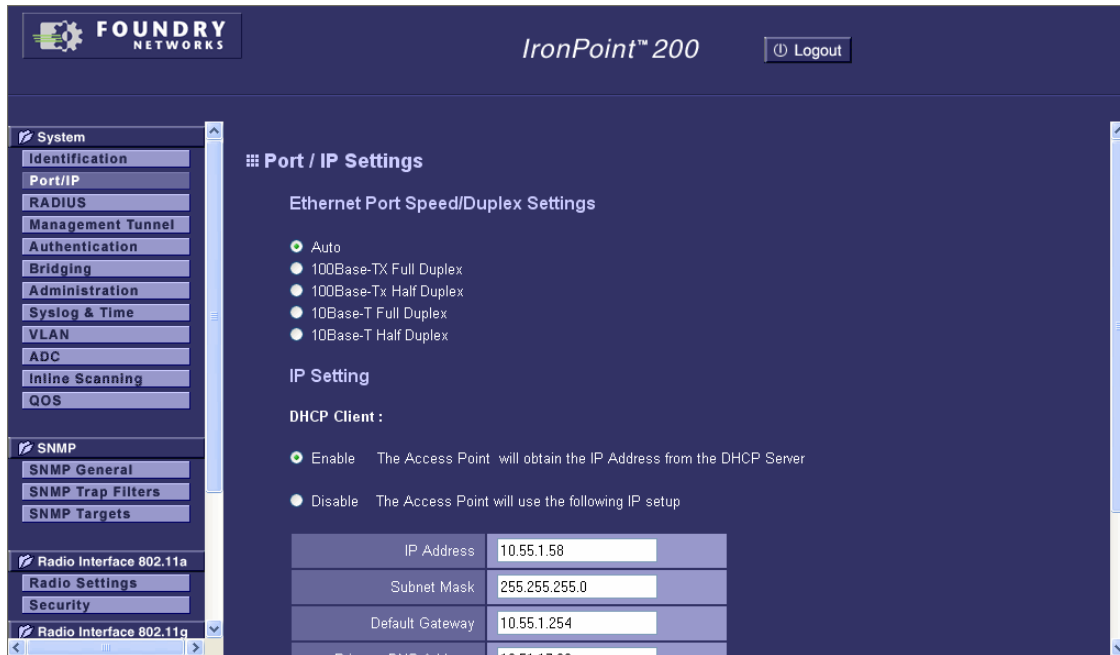
Command Mode

Exec

Command Usage

Using the Web Management Interface

From the System menu, click Port/IP. Select the speed and duplex mode setting to match that of the connected device, or select autonegotiation. Click Apply.



Configurable Parameters

Auto – Enables autonegotiation to set the speed and duplex mode of the access point's Ethernet port. (Default: Enabled)

100Base-TX Full Duplex – Disables autonegotiation and forces the Ethernet port to operate at 100 Mbps full-duplex mode.

100Base-TX Half Duplex – Disables autonegotiation and forces the Ethernet port to operate at 100 Mbps half-duplex mode.

10Base-T Full Duplex – Disables autonegotiation and forces the Ethernet port to operate at 10 Mbps full-duplex mode.

10Base-T Half Duplex – Disables autonegotiation and forces the Ethernet port to operate at 10 Mbps half-duplex mode.

Chapter 21

Radio Interface Configuration

The IEEE 802.11a and 802.11g interfaces include configuration options for radio signal characteristics and wireless security features. The configuration options for radio parameters are nearly identical and are both covered in this section.

The access point can operate in three modes, IEEE 802.11a only, 802.11b/g only, or a mixed 802.11a/b/g mode. Also note that 802.11g is backward compatible with 802.11b.

A physical radio interface on an access point can be configured with up to four *virtual access points* (VAP). Each VAP functions as a separate access point. Wireless clients can associate with these access points in the same way they associate with a physical access point.

A VAP functions like a VLAN. Each VAP can be matched with a VLAN ID. You can separate traffic to the access point using VAP (for example, voice traffic on one VAP while data traffic goes on another VAP). You can also apply different wireless security methods on each VAP without having to purchase additional access points.

You can configure up to four VAP per radio, numbered 0 to 3. Each VAP interface can be configured to have its own Service Set Identification (SSID) and security settings. Each VAP can have up to 64 wireless clients.

Note: The radio channel settings for the access point are limited by local regulations, which determine the number of channels that are available. This user guide shows channels and settings that apply to United States and Canada with 13 channels available for the 802.11a interface and 11 channels for the 802.11g interface. Other regions may have different channels and settings available.

You can configure access points to automatically select a channel and transmission power for its radios. This new feature will aid in deploying multiple access points without the need to configure channel and transmit power for each access point. The access point will then select the least used channel and the appropriate transmit power and help prevent channel overlap and interference. The feature also allows you to configure how often an access point scans the airwaves to see if channel selection and transmit power need to be adjusted.

Configuring Radio Settings (802.11a)

The IEEE 802.11a radio operates within the 5 GHz band, at up to 54 Mbps in normal mode or up to 108 Mbps in Turbo mode.

The 802.11a radio supports four VAP interfaces, each VAP is defined by its SSID. You should set an SSID to identify the wireless network service provided by the VAP. Only clients with the same SSID can associate with the VAP.

Note: You must first enable VAP interface 0 before you can enable VAP interfaces 1, 2, or 3.

Using the CLI

From the CLI configuration mode, use the **interface wireless a** command to access the interface mode for the 802.11a radio. From the 802.11a interface mode, you can access radio settings that apply to all VAP interfaces. Use the **turbo** command to enable this feature before setting the radio channel with the **channel** command. To access each VAP interface (numbered 0 to 3), use the **vap** command. You should set each VAP interface SSID using the **ssid** command and, if required, configure a name for each interface using the **description** command. Set any other parameters as required before enabling the VAP interface with the **no shutdown** command.

```
Foundry AP(config)#interface wireless a
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless a)#turbo
Foundry AP(if-wireless a)#channel 42
Foundry AP(if-wireless a)#speed 54
Foundry AP(if-wireless a)#multicast-data-rate 6
Foundry AP(if-wireless a)#beacon-interval 150
Foundry AP(if-wireless a)#dtim-period 5
Foundry AP(if-wireless a)#fragmentation-length 512
Foundry AP(if-wireless a)#rts-threshold 256
Foundry AP(if-wireless a)#transmit-power half
Foundry AP(if-wireless a)#datarate-based-access 6
Foundry AP(if-wireless a)#rssi-based-access 4
Foundry AP(if-wireless a)#vap 0
Foundry AP(if-wireless a: VAP[0])#description IP-VAP0
Foundry AP(if-wireless a: VAP[0])#ssid ironpoint-vap0
Foundry AP(if-wireless a: VAP[0])#association-timeout-interval 20
Foundry AP(if-wireless a: VAP[0])#authentication-timeout-interval 30
Foundry AP(if-wireless a: VAP[0])#max-association 32
Foundry AP(if-wireless a: VAP[0])#closed-system
Foundry AP(if-wireless a: VAP[0])#no shutdown
Foundry AP(if-wireless a: VAP[0])#
```

To configure automatic channel and transmission power selection, enter the following commands:

```
Foundry AP(config)#interface wireless a
Foundry AP(if-wireless a)#channel auto
Foundry AP(if-wireless a)#auto-refresh-rate 1440
Foundry AP(if-wireless a)#transmit-power auto
```


To view the current 802.11a radio settings for the VAP interface, use the **show interface wireless a** command.

```

Foundry AP#show interface wireless g 0
Wireless Interface G VAP 0 Information
=====
-----Identification-----
Description                : Foundry 802.11g Access Point
SSID                      : Foundry AP 0
BSSID                    : 00-12-F2-E8-AE-88
Channel                  : 11 (AUTO)
Status                   : Disabled
----- Auto Channel Selection & Transmit Power Control Parameters -----
Auto Refresh Interval      : 1440 min.
Auto Channel Selection Mode : NON_OVERLAP
Auto Transmit Power Control : Disabled
-----802.11 Parameters-----
Radio Mode                 : 802.11b+g
Transmit Power             : FULL (16 dBm)
Max Station Data Rate      : 54Mbps
Multicast Data Rate        : 1Mbps
Fragmentation Threshold    : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval            : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval : 30 Mins
DTIM Interval              : 1 beacon
Preamble Length            : SHORT-OR-LONG
Maximum Association        : 64 stations
VLAN ID                   : 1
Load Balance               : Disabled
SSID Prioritization Threshold : 0
Priority Level              : Low
RSSI Based Access          : 4
Data Rate Based Access     : 5.5 Mbps
-----Security-----
Closed System              : Disabled
WPA clients                : Disabled
WPA Key Mgmt Mode          : PRE SHARED KEY
WPA PSK Key Type           : PASSPHRASE
PMKSA Lifetime             : 720 minutes
Encryption                 : Disabled
WEP Key Length             : None
Default Transmit Key       : 1
WEP Key Type               : Key 1: HEX      Key 2: HEX
                           : Key 3: HEX      Key 4: HEX
Common Static Keys         : Key 1: EMPTY   Key 2: EMPTY
                           : Key 3: EMPTY   Key 4: EMPTY
Authentication Type        : OPEN
-----Antenna-----
Antenna Control method     : Full diversity
Antenna ID                 : Integrated
-----Authentication Parameters-----
802.1x                     : Disabled
Broadcast Key Refresh Rate : 120 min
802.1x Session Timeout Value : 0 min
Pre-Authentication         : Disabled
=====

```

antenna

This command selects the built-in antennas or an optional high-gain antenna attached to the socket on the right antenna.

Syntax

antenna <type | diversity | location>

- **type** - Selects the antenna to be used by the access point
 - For Radio a, select one of the following:
 - **id = 0x0000, Module** - Foundry integrated Antenna
 - **id = 0x0100, Module** - Foundry external 2.4GHz (6dBi) and 5GHz (8dBi) dual bands, Omnidirectional Antenna
 - For Radio b/g, select one of the following:
 - **id = 0x0000, Module** - Foundry integrated Antenna
 - **id = 0x0100, Module** - Foundry external 2.4GHz (6dBi) and 5GHz (8dBi) dual bands, Omnidirectional Antenna
 - **id = 0x0101, Module** - Foundry external 2.4GHz (4dBi) single band, Bi-Directional Antenna
 - **id = 0x0102, Module** - Foundry external 2.4GHz (13dBi) single band Directional Panel Antenna
- **diversity** - Selects the antenna diversity to use.
 - **full** - Selects the built-in diversity antennas. The transmitted signal is sent out both antennas, and the antenna with the best incoming signal is used for reception.
 - **fixed_A** - The right antenna is used both for transmission and reception. Use this setting when an optional high-gain antenna is attached to the access point.
- **location** - Selects the mounting location of the antenna in use; either “Indoor” or “Outdoor.”

Default Setting

Type: Integrated
 Diversity: Full
 Location: Indoor

Command Mode

Interface Configuration (Wireless)

Command Usage

Only the 802.11a interface supports the **location** setting. The 802.11g interface is fixed at “Indoor” and is not configurable.

association-timeout-interval

This command configures the idle time interval (when no frames are sent) after which the client is disassociated from the VAP interface.

Syntax

association-timeout-interval <minutes>

minutes - The number of minutes of inactivity before disassociation. (Range: 5-60)

Default Setting

30

Command Mode

Interface Configuration (Wireless-VAP)

authentication-timeout-interval

This command configures the time interval after which clients must be re-authenticated to access the VAP interface.

Syntax**authentication-timeout-interval** <minutes>*minutes* - The number of minutes before re-authentication. (Range: 5-60)**Default Setting**

60

Command Mode

Interface Configuration (Wireless-VAP)

auto-refresh-rate

This command sets the scan interval for a radio. At the specified interval, the access point scans the airwaves and collects beacons from nearby access points to select a channel. If there is no nearby access point, the access point does not collect any beacons, but randomly selects a channel as follows:

- On the 802.11a radio, the access point selects any channel.
- On the 802.11b/g radio, the access point selects one of the three non-overlapping channels: 1, 6, or 11

If there are adjacent access points and the access points collect beacons, the access point selects the least congested channel based on the RSSI.

The access point selects the appropriate transmit power based on the RSSI value of an access point on the same and adjacent channels.

Syntax**auto-refresh-rate** <minutes>*minutes* - The number of minutes a radio waits before it starts the next scan.
(Range: 0, 180 – 10080 minutes. Use 0 to disable this feature.)**Default Setting**

1440

Command ModeInterface Configuration (Wireless - 802.11a)
Interface Configuration (Wireless - 802.11b/g)**Command Usage**

Use the **channel auto** command to enable automatic channel selection on the radio. Once automatic channel selection is enabled, the radio scan the airwaves at the interval specified by the **auto-refresh-rate** command to find a channel that is not in use. This command applies to both 802.11a and 802.11b/g radios.

beacon-interval

This command configures the rate at which beacon signals are transmitted from the access point.

Syntax

beacon-interval <interval>

interval - The rate for transmitting beacon signals. (Range: 20-1000 milliseconds)

Default Setting

100

Command Mode

Interface Configuration (Wireless)

Command Usage

The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information.

channel

This command configures the radio channel through which the access point communicates with wireless clients.

Syntax

channel <channel | auto>

- *channel* - Manually sets the radio channel used for communications with wireless clients. Refer to "Country Channel Allocations" on page C-1 for a list of channels that you can set.
- **auto** - Automatically selects an unoccupied channel (if available). Otherwise, the lowest channel is selected.

Default Setting

Automatic channel selection

Command Mode

Interface Configuration (Wireless)

Command Usage

- The available channel settings are limited by local regulations, which determine the number of channels that are available.
- When multiple access points are deployed in the same area, be sure to choose a channel separated by at least four channels for 802.11a to avoid having the channels interfere with each other, and at least five channels for 802.11g. You can deploy up to four access points in the same area for 802.11a and three access points for 802.11g.
- For most wireless adapters, the channel for wireless clients is automatically set to the same as that used by the access point to which it is linked.

closed-system

This command prevents access from clients without a pre-configured SSID. Use the **no** form to disable this feature.

Syntax

closed-system
no closed-system

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

When enabled, the VAP interface does not include its SSID in beacon messages. Nor does it respond to probe requests from clients that do not include a fixed SSID.

datarate-based-access

This command sets the lowest data rate that the station is allowed to use to transmit data frames. The rate you enter here is the lowest rate displayed in the Supported Rates Information Element of the 802.11 beacon frame and other management frames. Use this command to prevent clients from transmitting data frames to the access point with lower data rates .

This command is available on IronPoint 200 running software release 02.02.04.

Syntax

datarate-based-access *<rate>*
no datarate-based-access

rate - Lowest data rate that a station can use for transmission of data frames.

Options for *rate* are as follows:

- For 802.11a: 6, 9, or 12 Mbps
- For 802.11b: 1, 2, 5.5, or 11 Mbps
- For 802.11g: 6, 9, or 12 Mbps
- For 802.11 b/g: 1, 2, 5.5, 6, 9, 11, or 12 Mbps

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

Indicate the data rate when configuring this feature.

Use the **no** form of the command to disable this feature.

description

This command adds a description to a VAP interface. Use the **no** form to remove the description.

Syntax

description *<string>*
no description

string - Comment or a description for this interface.
(Range: 1-80 characters)

Default Setting

None

Command Mode

Interface Configuration (Wireless-VAP)

dtim-period

This command configures the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

Syntax

dtim-period *<interval>*

interval - Interval between the beacon frames that transmit broadcast or multicast traffic.
(Range: 1-255 beacon frames)

Default Setting

1

Command Mode

Interface Configuration (Wireless)

Command Usage

- The Delivery Traffic Indication Map (DTIM) packet interval value indicates how often the MAC layer forwards broadcast/multicast traffic. This parameter is necessary to wake up stations that are using Power Save mode.
- The DTIM is the interval between two synchronous frames with broadcast/multicast information. The default value of 2 indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon.
- Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames.

fragmentation-length

This command configures the minimum packet size that can be fragmented when passing through the access point.

Syntax

fragmentation-length *<length>*

length - Minimum packet size for which fragmentation is allowed. (Range: 256-2346 bytes)

Default Setting

2346

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the packet size is smaller than the preset Fragment size, the packet will not be segmented.
- Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames.

max-association

This command configures the maximum number of clients that can be associated with the VAP interface at the same time.

Syntax

max-association *<count>*

count - Maximum number of associated stations. (Range: 0-64 per VAP interface)

Default Setting

64

Command Mode

Interface Configuration (Wireless-VAP)

multicast-data-rate

This command configures the maximum data rate at which the access point transmits multicast packets on the wireless interface.

Syntax

speed *<speed>*

speed - Maximum transmit speed allowed for multicast data. (Options: 1, 2, 5.5, 11 Mbps for 802.11b/g; 6, 12, 24 Mbps for 802.11a)

Default Setting

1 Mbps for 802.11b/g

6 Mbps for 802.11a

Command Mode

Interface Configuration (Wireless)

rssi-based-access

This command sets the Received Signal Strength Indication (RSSI) threshold on the amount of signal required in order for a client to associate and remain associated with an access point. A station (client) can associate with an access point only if the station sends authentication and association frames with an RSSI % that is greater than the configured association threshold. If a station sends a set of frames with an RSSI % that is less than the configured disassociation threshold, then the access point will deauthenticate that station.

This command is available in IronPoint 200 running software release 02.02.04.

Syntax

rssi-based-access <level>

level - A number that represents the minimum RSSI value for association and RSSI value for disassociation. *Level* is a percentage of the maximum possible RSSI value. (Options: None, 1 - 10. Values for Levels 1- 10 are presented below:

Level	Threshold for Disassociation (RSSI percent)	Threshold for Association (RSSI percent)
None	Entering None for level disables the command	
1	5%	15%
2	10%	20%
3	15%	25%
4	20%	30%
5	25%	35%
6	30%	40%
7	35%	45%
8	40%	50%
9	45%	55%
10	50%	60%

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

Specify a number from 1 - 10 to enable this feature and set the threshold. See the table above.

Enter the **None** for *level* to disable this feature.

Example:

```
Foundry AP#configure
Foundry AP(config)#interface wireless a
Foundry AP(if-wireless a)#rssi-based-access 2
```


In the configuration above, (`rssi-based-access 2`) the access point deauthenticates any client that sends a series of frames with RSSI % that is less than 10% . It will only authenticate and associate clients that send authentication and association frames with an RSSI % that is greater than 20%. Any client sending authentication and association frames with an RSSI % that is less than 20% will be ignored.

rts-threshold

This command sets the packet size threshold at which a Request to Send (RTS) signal must be sent to the receiving station prior to the sending station starting communications.

Syntax

rts-threshold <threshold>

threshold - Threshold packet size for which to send an RTS. (Range: 0-2347 bytes)

Default Setting

2347

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the threshold is set to 0, the access point never sends RTS signals. If set to 2347, the access point always sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.
- The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS frame to notify the sending station that it can start sending data.
- Access points contending for the wireless medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node" problem.

speed

This command configures the maximum data rate at which the access point transmits unicast packets on the wireless interface.

Syntax

speed <speed>

speed - Maximum transmit speed to wireless clients. (Options: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps)

Default Setting

54 Mbps

Command Mode

Interface Configuration (Wireless)

Command Usage

The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance.

ssid

This command configures the VAP service set identifier (SSID).

Syntax

ssid <string>

string - The name of a basic service set supported by the VAP interface. (Range: 1 - 32 characters)

Default Setting

IronPoint 200: Foundry AP (0 to 3 for each VAP)

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

Clients that want to connect to the wireless network via an access point must set their SSIDs to the same as that of the access point.

transmit-power

This command adjusts the power of the radio signals transmitted from the access point.

Syntax

transmit-power <signal-strength>

signal-strength - Signal strength transmitted from the access point. (Options: full, half, quarter, eighth, min, auto)

Default Setting

full

Command Mode

Interface Configuration (Wireless)

Command Usage

Note: When operating the IronPoint Access Point using 5 GHz channels in a European Community country, the end user or installer is obligated to operate the device in accordance with European regulatory requirements for Transmit Power Control (TPC).

- This command applies to both 802.11a and 802.11b/g radios.
- The “min” keyword indicates minimum power.
- The longer the transmission distance, the higher the transmission power required. But to support the maximum number of users in an area, you must keep the power as low as possible. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high strength signals do not interfere with the operation of other radio devices in your area.
- Check with your country’s regulations for wireless products to see if there are restrictions for using the transmit power command.
- Use the “auto” keyword to allow the access point to automatically select a transmission power for the radio.
- To disable “auto” simply change the transmit power to another value.

turbo

This command sets the 802.11a radio interface to an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Use the **no** form to disable the high data-rate mode.

This command is not available for the 802.11g radio interface.

Syntax

turbo
no turbo

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless - 802.11a)

Command Usage

- The normal 802.11a wireless operation mode provides connections up to 54 Mbps. Turbo Mode is an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Enabling Turbo Mode allows the access point to provide connections up to 108 Mbps.
- In normal mode, the access point provides a channel bandwidth of 20 MHz, and supports the maximum number of channels permitted by local regulations (e.g., 13 channels for the United States). In Turbo Mode, the channel bandwidth is increased to 40 MHz to support the increased data rate. However, this reduces the number of channels supported (e.g., 5 channels for the United States).

Note: The use of Turbo Mode is not permitted in some countries, such as those in the European Community. You should check your country's regulations for wireless products to see if Turbo Mode is allowed.

vap

This command provides access to the VAP interface configuration mode.

Syntax

vap <vap-id>

vap-id - The number that identifies the VAP interface. (Options: 0, 1, 2, or 3)

Default Setting

None

Command Mode

Interface Configuration (Wireless)

shutdown

This command disables the VAP interface. Use the **no** form to restart the interface.

Syntax

shutdown
no shutdown

Default Setting

Interface enabled

Command Mode

Interface Configuration (Wireless-VAP)

show auto

This command displays the configuration of the access point for automatic channel and transmission power assignment.

Syntax

show auto

Command Mode

Exec

Example:

```

Foundry AP#show auto
AUTO CHANNEL & TX POWER          RADIO-A          RADIO-B/G
-----
Auto Refresh Interval (min) :          30          30
Number of Scans done          :          3          3
Time to next scan              :    0 hrs  20 min.    0 hrs  29 min.
Auto Channel Selection Mode    :                                OVERLAP

```

The “Auto Refresh Interval” shows the configured duration between scans for each radio.

The “Number of Scans done” shows the number of scans that were done since the access point rebooted

The “Time to next scan” shows the number of minutes remaining before the next scan.

The “Auto Channel Selection Mode” shows if the auto channel selection mode overlap is enabled for Radio b/g. The characters “OVERLAP” mean the selection mode is disabled. The characters “NON-OVERLAP” appear if the feature is enabled.

show bssid

This command displays the BSSID for each VAP interface.

Syntax

show bssid

Command Mode

Exec

show interface wireless

This command displays the status for the VAP interface.

Syntax

show interface wireless <a | g> <*vap-id*>

- **a** - 802.11a radio interface.
- **g** - 802.11g radio interface.
- *vap-id* - The number that identifies the VAP interface. (Options: 0, 1, 2, or 3)

Command Mode

Exec

Example:

```

Foundry AP#show interface wireless g 0
Wireless Interface G VAP 0 Information
=====
-----Identification-----
Description                : Foundry 802.11g Access Point
SSID                      : Foundry AP 0
BSSID                    : 00-12-F2-E8-AE-88
Channel                   : 11 (AUTO)
Status                   : Disabled
----- Auto Channel Selection & Transmit Power Control Parameters -----
Auto Refresh Interval     : 1440 min.
Auto Channel Selection Mode : NON_OVERLAP
Auto Transmit Power Control : Disabled
-----802.11 Parameters-----
Radio Mode                : 802.11b+g
Transmit Power            : FULL (16 dBm)
Max Station Data Rate     : 54Mbps
Multicast Data Rate       : 1Mbps
Fragmentation Threshold   : 2346 bytes
RTS Threshold             : 2347 bytes
Beacon Interval           : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval : 30 Mins
DTIM Interval             : 1 beacon
Preamble Length           : SHORT-OR-LONG
Maximum Association       : 64 stations
VLAN ID                  : 1
Load Balance              : Disabled
SSID Prioritization Threshold : 0
Priority Level             : Low
RSSI Based Access         : 4
Data Rate Based Access    : 5.5 Mbps
-----Security-----
Closed System             : Disabled
WPA clients               : Disabled
WPA Key Mgmt Mode         : PRE SHARED KEY
WPA PSK Key Type          : PASSPHRASE
PMKSA Lifetime            : 720 minutes
Encryption                : Disabled
WEP Key Length            : None
Default Transmit Key      : 1
WEP Key Type              : Key 1: HEX      Key 2: HEX
                          : Key 3: HEX      Key 4: HEX
Common Static Keys        : Key 1: EMPTY   Key 2: EMPTY
                          : Key 3: EMPTY   Key 4: EMPTY
Authentication Type        : OPEN
-----Antenna-----
Antenna Control method    : Full diversity
Antenna ID                : Integrated
-----Authentication Parameters-----
802.1x                    : Disabled
Broadcast Key Refresh Rate : 120 min
802.1x Session Timeout Value : 0 min
Pre-Authentication        : Disabled
=====

```

show neighbor-ap

You can display a list of access points that have been detected on the network by entering the following command:

Syntax

show neighbor-ap

Command Mode

Exec

```
Foundry AP#show neighbor-ap
```

BSSID	CHANNEL	RSSI
-----	-----	-----
00:0c:db:8a:84:ec	42	28
00:0c:db:8a:84:ed	42	29
00:0c:db:8a:84:ee	42	29
00:0c:db:8a:83:88	1	29
00:0c:db:8a:83:89	1	28
00:0c:db:8a:83:b8	1	8
00:0c:db:8a:83:b9	1	11
00:0c:db:8a:ea:68	1	24
00:0c:db:8a:ea:69	1	22
00:0c:db:8a:ea:6a	1	23
00:0c:db:8a:ea:6b	1	21
00:0c:db:8b:20:e8	1	10
00:0c:db:8c:03:f8	1	30

The report shows the broadcast SSIDs of the neighboring access points, the channels they are using, and the strength of the signal of the channel in dBm.

Using the Web Management Interface

From the Radio Interface 802.11a menu, click Radio Settings. For each VAP interface and Hidden-SSID.

The screenshot shows the Foundry IronPoint 200 Web Management Interface. The left sidebar contains a navigation menu with the following items: System (selected), Identification, Port/IP, RADIUS, Management Tunnel, Authentication, Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP (selected), SNMP General, SNMP Trap Filters, SNMP Targets, Radio Interface 802.11a (selected), Radio Settings (selected), Security, and Radio Interface 802.11g. The main content area is titled "802.11a Radio Settings" and contains two sections: "Individual" and "Hidden SSID".

Individual

Default VLAN ID (1 ~ 4094) :

VAP	VLAN ID
VAP 0	1
VAP 1	1
VAP 2	1
VAP 3	1

Hidden SSID :

VAP	Hidden SSID
VAP 0	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 1	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 2	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 3	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Set the authentication and association timeout intervals, as well as the maximum associated client limit.

The screenshot shows the Foundry IronPoint 200 Web Management Interface. The left sidebar contains a navigation menu with the following items: System, Identification, Port/IP, RADIUS, Management Tunnel, Authentication, Bridging, Administration, Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP, SNMP General, SNMP Trap Filters, SNMP Targets, Radio Interface 802.11a, Radio Settings (selected), Security, and Radio Interface 802.11g. The main content area is titled "Authentication Timeout Interval (5-60) : (Mins)" and contains two sections: "Authentication Timeout Interval (5-60) : (Mins)" and "Association Timeout Interval (5-60) : (Mins)".

Authentication Timeout Interval (5-60) : (Mins)

VAP	Timeout Interval (Mins)
VAP 0	60
VAP 1	60
VAP 2	60
VAP 3	60

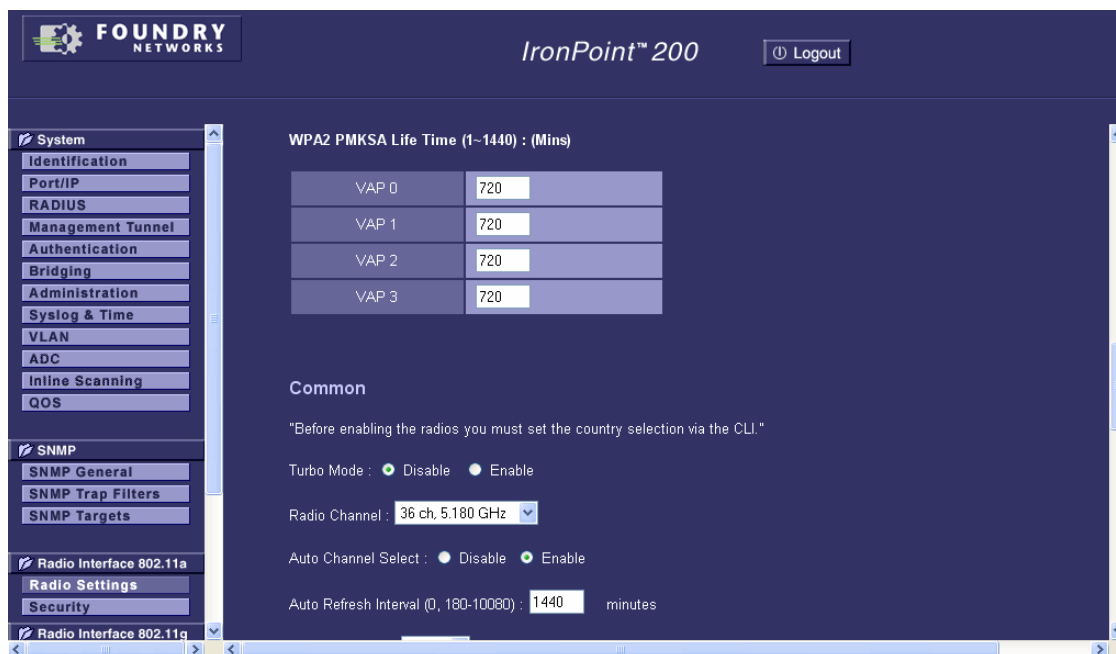
Association Timeout Interval (5-60) : (Mins)

VAP	Timeout Interval (Mins)
VAP 0	30
VAP 1	30
VAP 2	30
VAP 3	30

Max Associated Clients (0-64) :

VAP	Max Associated Clients
VAP 0	64
VAP 1	64

Define the WPA2 PMKSA Life Time value for the VAP. Also define values for parameters common to all VAPs.



WPA2 PMKSA Life Time (1~1440) : (Mins)

VAP 0	720
VAP 1	720
VAP 2	720
VAP 3	720

Common

"Before enabling the radios you must set the country selection via the CLI."

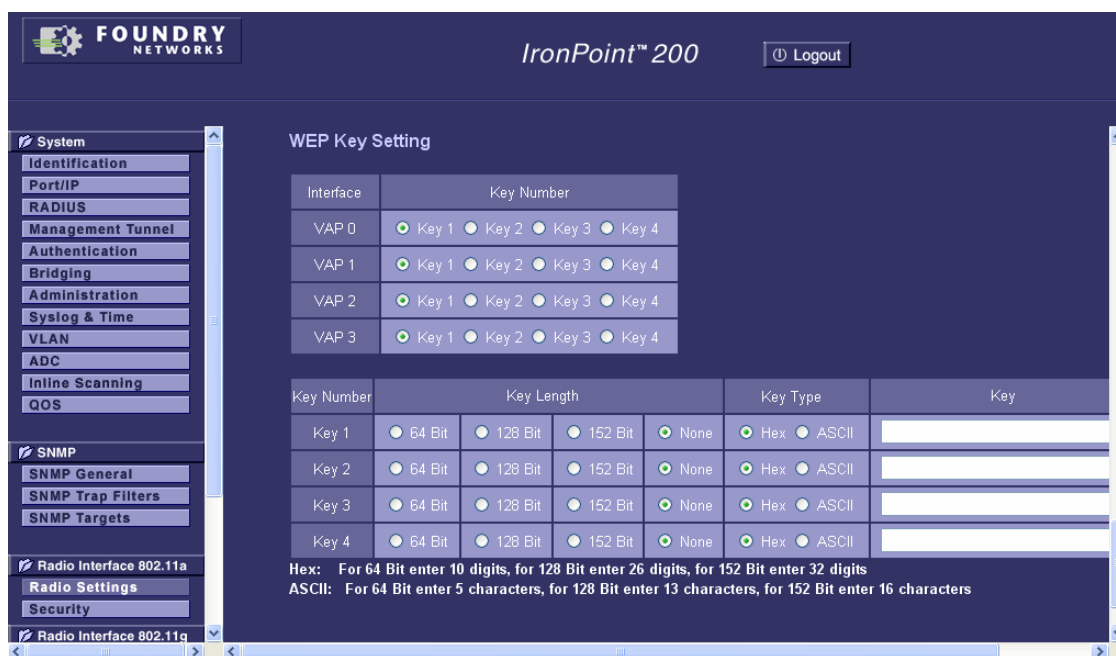
Turbo Mode : ☒ Disable ☐ Enable

Radio Channel : 36 ch, 5.180 GHz

Auto Channel Select : ☐ Disable ☒ Enable

Auto Refresh Interval (0, 180-10080) : 1440 minutes

If you are using WEP keys, enter at least one key and set the keys to use for each VAP interface. Modify other settings as required. Click Apply.



WEP Key Setting

Interface	Key Number
VAP 0	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 1	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 2	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 3	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4

Key Number	Key Length	Key Type	Key
Key 1	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 2	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 3	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 4	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	

Hex: For 64 Bit enter 10 digits, for 128 Bit enter 26 digits, for 152 Bit enter 32 digits
 ASCII: For 64 Bit enter 5 characters, for 128 Bit enter 13 characters, for 152 Bit enter 16 characters

Configurable Parameters

Enable – Enables radio communications using the VAP interface. (Default: Disable)

SSID – The name of the basic service set provided by a VAP interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of an access point VAP interface. (Default: IronPoint 200 is Foundry AP (0 to 3), Range: 1-32 characters)

Individual VAP Parameters

Default VLAN ID – The VLAN ID assigned to wireless clients associated to the VAP interface that are not assigned to a specific VLAN by RADIUS server configuration. (Default: 1)

Hidden SSID – When enabled, the VAP interface does not include its SSID in beacon messages. Nor does it respond to probe requests from clients that do not include a fixed SSID. (Default: Disable)

Authentication Timeout Interval – The time interval after which clients must be re-authenticated to access the VAP interface. (Range: 5-60 minutes; Default: 60 minutes)

Association Timeout Interval – The the idle time interval (when no frames are sent) after which a client is disassociated from the VAP interface. (Range: 5-60 minutes; Default: 30 minutes)

Maximum Associated Clients – Sets the maximum number of clients that can be associated with a VAP interface at the same time. (Range: 0-64 per VAP interface; Default: 64)

WPA2 PMKSA Life Time – WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns reauthentication is not required. When a WPA2 client is first authenticated, it receives a Pairwise Master Key (PMK) that is used to generate other keys for unicast data encryption. This key and other client information form a Security Association that the access point names and holds in a cache. The lifetime of this security association can be configured with this command. When the lifetime expires, the client security association and keys are deleted from the cache. If the client returns to the access point, it requires full reauthentication. (Range: 1-1440 minutes; Default: 720 minutes)

Common Parameters

Turbo Mode – The normal 802.11a wireless operation mode provides connections up to 54 Mbps. Turbo Mode is an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Enabling Turbo Mode allows the access point to provide connections up to 108 Mbps. (Default: Disabled)

Note: In normal mode, the access point provides a channel bandwidth of 20 MHz, and supports the maximum number of channels permitted by local regulations (e.g., 13 channels for the United States). In Turbo Mode, the channel bandwidth is increased to 40 MHz to support the increased data rate. However, this reduces the number of channels supported (e.g., 5 channels for the United States).

Note: Check with your country's regulations for wireless products to see if Turbo Mode is allowed.

Radio Channel – The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least four channels apart to avoid interference with each other. Refer to "Country Channel Allocations" on page C-1 for a list of available channels for your country.

Auto Channel Select – Enables the access point to automatically select an unoccupied radio channel. (Default: Enabled)

Note: Check with your country's regulations for wireless products to see if Auto Channel can be disabled.

Auto Refresh Rate - Enables the access point to automatically select an unoccupied radio channel. (Default: Enabled)

Transmit Power – Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Options: 100%, 50%, 25%, 12%, minimum; Default: 100%)

Note: When operating the IronPoint Access Point using 5 GHz channels in a European Community country, the end user or installer is obligated to operate the device in accordance with European regulatory requirements for Transmit Power Control (TPC).

Maximum Station Data Rate – The maximum data rate at which the access point transmits unicast packets on the wireless interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Options: 54, 48, 36, 24, 18, 12, 9, 6 Mbps; Default: 54 Mbps)

Multicast Data Rate - The maximum data rate at which the access point transmits multicast packets on the wireless interface. (Options: 6, 12, 24 Mbps; Default 6 Mbps)

Antenna Type – Selects the antenna to be used by the access point; either the integrated diversity antennas or an external antenna.

Antenna Diversity – Selects the antenna diversity to use. "Full" for the integrated antennas or "Fixed A" for an external antenna. (Default: Full)

Antenna Location – Selects the mounting location of the antenna in use; either "Indoor" or "Outdoor." (Default: Indoor)

Note: Only the 802.11a interface supports the Antenna Location setting. The 802.11g interface is fixed at "Indoor" and is not configurable.

Beacon Interval – The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)

Data Beacon Rate – The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions. Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of 2 indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after

every second beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 1 beacon)

RTS Threshold – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the access point never sends RTS signals. If set to 2347, the access point always sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

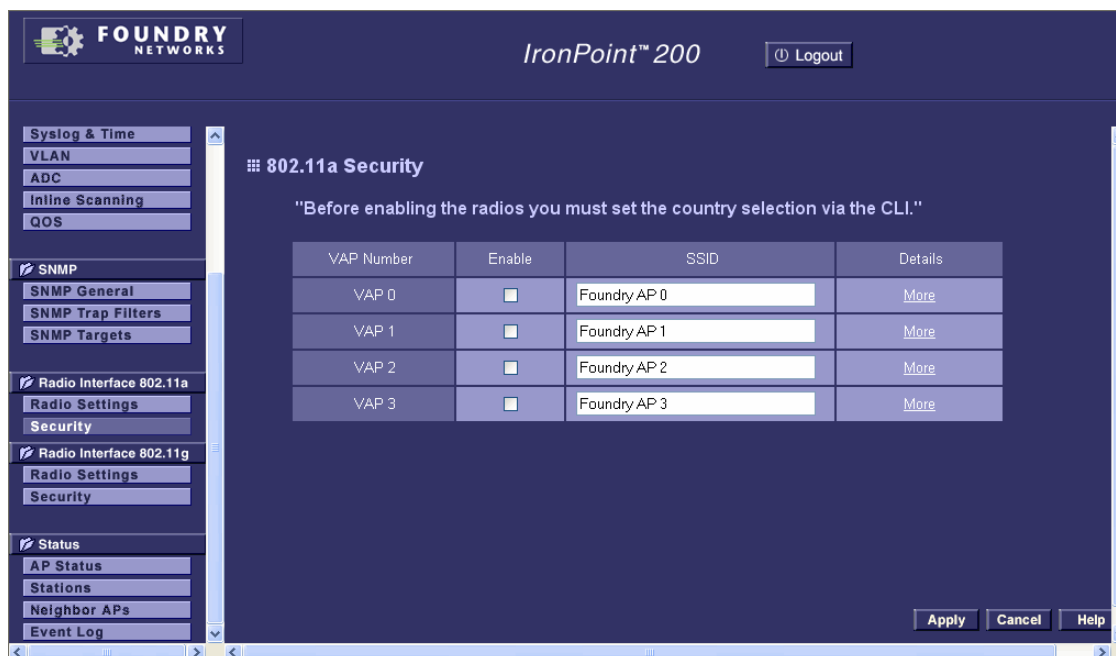
The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes; Default: 2347 bytes)

Key Type – Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys that are common for all VAP interfaces:

- Hexadecimal: Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys.
- Alphanumeric: Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys.
- VAP Transmit Key Select: Selects the key number to use for encryption for each VAP interface. If the clients have all four keys configured to the same values, you can change the encryption key to any of the four settings without having to update the client keys.
- Shared Key Setup – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. (Default: 128 Bit)
- Note: The 152-bit key applies only to the 802.11a wireless interface.
- Key: Enter the required key into this field.

Note: In a mixed-mode environment with clients using static WEP keys and WPA, select WEP transmit key index 2, 3, or 4. The access point uses transmit key index 1 for the generation of dynamic keys.

To configure the SSID for each VAP, click Security under the Radio Interface 802.11a menu. Set the SSID for each VAP interface and select Enable. Click Apply.



Configurable Parameters

Enable – Enables radio communications on the VAP interface. (Default: Disable)

SSID – The name of the basic service set provided by the VAP interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of a VAP interface. (Default: IronPoint 200 is Foundry AP (0 to 3), Range: 1-32 characters)

Click More if the VAP interface is using 802.11x. See “Using the Web Management Interface” on page 19-9 for details on additional parameters you need to configure for this mode.

Configuring Radio Settings (802.11g)

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Also note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

Note: For a description of commands and parameters not described in this section, see “Configuring Radio Settings (802.11a)” on page 21-1.

Using the CLI

From the CLI configuration mode, use the **interface wireless g** command to access the interface mode for the 802.11g radio. The 802.11g radio can be forced to an 802.11g-only, 802.11b-only, or mixed 802.11b/g operating mode using the **radio-mode** command. You should set the desired operating mode before configuring channel settings (the default is mixed 802.11b/g operation). Select a radio channel or set selection to Auto using the **channel** command. To access each VAP

interface (numbered 0 to 3), use the **vap** command. You should set each VAP interface SSID using the **ssid** command and, if required, configure a name for the interface using the **description** command. You can also use the **hidden-ssid** command to disable sending the SSID in beacon messages. Set any other parameters as required before enabling the VAP interface with the **no shutdown** command. To view the current 802.11g radio settings, use the **show interface wireless g** command (not shown in example).

```
Foundry AP(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless g)#radio-mode g
Foundry AP(if-wireless g)#antenna type 0101
Foundry AP(if-wireless g)#channel 1
Foundry AP(if-wireless g)#speed 54
Foundry AP(if-wireless g)#multicast-data-rate 11
Foundry AP(if-wireless g)#beacon-interval 150
Foundry AP(if-wireless g)#dtim-period 5
Foundry AP(if-wireless g)#fragmentation-length 512
Foundry AP(if-wireless g)#rts-threshold 256
Foundry AP(if-wireless g)#transmit-power half
Foundry AP(if-wireless g)#preamble long
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless g: VAP[0])#description IP-VAP0
Foundry AP(if-wireless g: VAP[0])#ssid ironpoint-vap0
Foundry AP(if-wireless g: VAP[0])#association-timeout-interval 20
Foundry AP(if-wireless g: VAP[0])#authentication-timeout-interval 30
Foundry AP(if-wireless g: VAP[0])#max-association 32
Foundry AP(if-wireless g: VAP[0])#hidden-ssid
Foundry AP(if-wireless g: VAP[0])#no shutdown
Foundry AP(if-wireless g: VAP[0])#
```

If you are configuring Radio b/g to automatically detect channel and transmission power, enter commands as in the following example:

```
Foundry AP(config)#interface wireless g
Foundry AP(if-wireless a)#channel auto
Foundry AP(if-wireless g)#auto-channel-selection-mode-overlap
Foundry AP(if-wireless a)#auto-refresh-rate 1440
Foundry AP(if-wireless a)#transmit-power auto
```

auto-channel-selection-mode-overlap

This command allows the 802.11b/g radio to select any valid channel available, including overlapping and non-overlapping channels (1, 6, or 11).

Syntax

auto-channel-selection-mode-overlap
no auto-channel-selection-mode-overlap

Default Setting

non-overlap

Command Mode

Interface Configuration (Wireless - 802.11b/g)

Command Usage

Use the **channel auto** command to enable automatic channel selection on the radio. Once automatic channel selection is enabled, the radio scans the airwaves at the interval specified by the **auto-refresh** command to find a channel that is not in use. On the 802.11b/g radio, also enable the **auto-channel-selection-mode-overlap** to allow the 802.11b/g radio to select any valid channel that is available.

Use the **no auto-channel-selection-mode-overlap** form of the command to force the 802.11b/g radio to select only non-overlapping channels, which are channels 1, 6, or 11.

radio-mode

This command forces the operating mode for the 802.11g wireless interface.

Syntax

radio-mode <b | g | b+g>

- **b** - b-only mode: Both 802.11b and 802.11g clients can communicate with the access point, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).
- **g** - g-only mode: Only 802.11g clients can communicate with the access point (up to 54 Mbps).
- **b+g** - b & g mixed mode: Both 802.11b and 802.11g clients can communicate with the access point (up to 54 Mbps).

Default Setting

b+g mode

Command Mode

Interface Configuration (Wireless - 802.11g)

Command Usage

- Refer to “Country Channel Allocations” on page C-1 for available channels in **b**, **g**, or **b+g** modes.
- Both the 802.11g and 802.11b standards operate within the 2.4 GHz band. If you are operating in **g** mode, any 802.11b devices in the service area will contribute to the radio frequency noise and affect network performance.

preamble

This command sets the length of the signal preamble that is used at the start of a 802.11b/g data transmission.

Syntax

preamble [long | short-or-long]

- **long** - Sets the preamble to long (192 microseconds).
- **short-or-long** - Sets the preamble according to the capability of clients that are currently associated. Uses a short preamble (96 microseconds) if all associated clients can support it, otherwise a long preamble is used.

Default Setting

Short-or-long

Command Mode

Interface Configuration (Wireless - 802.11g)

Command Usage

- Using a short preamble instead of a long preamble can increase data throughput on the access point, but requires that all clients can support a short preamble.
- Set the preamble to long to ensure the access point can support all 802.11b and 802.11g clients.

Using the Web Management Interface

From the Radio Interface 802.11g menu, click Radio Settings.

FOUNDRY NETWORKS *IronPoint™ 200* [Logout](#)

802.11g Radio Settings

Individual

Default VLAN ID (1 ~ 4094) :

VAP 0	<input type="text" value="1"/>
VAP 1	<input type="text" value="1"/>
VAP 2	<input type="text" value="1"/>
VAP 3	<input type="text" value="1"/>

Hidden SSID :

VAP 0	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 1	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 2	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VAP 3	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

For each VAP interface, set the Default VLAN ID and Hidden SSID.

Also define the authentication and association timeout intervals, as well as the maximum number of clients that can associate with each VAP.

Authentication Timeout Interval (5-60) : (Mins)	
VAP 0	60
VAP 1	60
VAP 2	60
VAP 3	60

Association Timeout Interval (5-60) : (Mins)	
VAP 0	30
VAP 1	30
VAP 2	30
VAP 3	30

Max Associated Clients (0-64) :	
VAP 0	64
VAP 1	64
VAP 2	64
VAP 3	64

Define the WPA2 PMKSA Life Time value for the VAP. Also define values for parameters common to all VAPs, such as radio mode, radio channel, and others.

WPA2 PMKSA Life Time (1-1440) : (Mins)	
VAP 0	720
VAP 1	720
VAP 2	720
VAP 3	720

Common

"Before enabling the radios you must set the country selection via the CLI."

Radio Mode : 802.11b+g

Radio Channel : 11

Auto Channel Select : ☐ Disable ☒ Enable

Auto Refresh Interval (0, 180-10080) : 1440 minutes

Select Enable for the radio and select an operating mode. Then configure a specific radio channel from the drop-down list, or select Auto Channel Select.

If you are using WEP keys, enter at least one key and set the keys to use for each VAP interface. Modify other settings as required. Click Apply.

WEP Key Setting

Interface	Key Number
VAP 0	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 1	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 2	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 3	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4

Key Number	Key Length	Key Type	Key
Key 1	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 2	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 3	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 4	<input checked="" type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	

Hex: For 64 Bit enter 10 digits, for 128 Bit enter 26 digits, for 152 Bit enter 32 digits
 ASCII: For 64 Bit enter 5 characters, for 128 Bit enter 13 characters, for 152 Bit enter 16 characters

Configurable Parameters

Enable – Enables radio communications on the access point. (Default: Disable)

SSID – The name of the basic service set provided by the access point. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point. (Default: IronPoint 200 is Foundry AP (0 to 3), Range: 1-32 characters)

Common Parameters

Radio Mode – Selects the operating mode for the 802.11g wireless interface. (Default: 802.11b+g)

- **802.11b+g** - b & g mixed mode: Both 802.11b and 802.11g clients can communicate with the access point (up to 54 Mbps).
- **802.11b only** - Both 802.11b and 802.11g clients can communicate with the access point, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).
- **802.11g only** - Only 802.11g clients can communicate with the access point (up to 54 Mbps).

Note: For Japan, only 13 channels are available when set to **802.11g only** or **802.11b+g** modes. When set to **802.11b only** mode, 14 channels are available.

Radio Channel – The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, in the United States you can deploy up to three access points in the same area (e.g., channels 1, 6, 11).

Also note that the channel for wireless clients is automatically set to the same as that used by the access point to which it is linked. (Range: 1-11; Default: 1)

Auto Channel Select – Enables the access point to automatically select an unoccupied radio channel. (Default: Enabled)

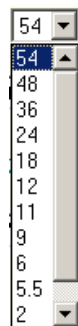
Auto Refresh Rate – Enables the access point radio to scan the air waves at the specified interval so it can automatically select a channel. (Options: 0, 180 – 10080 minutes; Default: 1440 minutes)

Auto Channel Selection Mode – Sets automatic channel selection mode to select overlapping or non-overlapping channels. (Default: Non-Overlap)

Transmit Power – Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Options: 100%, 50%, 25%, 12%, minimum, auto; Default: 100%)

Note: When operating the IronPoint Access Point using 5 GHz channels in a European Community country, the end user or installer is obligated to operate the device in accordance with European regulatory requirements for Transmit Power Control (TPC).

Maximum Station Data Rate – The maximum data rate at which a client can connect to the access point. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Default: 54 Mbps)



Multicast Data Rate – The maximum data rate at which the access point transmits multicast packets on the wireless interface. (Options: 6, 12, 24 Mbps; Default: 6 Mbps)

Antenna Type – Selects the antenna to be used by the access point; either the integrated diversity antennas or an external antenna. (Default: Foundry Integrated Antenna)

Antenna Diversity – Selects the antenna diversity to use. “Full” for the integrated antennas or “Fixed A” for an external antenna. (Default: Full)

Beacon Interval – The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)

Data Beacon Rate – The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions. Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of 2 indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more

timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 2 beacons)

RTS Threshold – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the access point never sends RTS signals. If set to 2347, the access point always sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes; Default: 2347 bytes)

Key Type – Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys that are common for all VAP interfaces:

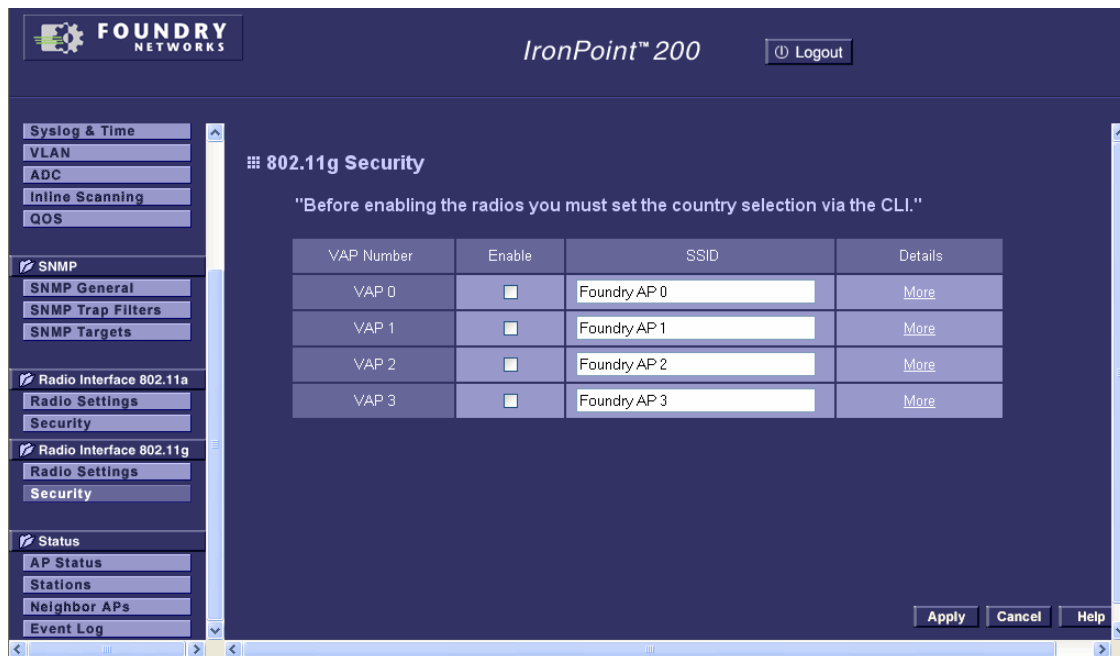
- **Hexadecimal:** Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys or 26 hexadecimal digits for 128 bit keys.
- **Alphanumeric:** Enter keys as 5 alphanumeric characters for 64 bit keys or 13 alphanumeric characters for 128 bit keys.
- **VAP Transmit Key Select:** Selects the key number to use for encryption for each VAP interface. If the clients have all four keys configured to the same values, you can change the encryption key to any of the four settings without having to update the client keys.
- **Shared Key Setup** – Select 64 Bit Or 128 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. (Default: 128 Bit)

Note: The 152 bit key, which is available in the 802.11a wireless interface, is not supported on the 802.11b/g wireless interface.

- **Key:** Enter the required key into this field.

Note: In a mixed-mode environment with clients using static WEP keys and WPA, select WEP transmit key index 2, 3, or 4. The access point uses transmit key index 1 for the generation of dynamic keys.

To configure the SSID for each VAP, click Security under the Radio Interface 802.11g menu. Set the SSID for each VAP interface and select Enable. Click Apply.



Configurable Parameters

Enable – Enables radio communications on the VAP interface. (Default: Disable)

SSID – The name of the basic service set provided by the VAP interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of a VAP interface. (Default: IronPoint 200 is Foundry AP (0 to 3), Range: 1-32 characters)

Click More if the VAP interface is using 802.11x. See “Using the Web Management Interface” on page 19-9 for details on additional parameters you need to configure for this mode.

Configuring Access Point Load Balancing

The ideal scenario in a wireless network environment is for each access point to have the same number of clients associated with them. However, because of the roaming criteria specified by the IEEE 802.11 standards, wireless clients stay associated with an access point even if there is an access point closer to that client; therefore, more wireless clients may be associated with one access points than with another.

To help alleviate this situation, load balancing, when enabled, associates wireless clients with the access point closes to their location. A client stays associated with an access point, even if that client moves to another location. When the client is disassociated from the network, the client will be associated with the closest access point the next time that client becomes authenticated. The closest access point is one from which the client receives the strongest signal.

Using the CLI

To configure this feature, enter commands such as the following:

```

Foundry AP(config)#interface wireless a
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless a)#vap 0
Foundry AP(if-wireless a: VAP[0])#description IP-VAP0
Foundry AP(if-wireless a: VAP[0])#ssid ironpoint-vap0
Foundry AP(if-wireless a: VAP[0])#association-timeout-interval 20
Foundry AP(if-wireless a: VAP[0])#exit
Foundry AP(if-wireless a)#exit
Foundry AP(config)#loadbalance 6
Foundry AP(config)#exit
    
```

loadbalance

Enables the load balancing feature, which associates wireless clients with the access point closes to their location. (See introduction above.)

Syntax

loadbalance <*weight*>

no loadbalance

weight - The weight of the signal that corresponds to the desired management RSSI, the received signal strength of the 802.11 management packets, as presented in the following table:

Weight	Management RSSI
1	28%
2	31%
3	34%
4	37%
5	41%
6	44%
7	47%
8	50%
9	53%
10	56%

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless - 802.11a or Wireless - 802.11b/g)

Command Usage

A wireless client remains associated with an access point until the client either disconnects or is disassociated from the access point because the association timeout interval has expired.

Use the **association-timeout-interval** command to configures the idle time interval (when no frames are sent) after which the client is disassociated from the VAP interface.

Use the **no loadbalance** command to disable the feature.

Use the **show interface wireless** command to display the current load balance setting

show interface wireless

The show interface wireless command now includes an entry that shows if load balance is enabled or disabled.

```

Foundry AP#show interface wireless g 0
Wireless Interface G VAP 0 Information
=====
-----Identification-----
Description                : Foundry 802.11g Access Point
SSID                      : Foundry AP 0
BSSID                    : 00-12-F2-E8-AE-88
Channel                  : 11 (AUTO)
Status                   : Disabled
----- Auto Channel Selection & Transmit Power Control Parameters -----
Auto Refresh Interval     : 1440 min.
Auto Channel Selection Mode : NON_OVERLAP
Auto Transmit Power Control : Disabled
-----802.11 Parameters-----
Radio Mode                : 802.11b+g
Transmit Power            : FULL (16 dBm)
Max Station Data Rate     : 54Mbps
Multicast Data Rate       : 1Mbps
Fragmentation Threshold   : 2346 bytes
RTS Threshold             : 2347 bytes
Beacon Interval           : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval : 30 Mins
DTIM Interval             : 1 beacon
Preamble Length           : SHORT-OR-LONG
Maximum Association        : 64 stations
VLAN ID                   : 1
Load Balance              : Disabled
SSID Prioritization Threshold : 0
Priority Level             : Low
RSSI Based Access         : 4
Data Rate Based Access    : 5.5 Mbps
-----Security-----
Closed System              : Disabled
WPA clients                : Disabled
WPA Key Mgmt Mode          : PRE SHARED KEY
WPA PSK Key Type           : PASSPHRASE
PMKSA Lifetime             : 720 minutes
Encryption                 : Disabled
WEP Key Length             : None
Default Transmit Key       : 1
WEP Key Type               : Key 1: HEX      Key 2: HEX
                           : Key 3: HEX      Key 4: HEX
Common Static Keys         : Key 1: EMPTY   Key 2: EMPTY
                           : Key 3: EMPTY   Key 4: EMPTY
Authentication Type        : OPEN
-----Antenna-----
Antenna Control method     : Full diversity
Antenna ID                 : Integrated
-----Authentication Parameters-----
802.1x                     : Disabled
Broadcast Key Refresh Rate : 120 min
802.1x Session Timeout Value : 0 min
Pre-Authentication         : Disabled
=====

```


Using the Web Management Interface

See the “Using the Web Management Interface” on page 25-6 if you want to configure load balancing using the Web Management Interface.

Chapter 22

Wireless Security Configuration

The access point is configured by default as an “open system,” which broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

To improve wireless network security, you have to implement two main functions:

- **Authentication:** It must be verified that clients attempting to connect to the network are authorized users.
- **Traffic Encryption:** Data passing between the access point and clients must be protected from interception and eaves dropping.

For a more secure network, the access point can implement one or a combination of the following security mechanisms:

- Wired Equivalent Privacy (WEP) page 22-4
- IEEE 802.1x page 19-7
- Wireless MAC address filtering page 19-2
- Wi-Fi Protected Access (WPA) or WPA2 page 22-4

The security mechanisms that may be employed depend on the level of security required, the network and management resources available, and the software support provided on wireless clients. A summary of wireless security considerations is listed in the following table.

Security Mechanism	Client Support	Implementation Considerations
Static WEP shared keys	Built-in support on all 802.11a, 802.11b and 802.11g devices	<ul style="list-style-type: none">• Provides only weak security• Requires manual key management
802.1x with dynamic WEP keys	Requires 802.1x client support in system or by add-in software (support provided in Windows 2000 SP3 or later and Windows XP)	<ul style="list-style-type: none">• Provides dynamic key rotation for improved WEP security• Requires configured RADIUS server• 802.1x EAP type may require management of digital certificates for clients and server

Security Mechanism	Client Support	Implementation Considerations
MAC address filtering	Uses the MAC address of client network card	<ul style="list-style-type: none"> Provides only weak user authentication Management of authorized MAC addresses Can be combined with other methods for improved security Optionally configured RADIUS server
802.1x WPA Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	<ul style="list-style-type: none"> Provides robust security in WPA-only mode Offers support for legacy WEP clients, but with increased security risk Requires configured RADIUS server 802.1x EAP type may require management of digital certificates for clients and server
WPA Pre-Shared Key Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	<ul style="list-style-type: none"> Provides good security in small networks Requires manual management of pre-shared key
802.1x WPA2 Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	<ul style="list-style-type: none"> Provides the strongest security in WPA2-only mode Provides robust security in mixed mode for WPA and WPA2 clients Offers fast roaming for time-sensitive client applications Requires configured RADIUS server 802.1x EAP type may require management of digital certificates for clients and server Clients may require hardware upgrade to be WPA2 compliant
WPA2 Pre-Shared Key Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	<ul style="list-style-type: none"> Provides robust security in small networks Requires manual management of pre-shared key Clients may require hardware upgrade to be WPA2 compliant

The access point can simultaneously support clients using various different security mechanisms. The configuration for these security combinations are outlined in the following table. Note that MAC address authentication can be configured independently to work with all security mechanisms and is indicated separately in the table. Required RADIUS server support is also listed.

Client Security Combination	Configuration Summary ¹	MAC Authentication ²	RADIUS Server
No encryption and no authentication	VAP interface settings: Authentication: Open Encryption: Disable 802.1x: Disable	Local, RADIUS, or Disabled	Yes ³
Static WEP only (with or without shared key authentication)	Enter 1 to 4 WEP keys Select a WEP transmit key VAP interface settings: Authentication: Shared Key or Open Encryption: WEP 802.1x: Disable	Local, RADIUS, or Disabled	Yes ³
Dynamic WEP (802.1x) only	VAP interface settings: Authentication: 802.1x Set 802.1x key refresh and reauthentication rates Encryption: WEP	Local, RADIUS, or Disabled	Yes ³

Client Security Combination	Configuration Summary¹	MAC Authentication²	RADIUS Server
802.1x WPA only	VAP interface settings: Authentication: 802.1x Set 802.1x key refresh and reauthentication rates Encryption: WPA-TKIP	Local or Disabled	Yes
WPA Pre-Shared Key only	VAP interface settings: Authentication: Pre-Shared Key Encryption: WPA-TKIP WPA Pre-shared Key Type: Hexadecimal or Alphanumeric Enter a WPA Pre-shared key	Local only	No
Static and dynamic (802.1x) WEP keys	Enter 1 to 4 WEP keys Select a WEP transmit key VAP interface settings: Authentication Type: 802.1x and User Shared Key Set 802.1x key refresh and reauthentication rates Encryption: WEP	Local or Disabled	Yes
Dynamic WEP and 802.1x WPA	VAP interface, Advanced settings: Authentication Type: WPA 802.1x: Required Set 802.1x key refresh and reauthentication rates Data Encryption: Enable WPA Configuration: Supported Cipher Suite: WEP	Local or Disabled	Yes
Static and dynamic (802.1x) WEP keys and 802.1x WPA	Enter 1 to 4 WEP keys Select a WEP transmit key VAP interface, Advanced settings: Authentication Type: WPA 802.1x: Required Set 802.1x key refresh and reauthentication rates Data Encryption: Enable WPA Configuration: Supported Cipher Suite: WEP	Local or Disabled	Yes
802.1x WPA2 only	VAP interface settings: Authentication: 802.1x Set 802.1x key refresh and reauthentication rates Encryption: WPA2-AES CCMP	Local or Disabled	Yes
WPA2 Pre-Shared Key only	VAP interface settings: Authentication: Pre-Shared Key Encryption: WPA2-AES CCMP WPA Pre-shared Key Type: Hexadecimal or Alphanumeric Enter a WPA Pre-shared key	Local or Disabled	No
802.1x WPA-WPA2 Mixed Mode	VAP interface settings: Authentication: 802.1x Set 802.1x key refresh and reauthentication rates Encryption: WPA2-AES CCMP and AES-TKIP Mixed Mode	Local or Disabled	Yes
WPA-WPA2 Mixed Mode Pre-Shared Key	VAP interface settings: Authentication: Pre-Shared Key Encryption: WPA2-AES CCMP and AES-TKIP Mixed Mode WPA Pre-shared Key Type: Hexadecimal or Alphanumeric Enter a WPA Pre-shared key	Local or Disabled	No

1. The configuration summary does not include the set up for MAC authentication (see page 19-2) or RADIUS server (see page 15-1).

2. The configuration of RADIUS MAC authentication together with 802.1x WPA is not supported.
3. RADIUS server required only when RADIUS MAC authentication is configured.

Note: If you choose to configure RADIUS MAC authentication together with 802.1x, the RADIUS MAC address authentication occurs prior to 802.1x authentication. Only when RADIUS MAC authentication succeeds is 802.1x authentication performed. When RADIUS MAC authentication fails, 802.1x authentication is not performed.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, WEP has been found to be seriously flawed and cannot be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA) for improved data encryption and user authentication.

Setting up shared keys enables the basic IEEE 802.11 Wired Equivalent Privacy (WEP) on the access point to prevent unauthorized access to the network.

If you choose to use WEP shared keys instead of an open system, be sure to define at least one static WEP key for user authentication and data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

Wi-Fi Protected Access (WPA)

WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks.

The access point supports the following WPA components and features:

- **IEEE 802.1x and the Extensible Authentication Protocol (EAP):** WPA employs 802.1x as its basic framework for user authentication and dynamic key management. The 802.1x client and RADIUS server should use an appropriate EAP type—such as EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS), or PEAP (Protected EAP)—for strongest authentication. Working together, these protocols provide “mutual authentication” between a client, the access point, and a RADIUS server that prevents users from accidentally joining a rogue network. Only when a RADIUS server has authenticated a user’s credentials will encryption keys be sent to the access point and client.

Note: To implement WPA on wireless clients requires a WPA-enabled network card driver and 802.1x client software that supports the EAP authentication type that you want to use. Windows XP provides native WPA support, other systems require additional software.

- **Temporal Key Integrity Protocol (TKIP):** WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. Basically, TKIP starts with a master (temporal) key for each user session and then mathematically generates other keys to encrypt each data packet. TKIP provides further

data encryption enhancements by including a message integrity check for each packet and a re-keying mechanism, which periodically changes the master key.

- **WPA Pre-Shared Key (PSK) Mode:** For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

WPA2 – WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption. The main differences and enhancements in WPA2 can be summarized as follows:

- **Advanced Encryption Standard (AES):** WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. The AES-CCMP encryption cipher is specified as a standard requirement for WPA2. However, the computationally intensive operations of AES-CCMP requires hardware support on client devices. Therefore to implement WPA2 in the network, wireless clients must be upgraded to WPA2-compliant hardware.
- **WPA2 Mixed-Mode:** WPA2 defines a transitional mode of operation for networks moving from WPA security to WPA2. WPA2 Mixed Mode allows both WPA and WPA2 clients to associate to a common SSID interface. In mixed mode, the unicast encryption cipher (TKIP or AES-CCMP) is negotiated for each client. The access point advertises its supported encryption ciphers in beacon frames and probe responses. WPA and WPA2 clients select the cipher they support and return the choice in the association request to the access point. For mixed-mode operation, the cipher used for broadcast frames is always TKIP. WEP encryption is not allowed.
- **Key Caching:** WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns reauthentication is not required. When a WPA2 client is first authenticated, it receives a Pairwise Master Key (PMK) that is used to generate other keys for unicast data encryption. This key and other client information form a Security Association that the access point names and holds in a cache.
- **Preauthentication:** Each time a client roams to another access point it has to be fully re-authenticated. This authentication process is time consuming and can disrupt applications running over the network. WPA2 includes a mechanism, known as preauthentication, that allows clients to roam to a new access point and be quickly associated. The first time a client is authenticated to a wireless network it has to be fully authenticated. When the client is about to roam to another access point in the network, the access point sends preauthentication messages to the new access point that include the client's security association information. Then when the client sends an association request to the new access point the client is known to be already authenticated, so it proceeds directly to key exchange and association.

Configuring Static WEP

Static shared WEP keys is the basic level of security defined for IEEE 802.11 wireless networks. All clients share the same keys, which are used for user authentication and data encryption. Up to four keys can be specified. These four keys are used for all VAP interfaces on the same radio.

Using the CLI

To enable WEP shared key security for the 802.11g interface, use the **interface wireless g** command from the CLI configuration mode to access the interface mode for the 802.11g radio. First use the **key** command to define up to four keys that can be used for all VAP interfaces. Then use the **vap** command to access each VAP interface to configure other security settings. From the VAP interface configuration mode, use the **authentication** command to enable WEP shared-key authentication. Then set one key as the transmit key for the VAP interface using the **transmit-key** command.

```
Foundry AP(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless g)#key 1 128 ascii abcdeabcdeabc
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless g: VAP[0])#authentication shared
802.1X is set to Disabled.
Data Encryption is set to Enabled.
Foundry AP(if-wireless g: VAP[0])#transmit-key 1
Foundry AP(if-wireless g: VAP[0])#end
```

Note that **authentication shared** command automatically enables WEP encryption and disables 802.1x.

To enable WEP-only encryption without authentication, use the **encryption** command to enable WEP encryption and leave authentication as “open” (the default).

```
Foundry AP(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless g)#key 1 128 ascii abcdeabcdeabc
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless g: VAP[0])#encryption
Foundry AP(if-wireless g: VAP[0])#transmit-key 1
Foundry AP(if-wireless g: VAP[0])#end
```

Note: If you reconfigure the access point from WPA or WPA2 security to WEP only, be sure to first use the **no 802.1x** command to disable 802.1X for the VAP interface.

To view the current 802.11g security settings, use the **show interface wireless g** command from the Exec level.

```

Foundry AP#show interface wireless g

Wireless Interface Information
=====
-----Identification-----
Description                : Foundry 802.11g Access Point
SSID                      : Foundry AP 0
BSSID                    : 00-0C-DB-84-40-80
Channel                   : 11 (AUTO)
Status                    : Disable
-----802.11 Parameters-----
Radio Mode                : 802.11b+g
Transmit Power            : FULL (13 dBm)
Max Station Data Rate     : 54Mbps
Multicast Data Rate       : 54Mbps
Fragmentation Threshold   : 2346 bytes
RTS Threshold             : 2347 bytes
Beacon Interval           : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval : 30 Mins
DTIM Interval             : 2 beacons
Preamble Length           : LONG
Maximum Association       : 64 stations
VLAN ID                   : 1
-----Security-----
Closed System              : DISABLED
Multicast cipher           : WEP
Unicast cipher             : TKIP and AES
WPA clients                : SUPPORTED
WPA Key Mgmt Mode          : PRE SHARED KEY
WPA PSK Key Type           : HEX
PMKSA Lifetime            : 720 minutes
Encryption                 : 128-BIT ENCRYPTION
Default Transmit Key       : 1
Common Static Keys         : Key 1: *****   Key 2: EMPTY
                           : Key 3: EMPTY     Key 4: EMPTY
Pre-Authentication         : Disabled
Authentication Type         : SHARED
-----Antenna-----
Antenna Control method     : Full diversity
Antenna ID                 : Integrated
-----Authentication Parameters-----
802.1x                     : DISABLED
Broadcast Key Refresh Rate : 120 min
Session Key Refresh Rate   : 120 min
802.1x Session Timeout Value : 0 min
=====
Foundry AP#

```

authentication

This command defines the 802.11 authentication type allowed by the VAP interface.

Syntax

authentication <open | shared | wpa | wpa-psk | wpa-wpa2-mixed | wpa-wpa2-psk-mixed | wpa2 | wpa2-psk> <required | supported>

- **open** - Accepts the client without verifying its identity using a shared key. “Open” authentication means either there is no encryption (if encryption is disabled) or WEP-only encryption is used (if encryption is enabled).
- **shared** - Authentication is based on a shared key that has been distributed to all stations. If encryption is enabled, “shared” authentication uses WEP-only encryption.
- **wpa** - Clients using WPA are accepted for authentication.
- **wpa-psk** - Clients using WPA Pre-shared Key are accepted for authentication.
- **wpa-wpa2-mixed** - Clients using WPA or WPA2 are accepted for authentication.
- **wpa-wpa2-psk-mixed** - Clients using WPA or WPA2 Pre-shared Key are accepted for authentication.
- **wpa2** - Clients using WPA2 are accepted for authentication.
- **wpa2-psk** - Clients using WPA2 Pre-shared Key are accepted for authentication.
- **required** - Clients are required to use WPA or WPA2.
- **supported** - Clients may use WPA or WPA2, if supported.

Default Setting

open

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- Shared key authentication can only be used when WEP-only is enabled with the **encryption** command, and at least one static WEP key has been defined with the **key** command.
- When WPA or WPA2 is selected, clients are authenticated using 802.1x via a RADIUS server. Each client has to be WPA-enabled or support 802.1X client software. A RADIUS server must also be configured and be available in the wired network.
- When the WPA or WPA2 Pre-shared Key mode is used, the key must first be generated and distributed to all wireless clients before they can successfully associate with the access point. Use the **wpa-preshared-key** command to configure the key.
- WPA2 defines a transitional mode of operation for networks moving from WPA security to WPA2. WPA2 Mixed Mode allows both WPA and WPA2 clients to associate to a common VAP interface. When the encryption cipher suite is set to TKIP, the unicast encryption cipher (TKIP or AES-CCMP) is negotiated for each client. The access point advertises it's supported encryption ciphers in beacon frames and probe responses. WPA and WPA2 clients select the cipher they support and return the choice in the association request to the access point. For mixed-mode operation, the cipher used for broadcast frames is always TKIP. WEP encryption is not allowed.
- The “required” option places the VAP into TKIP only mode. The “supported” option places the VAP into TKIP+AES+WEP mode. The “required” mode is used in WPA-only environments.

The “supported” mode can be used for mixed environments with legacy WPA products, specifically WEP. (For example, WPA+WEP. The WPA2+WEP environment is not available

because WPA2 does not support WEP). To place the VAP into AES only mode, use “required” and then select the “cipher-ccmp” option for the **cipher-suite** command.

encryption

This command defines whether or not data encryption is used to provide privacy for wireless communications. Use the **no** form to disable encryption.

Syntax

encryption
no encryption

Default Setting

disabled

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. For more secure data transmissions, enable data encryption with this command, and set at least one static WEP key with the **key** command.
- The WEP settings must be the same on each client in your wireless network.
- Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.
- You must enable data encryption in order to enable all types of encryption (WEP, TKIP, and AES) in the access point.

key

This command sets the keys used for WEP encryption. Use the **no** form to delete a configured key.

Syntax

key *<index>* *<size>* *<type>* *<value>*
no key *index*

- *index* - Key index. (Range: 1-4)
- *size* - Key size. (Options: 64, 128, or 152 bits)
- *type* - Input format. (Options: ASCII, HEX)
- *value* - The key string.
 - – For 64-bit keys, use 5 alphanumeric characters or 10 hexadecimal digits.
 - – For 128-bit keys, use 13 alphanumeric characters or 26 hexadecimal digits.
 - – For 152-bit keys, use 16 alphanumeric characters or 32 hexadecimal digits.

Note: The 152-bit key applies only to the 802.11a wireless interface.

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Command Usage

- To enable Wired Equivalent Privacy (WEP), use the **authentication shared** command to select shared key authentication, use the **encryption** command to enable data encryption, and use the **key** command to configure at least one key.
- If WEP is enabled, all wireless clients must be configured with the same shared keys to communicate with the access point.

transmit-key

This command sets the index of the key to be used for encrypting data frames broadcast or multicast from the VAP interface to wireless clients.

Syntax

transmit-key <index>

index - Key index. (Range: 1-4)

Default Setting

1

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- If you use WEP key encryption, the VAP interface uses the transmit key to encrypt multicast and broadcast data signals that it sends to client devices. Other keys can be used for decryption of data from clients.
- When using IEEE 802.1x, the access point uses a dynamic WEP key to encrypt unicast and broadcast messages to 802.1x-enabled clients. However, because the access point sends the WEP keys during the 802.1x authentication process, these keys do not have to appear in the client's WEP key list.
- In a mixed-mode environment with clients using static WEP keys and WPA, select WEP transmit key index 2, 3, or 4. The access point uses transmit key index 1 for the generation of dynamic keys.

Using the Web Management Interface

To configure a VAP interface to use static WEP shared keys, follow these steps:

1. From the Radio Interface 802.11a menu or Radio Interface 802.11g menu, click Radio Settings.
2. Select the type of key to enter, hexadecimal or alphanumeric.

FOUNDRY NETWORKS *IronPoint™ 200* [Logout](#)

WEP Key Setting

Interface	Key Number
VAP 0	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 1	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 2	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4
VAP 3	<input checked="" type="radio"/> Key 1 <input type="radio"/> Key 2 <input type="radio"/> Key 3 <input type="radio"/> Key 4

Key Number	Key Length	Key Type	Key
Key 1	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 2	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 3	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	
Key 4	<input type="radio"/> 64 Bit <input type="radio"/> 128 Bit <input type="radio"/> 152 Bit <input checked="" type="radio"/> None	<input checked="" type="radio"/> Hex <input type="radio"/> ASCII	

Hex: For 64 Bit enter 10 digits, for 128 Bit enter 26 digits, for 152 Bit enter 32 digits
 ASCII: For 64 Bit enter 5 characters, for 128 Bit enter 13 characters, for 152 Bit enter 16 characters

Note: On the Web interface, the key type you select for WEP keys applies only to keys that you are currently entering. It does not reflect the key types of existing WEP keys stored in the access point's configuration file.

You can have up to four WEP keys, which can be in hexadecimal or alphanumeric format and have different key lengths.

3. Select the required key length, 64-bit, 128-bit, or 152-bit.

Note: The 152-bit key applies only to the 802.11a wireless interface.

4. Enter the key.
5. To enter more than one key, repeat Step 3 through Step 4.
6. Select the transmit key that the VAP interface will use at the current time. If more than one key is entered, you can select different keys for each VAP interface. You can also change to a different key from time to time to provide additional security.
7. Click Apply.
8. From the Radio Interface 802.11a menu or the Radio Interface 802.11g, click Security.
9. For the VAP interface using static WEP keys, click More.
10. Set Authentication to User Shared Key.
11. Enable WEP Encryption.
12. Click Apply.

Configurable Parameters

VAP Transmit Key Select – Selects the key number to use for encryption for each VAP interface. If the clients have all four keys configured to the same values, you can change the encryption key to any of the four settings without having to update the client keys.

Note: In a mixed-mode environment with clients using static WEP keys and WPA, select WEP transmit key index 2, 3, or 4. The access point uses transmit key index 1 for the generation of dynamic keys.

Key Length – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. (Default: 128 Bit)

Note: The 152-bit key applies only to the 802.11a wireless interface.

Key Type – Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys:

- **Hexadecimal:** Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys.
- **Alphanumeric:** Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys.

Authentication – Sets the VAP interface to communicate as an open system that accepts network access attempts from any client, or with clients using 802.1x authentication or pre-configured static shared keys. (Default: Open)

- **802.1x:** Enables 802.1x authentication. Select this option when using dynamic WEP keys, or dynamic WPA or WPA2 security.
- **Pre-Shared Key:** Sets the VAP interface to use WPA or WPA2 pre-shared keys.
- **User Shared Key:** Sets the VAP interface to use WEP-only shared keys, if encryption is enabled. If this option is selected, you must configure at least one key on the access point and all clients.
- **Open:** If you don't set up any authentication on the VAP interface, the network either has no encryption, if encryption is not enabled, or WEP-only encryption, if encryption is enabled. If there is no authentication and no encryption, then the network has no protection and is open to all users. "Open" is the default setting.

Encryption – Enable or disable the VAP interface to use data encryption (WEP shared keys, WPA or WPA2). When WEP encryption is selected, you must configure at least one key on the access point and all clients. (Default: Disable)

Configuring WPA or WPA2 Pre-Shared Key

The WPA Pre-Shared Key security uses a single key for authentication that is manually distributed to all clients.

Using the CLI

The following example shows how to enable WPA Pre-shared Key security for VAP interface “0” on the 802.11g radio. From the CLI 802.11g interface configuration mode, use the **vap** command to access VAP interface configuration. Use the **authentication** command to set the VAP interface to “wpa-psk.” The **authentication** command automatically enables data encryption and sets the appropriate WPA mode and encryption ciphers. To enter a key value, use the **wpa-preshared-key** command to specify a hexadecimal or pass-phrase key and define the key. You can use the **cipher-suite** command to force specific unicast and multicast encryption ciphers. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

```
Foundry AP(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless g: VAP[0])#authentication wpa-psk required
Data Encryption is set to Enabled.
WPA2 Clients Mode is set to Disabled.
WPA Clients Mode is set to Required.
WPA Multicast Cipher is set to TKIP.
WPA Unicast Cipher can accept TKIP only.
WPA Authentication is set to Pre-Shared Key.
Foundry AP(if-wireless g: VAP[0])#wpa-preshared-key passphrase-key agoodsecret
Foundry AP(if-wireless a: VAP[0])#cipher-suite wep
Authentication mode is changed to WPA-TKIP-WEP due to multicas cipher is changed
to WEP.
Unicast Ciphers can accept TKIP only.
Multicast Cipher is set to WEP.
Foundry AP(if-wireless g: VAP[0])#
```

cipher-suite

This command defines the unicast and multicast encryption ciphers when using WPA or WPA2 security.

Syntax

cipher-suite <aes-ccmp | tkip | wep>

- **aes-ccmp** - Use AES-CCMP encryption for the unicast and multicast cipher.
- **tkip** - Use TKIP encryption for the multicast cipher. When WPA is set to “required,” TKIP is used for the unicast cipher. When WPA is set to “supported,” TKIP or AES-CCMP can be used for the unicast cipher depending on the capability of the client.
- **wep** - Use WEP encryption for the multicast cipher. When WPA is set to “required,” TKIP is used for the unicast cipher. When WPA is set to “supported,” TKIP or AES-CCMP can be used for the unicast cipher depending on the capability of the client.

Default Setting

wep

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- WPA enables the access point to support different unicast encryption keys for each client. However, the global encryption key for multicast and broadcast traffic must be the same for all clients.
- If any clients supported by the access point are not WPA enabled, the multicast-cipher algorithm must be set to WEP.
- WEP is the first generation security protocol used to encrypt data crossing the wireless medium using a fairly short key. Communicating devices must use the same WEP key to encrypt and decrypt radio signals. WEP has many security flaws, and is not recommended for transmitting highly sensitive data.
- TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
- TKIP defends against attacks on WEP in which the unencrypted initialization vector in encrypted packets is used to calculate the WEP key. TKIP changes the encryption key on each packet, and rotates not just the unicast keys, but the broadcast keys as well. TKIP is a replacement for WEP that removes the predictability that intruders relied on to determine the WEP key.
- AES-CCMP (Advanced Encryption Standard Counter-Mode/CBCMAC Protocol): WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES-CCMP encryption cipher is specified as a standard requirement for WPA2 and provides extremely robust data confidentiality using a 128-bit key. However, the computationally intensive operations of AES-CCMP requires hardware support on client devices. Therefore to implement WPA2 in the network, wireless clients must be upgraded to WPA2-compliant hardware.

wpa-preshared-key

This command defines a WPA or WPA2 preshared-key.

Syntax

wpa-preshared-key <hex | passphrase-key> <value>

- **hex** - Specifies hexadecimal digits as the key input format.
- **passphrase-key** - Specifies an ASCII pass-phrase string as the key input format.
- **value** - The key string. For ASCII input, specify a string between 8 and 63 characters. For HEX input, specify exactly 64 digits.

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- To support WPA or WPA2 for client authentication, use the **authentication** command to specify the authentication type, use the **wpa-preshared-key** command to specify one static key.
- If WPA or WPA2 is used in pre-shared-key mode, all wireless clients must be configured with the same pre-shared key to communicate with the access point VAP interface.

Using the Web Management Interface

To configure a VAP interface to use WPA Pre-shared Key, follow these steps:

1. From the Radio Interface 802.11a menu or the Radio Interface 802.11g menu, click Security.
2. For the VAP interface using WPA Pre-shared Key, click More.



3. Set Authentication to Pre-Shared Key.
4. Set Encryption to WPA-TKIP.
5. Select the WPA key type to enter, hexadecimal or alphanumeric.
6. Enter the key value in the WPA Pre-shared Key text field.
7. Click Apply.

Configurable Parameters

Authentication – Sets the VAP interface to communicate as an open system that accepts network access attempts from any client, or with clients using 802.1x authentication or pre-configured static shared keys. (Default: Open System)

- **802.1x:** Enables 802.1x authentication. Select this option when using dynamic WEP keys, or dynamic WPA or WPA2 security.
- **Pre-Shared Key:** Sets the VAP interface to use WPA or WPA2 pre-shared keys. When Pre-Shared Key is selected, you must define the type and value of the key under Pre-Shared Key Setting.
- **User Shared Key:** Sets the VAP interface to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients.

- **Open:** If you don't set up any other security mechanism on the VAP interface, the network has no protection and is open to all users. This is the default setting.

Encryption – Enable or disable the VAP interface to use data encryption (WEP shared keys, WPA or WPA2). For WPA Pre-Shared Key security, select one of the following encryption cipher options:

- **WPA-TKIP:** Use TKIP encryption for the multicast cipher. TKIP or AES-CCMP can be used for the unicast cipher under "supported" mode depending on the capability of the client. Under the WPA "required" mode, only the TKIP unicast cipher is allowed.
- **TKIP-WEP Mixed Mode:** Use WEP encryption for the multicast cipher. TKIP or AES-CCMP can be used for the unicast cipher depending on the capability of the client.
- **WPA2-AES CCMP:** Use AES-CCMP encryption for the unicast and multicast cipher.
- **AES-TKIP Mixed Mode:** Use TKIP encryption for the multicast cipher. TKIP or AES-CCMP can be used for the unicast cipher depending on the capability of the client.

WPA Pre-Shared Key Type – If the WPA pre-shared-key mode is used, all wireless clients must be configured with the same key to communicate with the VAP interface. (Default: Alphanumeric)

- **Hexadecimal:** Enter a key as a string of 64 hexadecimal numbers.
- **Alphanumeric:** Enter a key as an easy-to-remember form of letters and numbers. The string must be from 8 to 63 characters, which can include spaces.

Configuring WPA and WPA2 over 802.1x

WPA and WPA2 security use IEEE 802.1x and a RADIUS server for user authentication. Before enabling WPA or WPA2, be sure to have a configured RADIUS server available in the network and to set up the access point's RADIUS connection parameters.

See "RADIUS Client Settings" on page 15-1.

Using the CLI

The following example shows how to enable WPA over 802.1x security for a VAP interface on the 802.11g radio. From the CLI 802.11g interface configuration mode, use the **vap** command to access VAP interface configuration. Use the **authentication** command to set the VAP interface to "**wpa required**" and automatically enable data encryption, set the 802.1x and WPA modes, and configure the cipher suite. With 802.1x enabled you can also set appropriate key refresh rates and an

authentication timeout (for more information, see page 19-7). To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

```
Foundry AP(config)#interface wireless g
Enter Wireless configuration commands, one per line.
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless a: VAP[0])#authentication wpa required
Data Encryption is set to Enabled.
WPA2 Clients mode is set to Disabled.
WPA Clients Mode is set to Required.
WPA Multicast Cipher is set to TKIP.
WPA Unicast Cipher can accept TKIP only.
WPA Authentication is set to 802.1X Required.
Foundry AP(if-wireless g: VAP[0])#802.1x broadcast-key-refresh-rate 100
Foundry AP(if-wireless g: VAP[0])#802.1x session-timeout 30
Foundry AP(if-wireless g: VAP[0])#
```

Using WPA2 over 802.1x also allows you to enable pre-authentication and set the PMKSA lifetime. From the VAP interface configuration level, use the **802.1x pre-authentication** command to enable this feature for fast roaming. Use the **pmksa-lifetime** command to set the maximum time for fast roam back capability.

```
Foundry AP(if-wireless a: VAP[0])#802.1x pre-authentication enable
Foundry AP(if-wireless g: VAP[0])#pmksa-lifetime 60
Foundry AP(if-wireless g: VAP[0])#
```

802.1x pre-authentication

This command enables WPA2 pre-authentication for fast secure roaming.

Syntax

802.1x pre-authentication <enable | disable>

- **enable** - Enables pre-authentication for the VAP interface.
- **disable** - Disables pre-authentication for the VAP interface.

Default Setting

Disabled

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- Each time a client roams to another access point it has to be fully re-authenticated. This authentication process is time consuming and can disrupt applications running over the network. WPA2 includes a mechanism, known as pre-authentication, that allows clients to roam to a new access point and be quickly associated. The first time a client is authenticated to a wireless network it has to be fully authenticated. When the client is about to roam to another access point in the network, the access point sends pre-authentication messages to the new access point that include the client's security association information. Then when the client sends an association request to the new access point the client is known to be already authenticated, so it proceeds directly to key exchange and association.

- To support pre-authentication, both clients and access points in the network must be WPA2 enabled.
- Pre-authentication requires all access points in the network to be on the same IP subnet.

Example

```
Foundry AP(if-wireless a: VAP[0])#802.1x pre-authentication enable
Foundry AP(if-wireless a: VAP[0])#
```

pmksa-lifetime

This command sets the time for aging out cached WPA2 Pairwise Master Key Security Association (PMKSA) information for fast roaming.

Syntax

pmksa-lifetime <minutes>

minutes - The time for aging out PMKSA information. (Range: 1 - 1400 minutes)

Default Setting

720 minutes

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns reauthentication is not required.
- When a WPA2 client is first authenticated, it receives a Pairwise Master Key (PMK) that is used to generate other keys for unicast data encryption. This key and other client information form a Security Association that the access point names and holds in a cache. The lifetime of this security association can be configured with this command. When the lifetime expires, the client security association and keys are deleted from the cache. If the client returns to the access point, it requires full reauthentication.
- The access point can store up to 256 entries in the PMKSA cache.

Example

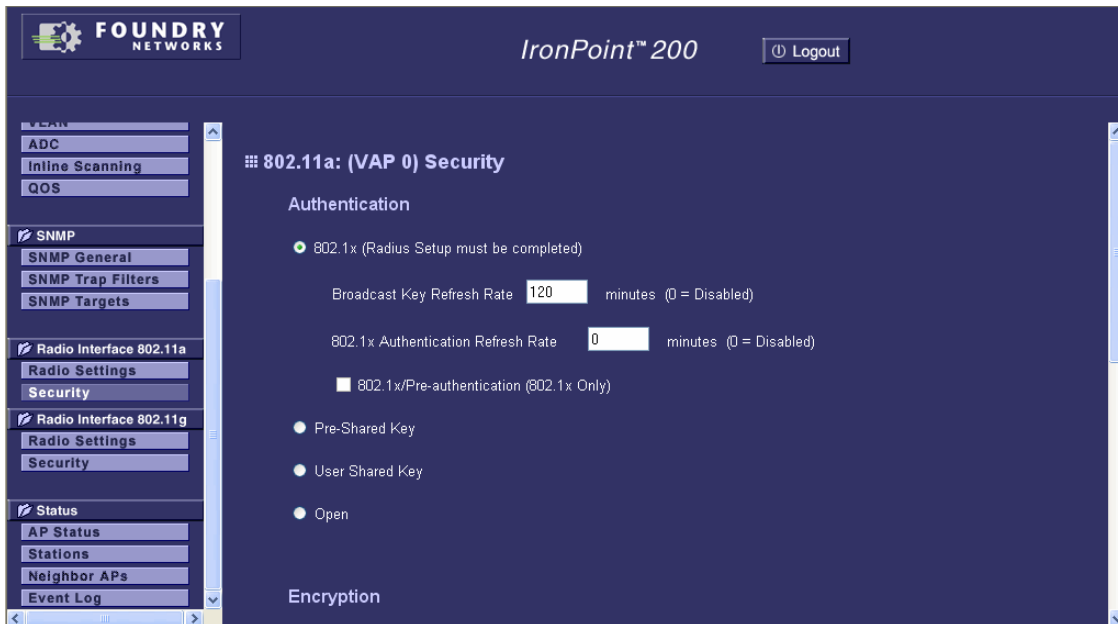
```
Foundry AP(if-wireless a: VAP[0])#pmksa-lifetime 300
Foundry AP(if-wireless a: VAP[0])#
```

Using the Web Management Interface

To configure a VAP interface to use WPA over 802.1x, first be sure to set up the RADIUS server details on the Radius page (see page 15-6), then follow these steps:

1. From the Radio Interface 802.11a menu or the 802.11g Radio Interface menu, click Security.

- For the VAP interface using WPA over 802.1x, click More.



- Set Authentication to 802.1x. (For more information on 802.1x configuration, see page 19-7.)
- Enter appropriate refresh rate for broadcast encryption keys.
- Enter a timeout to force 802.1x re-authentication for clients.
- Set Encryption to WPA-TKIP.
- Click Apply.

Configurable Parameters

Authentication – Sets the VAP interface to communicate as an open system that accepts network access attempts from any client, or with clients using 802.1x authentication or pre-configured static shared keys. (Default: Open System)

- 802.1x:** Enables 802.1x authentication. Select this option when using WPA or WPA2 over 802.1x.
- 802.1x/Pre-authentication(802.1x Only):** Enables pre-authentication, which allows clients to roam to a new access point and be quickly associated without performing full 802.1x authentication. (Default: Disabled)
- Pre-Shared Key:** Sets the VAP interface to use WPA or WPA2 pre-shared keys. When Pre-Shared Key is selected, you must define the type and value of the key under Pre-Shared Key Setting.
- User Shared Key:** Sets the VAP interface to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients.
- Open:** If you don't set up any other security mechanism on the VAP interface, the network has no protection and is open to all users. This is the default setting.

Encryption – Enable or disable the VAP interface to use data encryption (WEP shared keys, WPA or WPA2). For WPA or WPA2 over 802.1x security, select one of the following encryption cipher options. For WPA2 over 802.1x security, you can also enable pre-authentication:

- **WPA-TKIP:** Use TKIP encryption for the multicast cipher. TKIP or AES-CCMP can be used for the unicast cipher under "supported" mode depending on the capability of the client. Under the WPA "required" mode, only the TKIP unicast cipher is allowed.
- **TKIP-WEP Mixed Mode:** Use WEP encryption for the multicast cipher. TKIP or AES-CCMP can be used for the unicast cipher depending on the capability of the client.
- **WPA2-AES CCMP:** Use AES-CCMP encryption for the unicast and multicast cipher.
- **AES-TKIP Mixed Mode:** Use TKIP encryption for the multicast cipher. TKIP or AES-CCMP can be used for the unicast cipher depending on the capability of the client.

Web Management Interface Advanced Security

From the VAP interface Security page, you can click on the "Advanced" button to access a detailed security page where other security settings are available.



If security settings have been made using the CLI that can only be configured from the Advanced page, this page automatically displays instead of the basic security page.

From the bottom of the Advanced security page, click the "Basic" button to return to the basic VAP interface security page.

For the authentication type selected, only the relevant settings are displayed. Settings that do not apply for the authentication type are hidden.



Configurable Parameters

802.1X Setup – IEEE 802.1X is the standard framework for network access authentication used for WPA and WPA2. The 802.1X authentication packets are also used to pass unicast session keys and broadcast keys to wireless clients. When 802.1X is enabled, the broadcast and session key rotation intervals can also be configured.

- **Disabled** – 802.1X authentication is disabled for the VAP interface.
- **Supported** – The access point supports 802.1X authentication only for clients initiating the 802.1X authentication process (i.e., the access point does not initiate 802.1X authentication). For clients initiating 802.1X, only those successfully authenticated are allowed to access the network. For those clients not initiating 802.1X, access to the network is allowed after successful wireless association with the access point. The 802.1X supported mode allows access for clients not using WPA or WPA2 security.
- **Required** – The access point enforces 802.1X authentication for all associated wireless clients. If 802.1X authentication is not initiated by a client, the access point will initiate authentication. Only those clients successfully authenticated with 802.1X are allowed to access the network.
- **Broadcast Key Refresh Rate** – Sets the interval at which the broadcast keys are refreshed for stations using 802.1X dynamic keying. (Range: 0, 60-1440 minutes; Default: 0 means disabled)
- **802.1X Reauthentication Refresh Rate** – The time period after which a connected client must be re-authenticated. During the re-authentication process of verifying the client's credentials on the RADIUS server, the client remains connected the network. Only if re-authentication fails is network access blocked. (Range: 0, 60-1440 seconds; Default: 0 means disabled)

Encryption – Enable or disable the access point to use data encryption (WEP, TKIP, or AES-CCMP). If encryption is enabled when set to Open System, you must configure at least one WEP key on the access point and all clients. (Default: Disabled)

Authentication Setup – Sets the access point as an open system or using one of the following security settings. Relevant options are displayed when a security setting is selected, other settings that do not apply are hidden.

- **Open System:** If you don't set up any other security mechanism on the access point, the network has no protection and is open to all users. This is the default setting.
- **Shared Key:** Sets the access point to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients. You can manually disable encryption to use WEP keys for authentication only.
- **wpa:** Clients using WPA over 802.1X are accepted for authentication.
- **wpa2:** Clients using WPA2 over 802.1X are accepted for authentication.
- **wpa-wpa2-mixed:** Clients using WPA or WPA2 over 802.1X are accepted for authentication.
- **wpa-psk:** Clients using WPA Pre-shared Key are accepted for authentication.
- **wpa2-psk:** Clients using WPA2 Pre-shared Key are accepted for authentication.
- **wpa-wpa2-psk-mixed:** Clients using WPA or WPA2 Pre-shared Key are accepted for authentication.

WPA Configuration – Each interface can be configured to allow only WPA-enabled clients to access the network (Required), or to allow access to both WPA and WEP clients (Supported). (Default: Required)

Multicast Cipher Mode – Selects an encryption method for the global key used for multicast and broadcast traffic, which is supported by all wireless clients.

- **WEP:** WEP is used as the multicast encryption cipher. You should select WEP only when both WPA and WEP clients are supported.
- **TKIP:** TKIP is used as the multicast encryption cipher. Select TKIP when there are clients that may not support AES encryption.
- **AES-CCMP:** AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. If clients in the network are not WPA2 compliant, use TKIP encryption.

WPA Pre-Shared Key Type – If the WPA or WPA2 pre-shared-key mode is used, all wireless clients must be configured with the same key to communicate with the access point.

- **Hexadecimal:** Enter a key as a string of 64 hexadecimal numbers.
- **Alphanumeric:** Enter a key as an easy-to-remember form of letters and numbers. The string must be from 8 to 63 characters, which can include spaces.

Changing Encryption Types

You can change the encryption types used on the access points. However, for encryptions that use shared or pre-shared keys, if you change from one encryption type to another then back to the previous type, you must re-enter the keys. The keys that were previously entered may not be available in the access point's configuration file.

Chapter 23

VLAN Support

The access point can employ VLAN tagging support to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. There can be a VLAN assigned to each associated client and a management VLAN for the access point.

Note the following points about the access point's VLAN support:

- The management VLAN is for managing the access point. For example, the access point allows traffic that is tagged with the specified VLAN to manage the access point via remote management, SSH, SNMP, Telnet, etc.
- Each wireless client associated to the access point is assigned to the default VLAN ID for the VAP interface. If IEEE 802.1x is being used to authenticate wireless clients, specific VLAN IDs can be configured on the RADIUS server to be assigned to each client. The access point allows traffic tagged with assigned VLAN IDs or default VLAN IDs to access clients associated on the VAP interface.
- When VLAN support is enabled, the access point tags traffic passing to the wired network with the appropriate VLAN ID, either an assigned client VLAN ID, default VLAN ID, or the management VLAN ID. Traffic received from the wired network must also be tagged with one of these known VLAN IDs. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passing to the wired network and ignores the VLAN tags on any received frames.

Note: Before enabling the VLAN feature on the access point, you must setup the network switch port to support tagged VLAN packets from the access point. The switch port must also be configured to accept the access point's management VLAN ID, assigned client VLAN IDs, and default VLAN IDs. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Using IEEE 802.1x and a central RADIUS server, up to 64 VLAN IDs can be mapped to specific wireless clients, allowing users to remain within the same VLAN as they move around a campus site. This feature can also be used to control access to network resources from clients, thereby improving security.

A VLAN ID (1-4094) can be assigned to a client after successful IEEE 802.1x authentication. The client VLAN IDs must be configured on the RADIUS server for each user authorized to access the

network. If a client does not have a configured VLAN ID on the RADIUS server, the access point assigns the client to the configured default VLAN ID for the VAP interface.

Note: When using IEEE 802.1x to dynamically assign VLAN IDs, the access point must have 802.1x authentication enabled and a RADIUS server configured. Wireless clients must also support 802.1x client software.

When setting up VLAN IDs for each client on the RADIUS server, be sure to use the RADIUS attributes and values as indicated in the following table.

Number	RADIUS Attribute	Value
64	Tunnel-Type	VLAN (13)
65	Tunnel-Medium-Type	802
81	Tunnel-Private-Group-ID	VLANID (1 to 4094 as hexadecimal digits or a string)

Note: VLAN IDs on the RADIUS server can be entered as hexadecimal digits or a string (see “radius-server vlan-format” on page 15-5). The specific configuration of RADIUS server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS server software.

Enabling VLAN Support

Use the CLI or Web Management Interface to enable VLAN support for the access point.

Using the CLI

To enable VLAN support on the access point, first use the **management-vlanid** command from the CLI configuration mode to set the default VLAN ID for the Ethernet interface. You can also set the default VLAN ID for each VAP interface (see “vlan-id” on page 23-4). Then, enable VLANs using the **vlan enable** command. When you change the access point’s VLAN support setting, you must reboot the access point to implement the change. To view the current VLAN settings, use the **show system** command.

```
Foundry AP(config)#management-vlanid 3
Foundry AP(config)#vlan enable
Reboot system now? <y/n>: y
```

management-vlanid

This command configures the management VLAN ID for the access point Ethernet port.

Syntax

management-vlanid <vlan-id>

vlan-id - Management VLAN ID. (Range: 1-4094)

Default Setting

1

Command Mode

Global Configuration

Command Usage

- The management VLAN is for managing the access point. For example, the access point allows traffic that is tagged with the specified VLAN to manage the access point via remote management, SSH, SNMP, Telnet, etc.

vlan

This command enables VLANs for all traffic. Use the **no** form to disable VLANs.

Syntax

vlan enable
no vlan

Default

Disabled

Command Mode

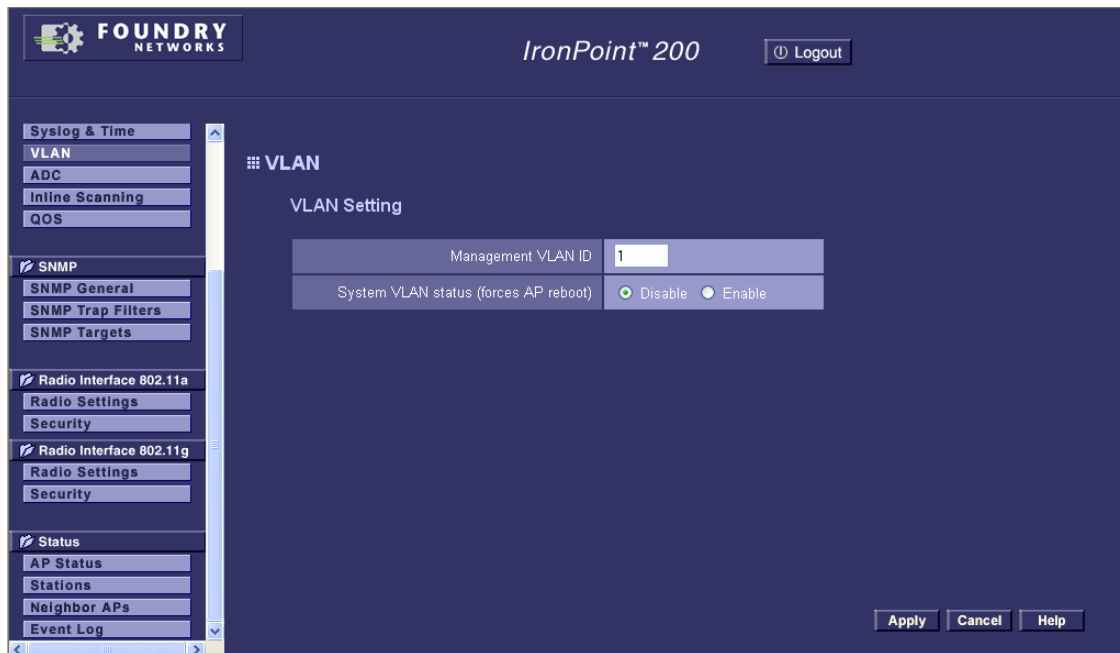
Global Configuration

Command Usage

- Changing the VLAN status of the access point forces a system reboot.
- When VLANs are enabled, the access point tags frames received from wireless clients with the default VLAN ID for the VAP interface. If IEEE 802.1x is being used to authenticate wireless clients, specific VLAN IDs can be configured on the RADIUS server to be assigned to each client. Using IEEE 802.1x and a central RADIUS server, up to 64 VLAN IDs can be mapped to specific wireless clients.
- If the VLAN ID has not been configured for a client on the RADIUS server, then the frames are tagged with the default VLAN ID of the VAP interface.
- When using IEEE 802.1x to dynamically assign VLAN IDs, the access point must have 802.1x authentication enabled and a RADIUS server configured. Wireless clients must also support 802.1x client software.
- Traffic entering the Ethernet port must be tagged with a VLAN ID that matches the access point's management VLAN ID, a VAP interface default VLAN ID, or with a VLAN tag that matches one of the wireless clients currently associated with the access point.

Using the Web Management Interface

From the System menu, click VLAN. To configure the access point to support VLANs, set VLAN to Enable and specify a management VLAN ID. Click Apply.



Configurable Parameters

Management VLAN ID – The VLAN ID that traffic must have to be able to manage the access point. (Range 1-4094; Default: 1)

System VLAN Status (forces AP reboot) – Enables or disables VLAN tagging support on the access point. Changing this parameter automatically reboots the access point. (Default: Disable)

Setting Default VLAN IDs

The access point allows a default VLAN ID to be assigned to each VAP interface.

Using the CLI

Use the **interface wireless** command to access the CLI configuration mode for the radio interface, then use the **vlan-id** command to assign a VLAN ID.

```
Foundry AP(config)#interface wireless g
Foundry AP(if-wireless g)#vap 0
Foundry AP(if-wireless g: VAP[0])#vlan-id 3
Foundry AP(if-wireless g: VAP[0])#
```

vlan-id

This command configures the default VLAN ID for the VAP interface.

Syntax

vlan-id <vlan-id>

vlan-id - default VLAN ID. (Range: 1-4094)

Default Setting

1

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

- To implement the default VLAN ID setting for VAP interface, the access point must enable VLAN support using the **vlan** command.
- When VLANs are enabled, the access point tags frames received from wireless clients with the default VLAN ID for the VAP interface. If IEEE 802.1x is being used to authenticate wireless clients, specific VLAN IDs can be configured on the RADIUS server to be assigned to each client. Using IEEE 802.1x and a central RADIUS server, up to 64 VLAN IDs can be mapped to specific wireless clients.
- If the VLAN ID has not been configured for a client on the RADIUS server, then the frames are tagged with the default VLAN ID of the VAP interface.

Using the Web Management Interface

From the Radio Interface 802.11a menu or Radio Interface 802.11g menu, click Radio Settings. Enter a default VLAN ID for each VAP interface. Click Apply.



Configurable Parameter

Default VLAN ID – The VLAN ID assigned to wireless clients that are not assigned to a specific VLAN by RADIUS server configuration. (Default: 1)

Chapter 24

System Information

Displaying the Access Point Status

Using the CLI or Web Management Interface, the access point provides information on basic system configuration settings, as well as the settings for the wireless interface.

Using the CLI

To view the current access point system settings, use the **show system** command from the Exec mode. To view the current radio interface settings, use the **show interface wireless a** or **show interface wireless g** command (see “show interface wireless” on page 21-15).

show system

This command displays basic system configuration settings.

Syntax

show system

Default Setting

None

Command Mode

Exec

```

Foundry AP(config)#system name IronPoint-AP
Foundry AP#show system

System Information
=====
Serial Number           : AN07290320
System Up time          : 3 days, 4 hours, 7 minutes, 3 seconds
System Name             : Foundry AP
System Location         :
System Contact          : Contact
System Country Code     : US - UNITED STATES
MAC Address             : 00-0C-DB-81-38-F9
IP Address              : 169.254.1.1
Subnet Mask             : 255.255.0.0
Default Gateway         : 169.254.1.254
VLAN State              : Disabled
Management VLAN ID(AP) : 1
ADC State               : Enabled
IAPP State              : Disabled
Inline Scanning         : Disabled
DHCP Client             : Disabled
HTTP Server             : Enabled
HTTP Server Port        : 80
HTTPS Server            : Enabled
HTTPS Server Port       : 443
Slot Status             : Dual band(a/g)
Software Version        : 02.02.02Tw8
SSH Server              : Enabled
SSH Server Port         : 22
Telnet Server           : Enabled
Wireless Broadcast Frame Rate-limit: Aggressive
Wireless Multicast Frame Rate-limit: Normal
=====
Foundry AP#

```

show version

This command displays the software version for the system.

Syntax

show version

Default Setting

None

Command Mode

Exec

Command Usage

See “RF Monitoring” on page 28-1 for additional information on “System Mode”.

Example

```
Foundry AP#show version

Version Information
=====
  Boot Rom Version   : 01.0.04Tv5
  Software Version   : 02.02.02Tv9
  Date               : Jan 10 2008
  Time               : 10:37:16
=====
Foundry AP#
```

show hardware

This command displays the hardware version of the system.

Syntax

show hardware

Default Setting

None

Command Mode

Exec

Example

```
Foundry AP#show hardware

Hardware Version Information
=====
Hardware version R01
=====
Foundry AP#
```

show tech-support

This command displays a complete list of all the system details and configuration settings as displayed by the CLI show commands listed below.

Syntax

show tech-support

Default Setting

None

Command Mode

Exec

- **Country:** The access point's Country Code setting.
- **System Contact:** Administrator responsible for the system.
- **Speed-Duplex Actual:** The current speed and duplex mode of the Ethernet port.
- **Speed-Duplex Configured:** The configured speed and duplex mode of the Ethernet port.
- **IP Address:** IP address of the management interface for this device.
- **IP Default Gateway:** IP address of the gateway router between this device and management stations that exist on other network segments.
- **HTTP Server:** Shows if management access via HTTP is enabled.
- **HTTP Server Port:** Shows the TCP port used by the HTTP interface.
- **HTTP Secure Server:** Shows if management access via secure HTTPS/SSL is enabled.
- **HTTP Secure Server Port:** Shows the TCP port used by the secure HTTPS/SSL interface.
- **Version:** Shows the version number for the runtime code.

AP Wireless Configuration – The AP Wireless Configuration table displays the wireless VAP interface settings listed below.

- **SSID:** The service set identifier for the VAP interface.
- **BSSID:** The basic service set identifier (access point wireless MAC address) for the VAP interface.
- **Radio Channel:** The radio channel through which the access point communicates with wireless clients.
- **Radio Encryption:** The key size used for data encryption.
- **Radio Authentication Type:** Shows if open system or shared key authentication is used.
- **802.1x:** Shows if IEEE 802.1x access control for wireless clients is enabled.

Displaying Wireless Client Information

Using the CLI or Web Management Interface, the access point provides information on the wireless clients currently associated with the access point.

Using the CLI

To view status of clients currently associated with the access point, use the **show station** command from the Exec mode.

The following is an example of the output on an IronPoint 200 running a release prior to software release 02.02.01:

```

Foundry AP#show station g 0

Station Table Information
=====
if-wireless G VAP [0] :
802.11g Channel : 1
      802.11g Channel Station Table
Station Address   : 00-04-E2-41-C2-9D VLAN ID: 0
Authenticated Associated Forwarding KeyType AuthTyp
TRUE             TRUE     TRUE     NONE OPEN
      Counters: pkts Tx / Rx, bytes Tx / Rx
                  44/ 0 6056/ 0
Time:Associated LastAssoc LastDisAssoc LastAuth
                  14644 0 0 0

=====
Foundry AP#

```

The output of the command shows the following:

- MAC address of the wireless client associated with the radio
- Whether or not the wireless client has been authenticated
- Whether or not the wireless client has associated with the access point
- If Forwarding is allowed
- The key type used by the client
- The Authentication type being used by the client
- Information about when the client associated and disassociated from the access point.

On an IronPoint 200 running software release 02.02.01 and later the output shows:

```

Foundry AP#show station

  MAC ADDRESS      RADIO  VAP CHANNEL VLAN  AUTH  ASSOC  FWD
=====
00-09-5B-69-FD-22   G      1      1      1    YES   YES   YES
=====

Current Station Count: 1

Stations on Radio A: 0
(ssid-prioritization disabled)
VAP[0]: 0.
VAP[1]: 0.
VAP[2]: 0.
VAP[3]: 0.

Stations on Radio B/G: 1
(ssid-prioritization disabled)
VAP[0]: 0.
VAP[1]: 1.
VAP[2]: 0.
VAP[3]: 0.
=====

```

- MAC address of the wireless client associated with the radio
- The radio to which the client is associated
- The VAP to which the client is associated
- The channel the client is using
- The VLAN membership of the client
- Whether or not the wireless client has been authenticated
- Whether or not the wireless client has associated with the access point
- If Forwarding is allowed
- The total number of clients (stations) associated with a radio, the number of clients (stations) associated to each radio VAP and SSID priority (if enabled) of each VAP.

If you do specify a radio, the output shows

:

```

Foundry AP#show station g
VAP:0
Station Table Information
=====
=====
VAP:1
Station Table Information
=====
if-wireless G VAP [1] :
802.11g Channel : 1
      802.11g Channel Station Table
Station Address : 00-09-5B-69-FD-22 VLAN ID: 1
Authenticated Associated Forwarding AuthType KeyType
TRUE TRUE TRUE WPA-PSK TKIP
Counters: pkts Tx/Rx bytes Tx/Rx
              70/3          9786/467
Time: Associated LastAssoc LastDisAssoc LastAuth
      3491         0         0         3529
=====
VAP:2
Station Table Information
=====
=====
VAP:3
Station Table Information
=====
=====
Current Station Count:

Stations on Radio B/G: 1
(ssid-prioritization disabled)
VAP[0]: 0.
VAP[1]: 1.
VAP[2]: 0.
VAP[3]: 0.
=====

```

show station

This command shows the wireless clients associated with the access point.

Syntax

show station [**a** | **g** | **all**] [*vap-id*]

- **a** - Clients associated to an 802.11a VAP interface.
- **g** - Clients associated to an 802.11g VAP interface.
- **all** - Clients associated to all VAP interfaces.
- *vap-id* - Specifies a VAP interface. (Options: 0, 1, 2, or 3)

Command Mode

Exec

Using the Web Management Interface

From the Status menu, click Stations. The Station Status page displays basic connection information for all associated stations. The page is divided by Radio a and Radio g. Note that this page is automatically refreshed every five seconds.

On the IronPoint 200 Access Point, the page shows the following:



Station Address: The MAC address of the wireless client.

Authenticated: Shows if the station has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to stations before attempting authentication.

Associated: Shows if the station has been successfully associated with the access point. Once authentication is completed, stations can associate with the current access point, or reassociate with a new access point. The association procedure allows the wireless system to track the location of each mobile client, and ensure that frames destined for each client are forwarded to the appropriate access point.

Forwarding Allowed: Shows if the station has passed 802.1x authentication and is now allowed to forward traffic to the access point.

Key Type: Displays one of the following:

- **None:** The client is not using data encryption keys.

- **Static WEP:** The client is using static WEP keys for encryption.
- **Dynamic WEP:** The client is using 802.1x authentication with dynamic WEP keys.
- **TKIP:** The client is using TKIP keys for unicast cipher.
- **AES:** The client is using AES keys for unicast cipher.
- **UNKNOWN type:** The key that the client is using cannot be recognized.

Auth Type: The client's authentication setting:

- **Open:** The client is not using WEP shared keys for authentication.
- **Shared:** The client is using WEP shared keys for authentication.
- **WPA-1X:** The client is using 802.1X for authentication.
- **WPA-PSK:** The client is using WPA pre-shared key for authentication.
- **UNKNOWN:** The authentication type that the client is using cannot be recognized.

VLAN ID: Displays the VLAN ID assigned to the client. Shows "Disabled" when VLAN support is disabled on the access point.

Displaying the AP Inventory Report

The AP Inventory report displays the status and configuration information of each VAP on an access point.

Using the CLI

Use the **show inventory** command to display an AP Inventory report.

show inventory

This command displays the status and configuration information for each VAP on an access point.

Syntax

show inventory

Default Setting

None.

Command Mode

Global Configuration

Command Usage

Use this command to display the following information on an access report:

- Name of the access point
- MAC address of the access point
- Information about each radio:
 - Current status of a radio channel (UP or DOWN) on the access point
 - Channel number
 - Power Level

Example

```
AP Inventory Report
=====
System Name       : Foundry AP
MAC Address      : 00-0C-DB-81-83-D4
=====
interface 802.11a information:
=====
802.11a: vap 0:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
802.11a: vap 1:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
802.11a: vap 2:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
802.11a: vap 3:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----

=====
interface 802.11g information:
=====
802.11g: vap 0:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
802.11g: vap 1:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
802.11g: vap 2:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
802.11g: vap 3:
-----
Status (up or down) : down
Channel              : 0 (AUTO)
Power Level          : FULL (5 dBm)
Antenna Control method : Full diversity
-----
```


Chapter 25

QoS Support

Quality of Service (QoS) allows you to specify which data packets have greater precedence when traffic is buffered in the access point due to congestion. Data packets received on an interface can be mapped to IEEE 802.1p priority levels based on the source or destination MAC address, or the Ethernet protocol type. At the transmit wireless interface, data packets with a high priority are transmitted before those of a lower priority.

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table.

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Note the following points about the access point's QoS support:

- When traffic classification is based on the source or destination MAC address, a table of MAC addresses mapped to 802.1p priority levels must be entered in the QOS Classifications section. Up to 10 MAC addresses can be specified.
- When traffic classification is based on the frame's priority tag, the MAC address and Ethernet type classification tables are not used. Up to 10 Ethernet protocol types can be specified.
- If traffic received on the Ethernet interface needs to be classified based on the tagged priority of frames, VLAN support must be enabled (see "Enabling VLAN Support" on page 23-2). If VLAN support is not enabled, the tags are stripped as frames are received on the Ethernet interface.
- Data packets received on the Ethernet interface are based directly on the 802.1p or VLAN tag. If no tag exists (such as when VLAN support is disabled), priority levels are mapped to the data based on the configured classification parameters or assigned the default priority level (zero).

- Data packets received on the wireless interfaces are mapped to an 802.1p priority level (or default zero) for optional tagging of the packet before transmitting on the Ethernet interface.

SVP Support – In addition, the access point provides support for SpectraLink Voice Priority (SVP), a QoS mechanism for prioritizing Voice over Internet Protocol (VoIP) traffic in wireless LANs. When SVP is enabled, the access point identifies SVP voice traffic and gives it a higher priority so that it can be transmitted from a wireless interface before other data traffic. This mechanism ensures a timely delivery of voice traffic and good audio quality for VoIP telephony.

When using SVP in the network, take note of the following requirements:

- When enabled, the access point identifies voice traffic by the SpectraLink Radio Protocol identifier in the IP header of the frame. The system requires support of SVP-enabled VoIP wireless phones and a SpectraLink NetLink SVP Server on the wired network.
- The number of SVP-enabled wireless phones that can be supported simultaneously by a single access point has a theoretical limit of seven. However, the practical limit is five, which still allows some bandwidth for other data traffic.
- SVP support on the access point operates independently from other QoS settings. There is no need to enable and configure any QoS parameters for SVP to function effectively.

Enabling QoS Support

Use the CLI or Web Management Interface to enable QoS support for the access point.

Using the CLI

To enable QoS support on the access point, first use the **qos mode** command from the CLI configuration mode to set the QoS classification method. If the classification method is source or destination MAC address, use the **qos mac-addr** command to build a table of MAC addresses mapped to 802.1p priority levels. If the classification method is Ethernet type, use the **qos ether-**

type command to build a table of Ethernet protocol types mapped to 802.1p priority levels. To view the current QoS settings, use the **show qos** command.

```

Foundry AP(config)#qos mode sa
Foundry AP(config)#qos mac-addr 00-80-e8-43-29-ab 6
Foundry AP(config)#qos mac-addr 00-80-e8-13-7a-15 6
Foundry AP(config)#qos mac-addr 00-80-e8-d6-62-c8 7
Foundry AP(config)#exit
Foundry AP#show qos
QoS information
=====
QoS Mode : Source Address
=====
QoS Address Entries
      Address                Priority
-----
      00-80-e8-43-29-ab      06
      00-80-e8-13-7a-15      06
      00-80-e8-d6-62-c8      07
Foundry AP(config)#svp
svp enable
Foundry AP(config)#exit
Foundry AP#show svp
SVP:      Enable
Foundry AP#

```

qos mode

This command sets the QoS traffic priority mode used by the access point. Use the **no** form to turn off QoS traffic priority.

Syntax

qos mode <sa | da | ether-type | 802.1p-tag>
no qos mode

- **sa** - Traffic classification is based on the source MAC address.
- **da** - Traffic classification is based on the destination MAC address.
- **ether-type** - Traffic classification is based on the Ethernet protocol type.
- **802.1p-tag** - Traffic classification is based on the frame's priority tag.

Default

Off

Command Mode

Global Configuration

Command Usage

- When traffic classification is based on the source or destination MAC address, the **qos mac-addr** command must be used to build a table of MAC addresses that are mapped to 802.1p priority levels.
- When traffic classification is based on the Ethernet protocol type, the **qos ether-type** command must be used to build a table of protocol types that are mapped to 802.1p priority levels.

- When traffic classification is based on the frame's priority tag, the MAC address and Ethernet type tables are not used.
- If traffic received on the Ethernet interface needs to be classified based on the tagged priority of frames, VLAN support must be enabled (see "vlan" on page 23-3). If VLAN support is not enabled, the tags are stripped as frames are received on the Ethernet interface.
- Data packets received on the Ethernet interface are based directly on the 802.1p or VLAN tag. If no tag exists (such as when VLAN support is disabled), priority levels are mapped to the data based on the configured classification parameters or assigned the default priority level (zero).
- Data packets received on the wireless interfaces are mapped to an 802.1p priority level for optional tagging of the packet before transmitting on the Ethernet interface.

qos mac-addr

This command builds a table of source and destination MAC addresses mapped to 802.1p priority levels. Use the **no** form to remove a MAC address entry from the table.

Syntax

```
qos mac-addr <mac-address> <priority>
no qos mac-addr <mac-address>
```

- *mac-address* - The MAC address of a source or destination. Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-d1-12-ab-89.
- *priority* - The 802.1p priority level assigned to the source or destination MAC address. (Range: 0 - 7, where 7 is the highest priority)

Default

No MAC addresses configured.

Command Mode

Global Configuration

Command Usage

- Up to 10 MAC address entries can be configured in the QoS MAC address table.
- Frames received with a MAC address not configured in the table are assigned to the default priority level (zero).

qos ether-type

This command builds a table of Ethernet protocol types mapped to 802.1p priority levels. Use the **no** form to remove an Ethernet type entry from the table.

Syntax

```
qos ether-type <type> <priority>
no qos ether-type <type>
```

- *type* - The Ethernet protocol type specified in hexadecimal format.

Range: 0000 - FFFF and the following:

```
0x0708
0x0800
0x0805
0x0806
0x0bad
0x1000
```


0x2000
0x6000
0x6001
0x6002
0x6004
0x8035
0x809b
0x80f3
0x8137
0x8138
0x872d
0x8729
0x888e
0x9000
0xf0f0

Note: You do not need to enter the “0x” character.

- *priority* - The 802.1p priority level assigned to the Ethernet protocol type. (Range: 0 - 7, where 7 is the highest priority)

Default

No Ethernet protocol types configured.

Command Mode

Global Configuration

Command Usage

- Up to 10 Ethernet type entries can be configured in the table.
- Frames received of an Ethernet type not configured in the table are assigned to the default priority level (zero).

show qos

This command shows the current QoS configuration.

Command Mode

Exec

svp

This command enables SpectraLink Voice Priority (SVP) support on the access point. Use the **no** form to disable SVP support.

Syntax

[no] svp

Default

Disabled

Command Mode

Global Configuration

Command Usage

- When enabled, the access point identifies voice traffic by the SpectraLink Radio Protocol identifier in the IP header of the frame. The system requires support of SVP-enabled VoIP wireless phones and a SpectraLink NetLink SVP Server on the wired network.
- The number of SVP-enabled wireless phones that can be supported simultaneously by a single access point has a theoretical limit of seven. However, the practical limit is five, which still allows some bandwidth for other data traffic.
- SVP support on the access point operates independently from other QoS settings. There is no need to enable and configure any QoS parameters for SVP to function effectively.

show svp

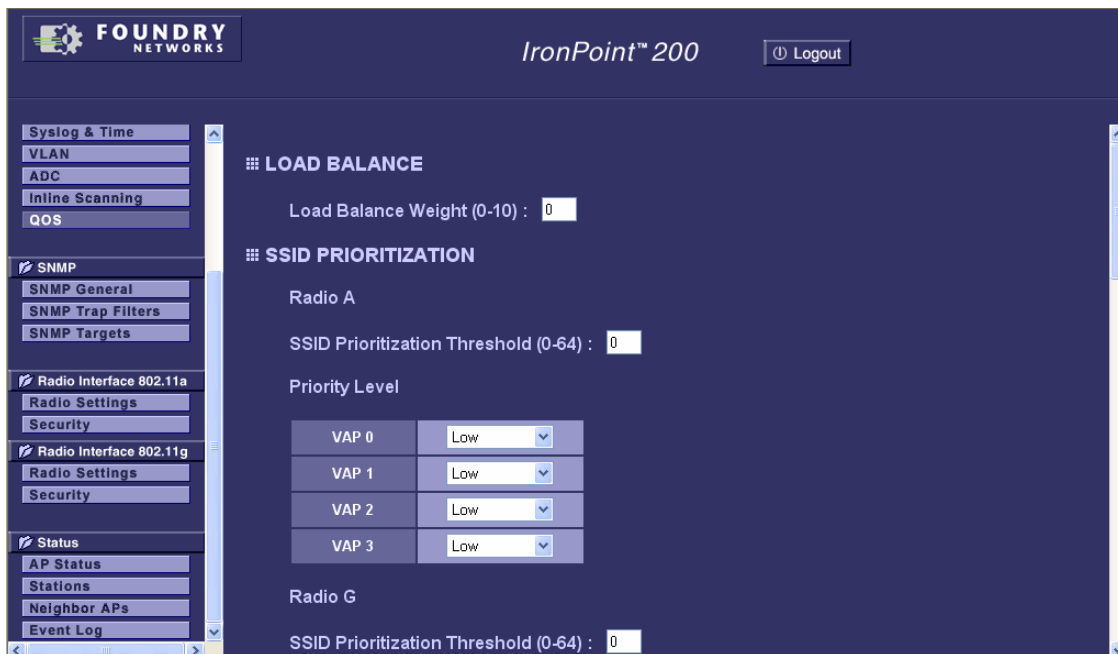
This command shows the current SVP setting.

Command Mode

Exec

Using the Web Management Interface

From the System menu, click QoS. To configure the access point to support QoS, select a QoS mode from the drop-down menu and, if appropriate, configure Ethernet types or MAC addresses in the classification tables. Click Apply.



Configurable Parameters

Load Balance - When enabled, Load Balancing associates wireless clients with the access point closest to their location. A client stays associated with an access point, even if that client moves to another location. When the client is disassociated from the network, the client will be associated with the closest access point the next time that client becomes authenticated. The closest access point is one from which the client receives the strongest signal.

To enable this feature, enter the weight of the signal that corresponds to the desired management RSSI, which is the received signal strength of the 802.11 management packets, as shown in the following table.

Weight	Management RSSI
1	28%
2	31%
3	34%
4	37%
5	41%
6	44%
7	47%
8	50%
9	53%
10	56%

Enter 0 to disable the feature. (Default: Disable)

SSID Prioritization - Grants levels of association for each VAP. Set an SSID Prioritization Threshold per radio on an access point, then assign priority levels to each VAP SSID.

- **SSID Prioritization Threshold (0-64):** Sets the maximum number of clients who can associate with a radio interface at any one time. Enter a value from 1 to 64 to enable SSID prioritization and to set the SSID Prioritization Threshold. Enter 0 to disable the feature. (Default: 0)

Note: If you change the SSID Prioritization Threshold, you must disable, then re-enable the VAP before the change will take effect. Enable or disable the VAP on the Security pages for each radio. See "Radio Interface Configuration" on page 21-1.

- **Priority Level:** Enter Guaranteed, High, Medium or Low for Priority Level. The High, Medium, and Low SSID priority levels restrict the number of clients who can associate with an access point radio to the value of the SSID Prioritization Threshold. The Guaranteed priority level allows clients to associate with an access point radio, beyond the SSID Prioritization Threshold, and up to the maximum number of clients that have been configured for the VAP. The Guaranteed priority is the highest priority, and takes precedence over the SSID Prioritization Threshold.

Note: If you change the Priority Level from Guaranteed to another setting, you must disable, then reenable the VAP before the change will take effect. Enable or disable the VAP on the Security pages for each radio. See "Radio Interface Configuration" on page 21-1.

QOS Mode – Sets the QoS traffic priority mode used by the access point or turns off QoS traffic priority. (Default: OFF)

- **OFF:** The access point does not prioritize traffic (except if SVP is enabled independently).

- **Source Address:** Traffic classification based on the source MAC address. If selected, be sure to enter MAC addresses in the QOS Classifications table.
- **Destination Address:** Traffic classification based on the destination MAC address. If selected, be sure to enter MAC addresses in the QOS Classifications table.
- **Ethernet Type:** Traffic classification based on the Ethernet protocol type. If selected, be sure to enter Ethernet types in the QOS Classifications table.
- **802.1p:** Traffic classification based on the frame's priority tag. Any data in the QOS Classifications tables is ignored.

SVP Status - Configures SpectraLink Voice Priority (SVP) support on the access point. (Default: Disable)

QOS Classifications – Configures tables for mapping MAC addresses and Ethernet protocol types to 802.1p priority levels.

- **Ethernet Type:** The Ethernet protocol type specified in hexadecimal format. (Range: 0000 - FFFF)
- **MAC Address:** The MAC address of a source or destination. Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-d1-12-ab-89.
- **Priority:** The 802.1p priority level assigned to the Ethernet protocol type or MAC address. (Range: 0 - 7, where 7 is the highest priority)

Chapter 26

SSID Prioritization

SSID Prioritization allows you to grant levels of association for each VAP. With SSID Prioritization, you set an SSID Prioritization Threshold per radio on an access point.

You then set a priority level for each SSID. There are four levels of SSID priority: Guaranteed, High, Medium and Low. Since there are four VAPs per access point radio, each VAP can be set to one of the four SSID priority level.

The High, Medium, and Low SSID priority levels restrict the number of clients who can associate with an access point radio to the value of the SSID Prioritization Threshold. The Guaranteed priority level allows clients to associate with an access point radio, beyond the SSID Prioritization Threshold, and up to the maximum number of clients that have been configured for the VAP. The Guaranteed priority is the highest priority, and takes precedence over the SSID Prioritization Threshold.

How SSID Prioritization Works

For example, a network administrator configures Radio A as follows:

- Maximum association limit for a VAP = 35
- SSID Prioritization Threshold = 20
- VAP 0 = SSID Priority of Guaranteed
- VAP 1 = SSID Priority of High
- VAP 2 = SSID Priority of Medium
- VAP 3 = SSID Priority of Low

This means the SSID Prioritization Threshold for Radio A will allow up to 20 clients to associate with all Radio A VAPs, but once the threshold is reached, every new association will be checked for priority and will be treated accordingly.

For example, if Client W wants to associate with Radio A, the access point checks to see if the SSID Prioritization Threshold has been reached for Radio A. If less than 20 clients are currently associated with Radio A, Client W will be allowed to associate with Radio A.

If there are already 20 clients associated with Radio A and Client X attempts to associate VAP 3 (SSID Priority set to Low), Client X will not be allowed to associate with Radio A. Client X must wait until one of the 20 clients disassociates from the Radio A.

Now, if Client Y attempts to associate with VAP 1 (SSID Priority set to High) then the access point checks to see if there is a client associated with a VAP that has a lower SSID priority. If there is, that client is dropped and the Client Y is allowed to associate with VAP 1. For example, if one client is associated with VAP 3 (SSID Priority set to Low) that client is dropped. However, if VAP 3 does not have any clients associated, then VAP 2 (SSID Priority set to Medium) is checked. If a client is associated with VAP 2, then that client is dropped so Client Y can associate with VAP 1. If no client is associated with VAP 2 or VAP 3, then Client Y is blocked.

If there are already 20 clients associated with Radio A, and if Client Z attempts to associate with VAP 0 (SSID Priority set to Guaranteed), then the access point allows Client Z to associate with the Radio A, even if the number of clients is over the Radio A SSID Prioritization Threshold. Then the access point checks the VAPs with the lower SSID Prioritization level to see if a client is associated. If a client is associated, that client is dropped.

Clients can keep associating with a VAP whose SSID prioritization is set to Guaranteed until maximum number of clients that can be associated with the VAP is reached.

Configuring SSID Prioritization for the IronPoint Access Point

Using the CLI

The following is an example of how to configure an IronPoint Access Point for SSID Prioritization for the example above:

1. Configure the SSID Prioritization Threshold for Radio A.

```
Foundry AP#configure
Foundry AP(config)#interface wireless a
Foundry AP(if-wireless a)#ssid-prioritization threshold 20
```

2. Assign an SSID to each VAP and set the SSID-Priority for each VAP on Radio A:

```
Foundry AP(if-wireless a)#vap 0
Foundry AP(if-wireless a: VAP[0])#ssid ironpoint-vap0
Foundry AP(if-wireless a: VAP[0])#max-association 35
Foundry AP(if-wireless a: VAP[0])#ssid-priority guaranteed
Foundry AP(if-wireless a: VAP[0])#
Foundry AP(if-wireless a: VAP[0])#exit
Foundry AP(if-wireless a)#vap 1
Foundry AP(if-wireless a: VAP[1])#ssid ironpoint-vap1
Foundry AP(if-wireless a: VAP[1])#max-association 35
Foundry AP(if-wireless a: VAP[1])#ssid-priority high
Foundry AP(if-wireless a: VAP[1])#exit
Foundry AP(if-wireless a)#vap 2
Foundry AP(if-wireless a: VAP[2])#ssid ironpoint-vap2
Foundry AP(if-wireless a: VAP[2])#max-association 35
Foundry AP(if-wireless a: VAP[2])#ssid-priority medium
Foundry AP(if-wireless a: VAP[2])#
Foundry AP(if-wireless a: VAP[2])#exit
Foundry AP(if-wireless a)#vap 3
Foundry AP(if-wireless a: VAP[3])#ssid ironpoint-vap3
Foundry AP(if-wireless a: VAP[3])#max-association 35
Foundry AP(if-wireless a: VAP[3])#ssid-priority low
Foundry AP(if-wireless a: VAP[3])#exit
Foundry AP(if-wireless a)#end
Foundry AP#
```

3. Finally, issue the **show interface** command for the VAP to make sure the configuration is correct.

```

Foundry AP#show interface wireless a 0
Wireless Interface A VAP 0 Information
=====
-----Identification-----
Description                : Foundry 802.11a Access Point
SSID                      : ironpoint-vap0
BSSID                    : 00-0C-DB-8A-F3-84
Turbo Mode                : OFF
Channel                   : 161
Status                    : Enabled
----- Auto Channel Selection & Transmit Power Control Parameters -----
Auto Refresh Interval      : 1440 min.
Auto Transmit Power Control : Disabled
-----802.11 Parameters-----
Transmit Power             : MIN (0 dBm)
Max Station Data Rate      : 54Mbps
Multicast Data Rate        : 6Mbps
Fragmentation Threshold    : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval            : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval : 30 Mins
DTIM Interval              : 1 beacon
Maximum Association         : 35 stations
VLAN ID                    : 170
Load Balance                : Disabled
SSID Prioritization Threshold : 20
Priority Level              : Guaranteed
-----Security-----
Closed System              : Disabled
WPA clients                : Disabled
WPA Key Mgmt Mode          : PRE SHARED KEY
WPA PSK Key Type           : PASSPHRASE
PMKSA Lifetime             : 720 minutes
Encryption                 : Disabled
WEP Key Length             : None
Default Transmit Key       : 1
WEP Key Type               : Key 1: HEX      Key 2: HEX
                           : Key 3: HEX      Key 4: HEX
Common Static Keys         : Key 1: ***** Key 2: *****
                           : Key 3: ***** Key 4: *****
Authentication Type         : OPEN
-----Antenna-----
Antenna Control method     : Full diversity
Antenna ID                 : Integrated
Antenna Location           : Indoor
-----Authentication Parameters-----
802.1x                     : Disabled
Broadcast Key Refresh Rate : 120 min
802.1x Session Timeout Value : 0 min
Pre-Authentication         : Disabled
=====
Foundry AP#

```


ssid-prioritization threshold

Sets the SSID Prioritization Threshold for an access point radio.

Syntax

ssid-prioritization threshold *<value>*

value - Enter 0 - 64 can be used for value, where 0 disables SSID prioritization for all the VAPs on a radio.

Default Setting

0 clients

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

Enter a value from 1 to 64 to enable SSID prioritization and to set the SSID Prioritization Threshold.

Set the value of this command to 0 to disable SSID prioritization. If SSID prioritization is disabled, the **show interface wireless** *<radio>* *<VAP#>* command displays "SSID Prioritization Threshold" as 0.

ssid-priority

Sets the priority for an SSID.

Syntax

ssid-priority *<priority-value>*

priority-value - guaranteed, high, medium, or low

Default Setting

low

Command Mode

Interface Configuration (Wireless-VAP)

Command Usage

Enter **guaranteed** for priority if your clients are to be associated with an SSID even if the SSID Prioritization Threshold has been reached or exceeded.

Using the Web Management Interface

To configure SSID Prioritization using the Web Management Interface, see "QoS Support" on page 25-1, "Using the Web Management Interface" on page 25-6.

Chapter 27

Miscellaneous Reports

This chapter presents the various reports you can display on the access point. You can display the following reports:

- “AP Status”
- Stations. See “Displaying the Access Point Status” on page 24-1.
- “Neighbor APs” on page 27-3
- Event Log. See “Displaying Log Messages” on page 12-5.

AP Status

You can display basic system configuration settings and settings for the wireless interface by displaying the AP Status page in the Web Management Interface.

Click AP Status button under the Status menu to display the page.

The screenshot displays the Foundry Networks IronPoint 200 Web Management Interface. The left sidebar contains a navigation menu with categories like Syslog & Time, VLAN, ADC, Inline Scanning, QOS, SNMP, Radio Interface 802.11a, Radio Interface 802.11g, and Status. The Status category is expanded, showing options for AP Status, Stations, Neighbor APs, and Event Log. The main content area is titled "AP Status" and "AP System Configuration". It contains a table with the following data:

System Up Time	3 days, 17 hours, 46 minutes, 22 seconds
MAC Address	00-0C-DB-81-38-F9
System Name	vishal
Country	UNITED STATES
System Contact	Contact
Speed Duplex Actual	100Base-TX Full Duplex
Speed Duplex Configured	Auto Select
IP Address	10.55.1.58
IP Default Gateway	10.55.1.254
HTTP Server	ENABLED
HTTP Server Port	80
HTTP Secure Server	ENABLED

Displayed Parameters

AP System Configuration – The AP System Configuration table displays the basic system configuration settings:

- **System Up Time:** Length of time the management agent has been up.
- **MAC Address:** The physical layer address for this device.
- **System Name:** Name assigned to this system.
- **Country:** The access point's Country Code setting.
- **System Contact:** Administrator responsible for the system.
- **IP Address:** IP address of the management interface for this device.
- **IP Default Gateway:** IP address of the gateway router between this device and management stations that exist on other network segments.
- **HTTP Server:** Shows if management access via HTTP is enabled.
- **HTTP Server Port:** Shows the TCP port used by the HTTP interface.
- **HTTP Secure Server:** Shows if management access via a secure HTTPS/SSL connection is enabled.
- **HTTP Secure Server Port:** Shows the UDP port number used for HTTPS/SSL interface.
- **Version:** Shows the version number for the runtime code.

AP Wireless Configuration – The AP Wireless Configuration table displays the wireless VAP interface settings listed below.

- **SSID:** The service set identifier for the VAP interface.
- **BSSID:** The basic service set identifier (access point wireless MAC address) for the VAP interface.
- **Radio Channel:** The radio channel through which the access point communicates with wireless clients.
- **Radio Encryption:** The key size used for data encryption.
- **Radio Authentication Type:** Shows if open system or shared key authentication is used.
- **802.1x:** Shows if IEEE 802.1x access control for wireless clients is enabled.

Neighbor APs

You can display a list of access points that have been detected on the network by clicking the Neighbor AP button under the Status menu.



The screenshot shows the Foundry Networks IronPoint 200 web interface. On the left is a navigation menu with categories like 'System & Time', 'VLAN', 'ADC', 'Inline Scanning', 'QoS', 'SNMP', 'Radio Interface 802.11a', 'Radio Interface 802.11g', 'Status', and 'Event Log'. The 'Status' category is expanded, showing 'AP Status', 'Stations', 'Neighbor APs', and 'Event Log'. The 'Neighbor APs' report is displayed in a table with the following data:

BSSID	Channel	RSSI	Last Seen
00:02:6F:3E:0E:C6	1	4	405321
00:0C:DB:34:79:F0	9	8	4138
00:0C:DB:8A:84:20	1	19	471442
00:0C:DB:8A:F3:B0	5	7	165626
00:0C:DB:8B:11:F0	6	3	375198
00:0C:DB:8B:30:88	1	42	471359
00:0C:DB:8B:36:88	1	8	471355
00:0C:DB:8B:36:89	1	9	471355
00:0C:DB:8B:A3:A8	1	12	471359
00:0C:DB:8B:E8:E8	1	8	93108
00:0C:DB:8B:E8:E9	1	12	93102
00:0C:DB:8C:67:08	1	3	456569

The report shows the broadcast SSIDs of the neighboring access points, the channels they are using, the strength of the signal of the channel in dBm and the last time the access point was detected by the RF sensor.

Chapter 28

RF Monitoring

Radio Frequency (RF) Monitoring uses a sensor to scan the airwaves for 802.11 packets. An IronPoint Access Point can be converted to a sensor to collect data on the 802.11 packets. Reports that use the data collected by the sensor provide information about the wireless environment.

Also, when an access point is converted to a sensor, the following occurs:

- The sensor's radios are automatically enabled.
- Only the following CLI commands are available on the sensor:
 - Commands to set the sensor's IP address, subnet mask, and default gateway
 - Commands to configure SNMP values
 - Commands to configure SNMP servers
 - Copy command

Converting an Access Point to a Sensor

You can convert an IronPoint access point to function as an RF Monitoring sensor by loading the sensor image. This procedure is performed only from the CLI and requires you to connect to the access point to a management console via the serial port.

- Notes:**
1. Any IronPoint Access Point can be converted to an RF Monitoring sensor. When converting the access point to a sensor, its current configuration may not be saved. It is strongly recommended that you upgrade the access point to the proper software release before you convert it to a sensor.
 2. If several sets of user name and password are configured on the access point, only the first set of user name and password will be available when the access point is converted to an RF sensor; however the complete list of user names and passwords are retained. When you convert the RF sensor back to an access point, all the user names and access points will be available in the access point.

Do the following to load the sensor image:

3. At the access point's CLI Exec level, enter the following command:

```
Foundry AP# copy tftp file  
or
```

```
Foundry AP# copy ftp file
```

4. Next, at the "Select the type of download <1, 2, 3> " prompt, enter 1 for Application Image, 2 for a configuration file, or 3 for a boot image. For example:

```
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:3
```

5. At the CLI prompt, enter the name of the source file. For example:

```
Foundry AP# IPSR020203.bin
```

6. Enter the IP address of the TFTP server. For example:

```
Foundry AP# 192.168.1.19
```

The download begins. Wait until you see the following prompt:

```
Current firmware version is 02.02.02Tv8. Copying new firmware version Run-Time
code v02.02.03. Please wait ...
Firmware copy complete. Reboot access point to complete firmware upgrade.
```

7. Manually reboot the access point by entering the **reset board** command.

```
Foundry AP#reset board
```

8. When it starts up, login and configure an IP address, subnet mask, and default gateway for the access point.
9. Enter SNMP community (for SNMP v1 or v2c) or user (for SNMP v3) settings.
10. Connect the sensor to the network.

Viewing Sensor Data

Use IronView Network Manager to view data collected by the sensor. IronView Network Manager contains several RF Monitoring reports. Refer to the release notes for the RF sensor to determine which version of IronView Network Manager can be used to collect data for a particular version of the sensor. Also, refer to the *Foundry IronView Network Manager User Guide* for details on the collected RF sensor data.

Converting a Sensor Back to an Access Point

If you want to convert a sensor back to an access point, refer to the release notes for Foundry IronPoint Access Point software version you want to use. Software versions for access point and RF sensor installed on the access point must match to allow for the seamless conversion of the access point to an RF sensor then back to an access point.

Appendix A

Troubleshooting

Check the following items before you contact Technical Support.

1. If wireless clients cannot access the network, check the following:

- Be sure the access point and the wireless clients are configured with the same Service Set ID (SSID).
- If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate pre-shared key, authentication or encryption keys. The wireless client's NIC must have the necessary drivers to support the security and authentication methods configured on the access point.
- If authentication is being performed through a RADIUS server, ensure that the clients are properly configured on the RADIUS server.
- If authentication is being performed through IEEE 802.1x, be sure the wireless users have installed and properly configured 802.1x client software.
- If MAC address filtering is enabled, be sure the client's address is included in the local filtering database or on the RADIUS server database.
- If the wireless clients are roaming between access points, make sure that all the access points and wireless devices in the Extended Service Set (ESS) are configured to the same SSID, and authentication method.

2. If the access point cannot be configured using the Telnet, a Web browser, or SNMP software:

- Be sure to have configured the access point with a valid IP address, subnet mask and default gateway.
- If VLANs are enabled on the access point, the management station should be configured to send tagged frames with a VLAN ID that matches the access point's management VLAN (default VLAN 1, see "management-vlanid" on page 23-2). However, to manage the access point from a wireless client, the access point Management Filter should be disabled (see "filter ap-manage" on page 18-3).
- Check that you have a valid network connection to the access point and that the Ethernet port or the wireless interface that you are using has not been disabled.
- If you are connecting to the access point through the wired Ethernet interface, check the network cabling between the management station and the access point. If you are connecting to access point from a wireless client, ensure that you have a valid connection to the access point.

- If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted (i.e, four sessions). Try connecting again at a later time.
3. If you cannot access the on-board configuration program via a serial port connection:
 - Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.
 - Check that the serial cable conforms to the pin-out connections provided in Appendix D.
 4. If you forgot or lost the password, set the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name “admin” with the password “admin” to access the management interface.
 5. If all other recovery measure fail, and the access point is still not functioning properly, take any of these steps:
 - Reset the access point’s hardware using the console interface, Web interface, or through a power reset.
 - Reset the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name “admin” with the password “admin” to access the management interface.

When you do contact Technical Support, you might be asked to issue a **show crashdump** command. Output for this command is available if the access point has previously crashed. note

show crashdump

Show information about the access point

Syntax

show crashdump

Default Setting

None

Command Mode

Exec

Command Usage

Issue this command only when Technical Support requests it.

Example

The following is only example of the **show crashdump** output.

```
Foundry AP#show crashdump
* Crash Dump: SIG 54524150, LEN 0000121C, ver F0492222 *
Crash time and date:    08:50:34  Sep 20, 2006
The system has been up for 0 days, 6 hours, 44 minutes, 31 seconds
System image: Version 02.01.05Tw8,
                  Compiled on Sep 13 2006 at 14:11:40

EXCEPTION VECTOR : 00000700
Exception type (cause of crash): Program
GPRs:
R0- R3: 00000000 01BFEF30 00000000 00080000
R4- R7: 012F9890 00000000 00000000 00000000
R8-R11: 00960000 00960000 00002928 00930000
R12-R15: 00000000 00000000 00000000 00000000
R16-R19: 00000000 00000000 00000000 00000000
R20-R23: 00000000 00000000 00000000 00000000
R24-R27: 00000000 00000000 00000000 00000001
R28-R31: 00000000 009D7030 012F9870 0000B032

Special purpose registers (SPRs):
SRR0 00000000 SRR1 0008B032 DEC 0003E26C XER 00000000
LR 006241F8 CTR 00000000 SDISR F7BCFF45
DAR 00000000 SDR1 01C0001F
SPRG0 0063A558 SPRG1 00000000 SPRG2 00000000 SPRG3 0000B032
CR 20000040 EAR 00000000

BAT registers (DBATS and IBATs):
IBAT0U 000003FF IBAT0L 00000002
IBAT1U FFF0001F IBAT1L FFF00022
IBAT2U FF00007F IBAT2L FF000022
IBAT3U FFF0001F IBAT3L FFF00022
DBAT0U 00000003 DBAT0L 0000001A
DBAT1U 000003FF DBAT1L 00000002
DBAT2U 80001FFF DBAT2L 8000002A
DBAT3U F0001FFF DBAT3L F000002A

Call Trace: (names wrong if running and crashed builds differ):
SRR0--> 00000000 ACCESS_DESCRIPTION_free + FFE11DF4
LR --> 006241F8 taskDestroy + 00000780
006241B4 taskDestroy + 0000073C
005FEDA8 excTask + 000000B4
0062B0B8 vxTaskEntry + 00000060
00000000 ACCESS_DESCRIPTION_free + FFE11DF4

Stack region 01BFEE30 length 00001000 bytes, is saved at 01FF421C.
Frame pointer was at 01BFEF30:
This print-out is only a portion.
```

```

01BFEE30:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEE40:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEE50:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEE60:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEE70:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEE80:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEE90:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEEA0:  EEEEEEEE EEEEEEEE EEEEEEEE EEEEEEEE
01BFEEB0:  EEEEEEEE EEEEEEEE 01BFEEED8 EEEEEEEE
01BFEEC0:  00960000 FFFFFFFF 10000003 01BFEEFE8
01BFEEED0:  01BFF204 00000000 01BFEEF0 0061FF70
01BFEEEE0:  01BFEEF0 00929860 00929854 00929860
01BFEEF0:  01BFEEF08 006212B0 01BFEEF30 0063A558
01BFEEF00:  00929854 012F4830 01BFEEF20 00606A20
01BFEEF10:  00000000 009D7030 01BFEEF20 0092C828
01BFEEF20:  01BFEEF30 006271A0 012F9870 0000B032
01BFEEF30:  01BFEEF50 006241B4 EEEEEEEE 00960000
01BFEEF40:  008A0000 00930000 00960000 00000000
01BFEEF50:  01BFEEF90 005FEDA8 00623A78 012F9870
01BFEEF60:  00000001 00000000 00000000 00000000
01BFEEF70:  00960000 EEEEEEEE EEEEEEEE 00000000
01BFEEF80:  00000000 00000000 00000000 005FECF4
01BFEEF90:  01BFEEFA8 0062B0B8 00000000 00000000
01BFEEFA0:  EEEEEEEE 00000000 00000000 00000000
.
.
.

```

Appendix B

Syslog Messages

General System

Message Level	Message	Explanation
Informational	Country ISO Name updated to <i><new-country></i>	The access point system Country Code has been changed to the specified new country.
Informational	Disable DayLight Saving: <i><from-start-date-to-end-date></i>	Daylight saving has been disabled.
Informational	Enable DayLight Saving: <i><from-start-date-to-end-date></i>	Daylight saving has been enabled.
Informational	Get time from SNTP Server Fail	An SNTP server could not be reached for a system time update.
Informational	Get time from SNTP Server Successfully	System time has been successfully updated via SNTP.
Informational	Regulatory Domain updated to <i><new-value></i>	The access point system Regulatory Domain (a group of countries with the same regulatory requirements) has changed to the specified value.
Informational	upap authentication failure for <i><user-id></i>	The user that logged in with the user ID displayed in the message failed to be authenticated. The displayed user ID is an administrator user ID.
Notice	System Down	System has shutdown.
Notice	System Up	System has started.
Notice	Working Radius Server has changed from <i><non-working server></i> to <i><working server></i>	System has changed to using the secondary RADIUS server when the primary was unreachable. Or, has changed back to the primary server when it has recovered.

Message Level	Message	Explanation
Warning	AP is receiving more than <num> broadcast frames per second. Potential network overload condition exists.	There are excessive multicast packets from the Ethernet side
Warning	AP is receiving more than <number-of-frames> <frame-type> wireless frames/sec. Potential RF overload condition exists	<p>The access point is receiving more broadcast or multicast frames than what is allowed for the wireless rate limiting type configured on the access point. An overload condition may occur.</p> <p><number-of-frames> can be:</p> <ul style="list-style-type: none"> • 10 - Aggressive • 25 = Normal • 50 Conservative <p><frame-type> can be broadcast or multicast</p>
Warning	Countermeasure is in progress, shutting down AP for 60 secs	The WPA Countermeasure has been triggered. The access point will not respond to wireless activity for 60 seconds and all clients will be disassociated.

802.1x

Message Level	Message	Explanation
Warning	802.1x Supplicant authentication failed on Radio <a b/g> VAP <vap-id>.	The access point has failed 802.1x supplicant authentication.
Notice	Updating session key for <MAC-address>	The encryption key for the client session is being updated.
Notice	Updating broadcast key for 802.1x clients VAP <vap-id>	The encryption key for broadcast data is being updated for all 802.1x clients associated to the specified VAP interface.
Notice	Successful 802.1x authentication for station <MAC-address-of-station> VAP <vap-id>	The wireless client with the specified MAC address has been successfully authenticated using 802.1x.
Notice	Failed 802.1x authentication for station <MAC-address-of-station> VAP <vap-id>	The wireless client with the specified MAC address has failed 802.1x authentication.
Informational	802.1x Supplicant has been authenticated on Radio <a b/g> VAP <vap-id>.	The access point has been successfully authenticated as an 802.1x supplicant.

MAC Authentication

Message Level	Message	Explanation
Notice	Successful Radius MAC Address Authentication for station <MAC-address-of-station> on Radio <a b/g> VAP <vap-id>	The wireless client with the specified MAC address has been successfully authenticated by the RADIUS server MAC address database.
Notice	Failed Radius MAC Address Authentication for station <MAC-address-of-station> on Radio <a b/g> VAP <vap-id>	The wireless client with the specified MAC address has failed authentication with the RADIUS server MAC address database.
Notice	Successful Local MAC Address Authentication for station <MAC-address-of-station> on Radio <a b/g> VAP <vap-id>	The wireless client with the specified MAC address has been successfully authenticated by the local MAC address database.
Notice	Failed Local MAC Address Authentication for station <MAC-address-of-station> on Radio <a b/g> VAP <vap-id>	The wireless client with the specified MAC address has failed authentication with the local MAC address database.

Radio Interface

Message Level	Message	Explanation
Alert	11b or 11a/11g Wireless Interface Failed	The 802.11a, 802.11b, or 802.11g radio interface has failed.
Notice	Auto Channel Scan selected <particular-value> MHz, channel <channel-number>	The specified radio interface has automatically selected a channel number at the specified band.
Informational	SSID updated to <new-ssid>	An SSID has been changed to the specified value.
Informational	Open System updated to <open close>	A VAP interface has enabled (close) or disabled (open) the Hidden SSID feature.
Informational	Requested Channel updated to <new-channel>	A radio interface has changed to the new specified channel.
Informational	Description updated to <new-description>	A VAP interface has changed to the new specified description.
Informational	11a Radio Interface Enabled VAP <vap-id>	The 802.11a radio interface has been enabled.
Informational	11g Radio Interface Enabled VAP <vap-id>	The 802.11g radio interface has been enabled.
Informational	11a Radio Interface Disabled VAP <vap-id>	The 802.11a radio interface has been disabled.

Message Level	Message	Explanation
Informational	11g Radio Interface Disabled VAP <vap-id>	The 802.11g radio interface has been disabled.
Informational	Association stale time updated to <new-time>	The association timeout interval has been changed to the specified value.
Informational	Short Retry Limit updated to <new-value>	The 802.11 short retry limit has been changed to the specified value.
Informational	Long Retry Limit updated to <new-value>	The 802.11 long retry limit has been changed to the specified value.
Informational	Max association clients updated to <new-value>	The maximum number of clients that can be associated with a VAP interface has been changed to the specified value.
Informational	Maximum Station Data Rate updated to 5.5 Mbps	The maximum unicast data rate for the 802.11g radio interface has changed to 5.5 Mbps.
Informational	Maximum Station Data Rate updated to <new-rate>	The maximum unicast data rate for the specified radio interface has changed to the specified rate.
Informational	RTS Length updated to <new-value>	The RTS threshold length for the specified radio interface has been changed to the specified value.
Informational	Transmit Power set to <FULL HALF QUARTER EIGHTH MINIMUM>	The transmit power for the specified radio interface has been changed to the specified value.
Informational	Fragmentation Threshold updated to <new-value>	The fragmentation threshold length for the specified radio interface has been changed to the specified value.
Informational	Beacon Interval updated to <new-value>	The beacon interval for the specified radio interface has been changed to the specified value.
Informational	Radio channel updated to <new-value>	The radio channel for the specified radio interface has been changed to the specified channel.
Informational	Turbo Mode Enabled	Turbo mode has been enabled on the 802.11a radio interface.
Informational	Turbo Mode Disabled	Turbo mode has been disabled on the 802.11a radio interface.
Informational	Outdoor Channel Enabled	The antenna location for the specified radio interface has been set to "Outdoor." Only channels specified for outdoor use are available.

Message Level	Message	Explanation
Informational	Outdoor Channel Disabled	The antenna location for the specified radio interface has been set to "Indoor." All channels permitted by the regulatory domain are available.
Informational	Preamble mode set to LONG	The preamble for the 802.11b/g radio has been set to "Long."
Informational	Preamble mode set to SHORT	The preamble for the 802.11b/g radio has been set to "Short."
Informational	DTIM period updated to <i><new-value></i>	The DTIM period for the specified radio interface has been changed to the specified value.
Informational	Radio channel updated to AUTO	The radio channel for the specified radio interface has been changed to auto.
Informational	Antenna ID updated to <i><new-value></i>	An external antenna ID for the specified radio interface has been changed to the new value.
Informational	Antenna Ctrl updated to <i><AUTO A B></i>	The specified radio interface has been set to use an external antenna on the right-side (A), both sides (B), or to automatically select antennas to use.
Informational	wlan <i><device-number></i> beacon transmission problem at <i><beacon-count></i>	The access point was not able to send a beacon frame on the specified radio interface for the indicated beacon count number.

Radio Security

Message Level	Message	Explanation
Notice	Updating group key for all WPA clients	The encryption key for broadcast data is being updated for all WPA clients associated to the specified VAP interface.
Informational	802.11<Radio ID>: Default Transmit Key updated to Key Index <i><new-value></i>	The WEP transmit key index has been changed to the new index value for the specified VAP interface.
Informational	802.11<Radio ID>: Authentication Mode set to SHARED KEY	The authentication mode for the specified VAP interface has been set to "Shared Key."
Informational	802.11<Radio ID>: Authentication Mode set to OPEN	The authentication mode for the specified VAP interface has been set to "Open."

Message Level	Message	Explanation
Informational	Authentication stale time updated to <i><new-time></i>	The authentication timeout interval has been changed to the specified value.
Informational	WEP Key Type updated to <i><HEX ASCII></i>	The WEP key type has been changed to the new value.
Informational	WEP Encryption Mode set to <i><64-bit-encryption 128-bit-encryption 152-bit-encryption></i>	The WEP key length has been changed to the new value.
Informational	WPA 4-way handshaking successes at <i><MAC-address> VAP <vap-id></i>	The wireless client with the specified MAC address has successfully authenticated using a WPA pre-shared key.
Informational	WPA 4-way handshaking fails at <i><MAC-address> VAP <vap-id></i>	The wireless client with the specified MAC address has failed authentication using a WPA pre-shared key.
Informational	WPA group key update successes at <i><MAC-address> VAP <vap-id></i>	The wireless client with the specified MAC address has successfully updated the WPA broadcast key.
Informational	WPA group key update fails at <i><MAC-address> VAP <vap-id></i>	The wireless client with the specified MAC address has failed to update the WPA broadcast key.
Informational	Data Encryption is set to Enabled. WPA2 Clients mode is set to Disabled. WPA Clients Mode is set to Supported/Required. WPA Multicast Cipher is set to WEP/TKIP. WPA Unicast Cipher can accept TKIP or AES-CCMP/TKIP only. WPA Authentication is set to 802.1X Supported/Required.	The WPA configuration on the specified VAP radio interface has been changed to the specified state.
Informational	Data Encryption is set to Enabled. WPA Clients Mode is set to Disabled. WPA2 Clients Mode is set to Supported/Required. WPA2 Multicast Cipher is set to TKIP/AES-CCMP. WPA2 Unicast Ciphers can accept TKIP or AES-CCMP/AES-CCMP only. WPA2 Authentication is set to 802.1X Supported/Required.	The WPA2 configuration on the specified VAP radio interface has been changed to the specified state.

Message Level	Message	Explanation
Informational	Data Encryption is set to Enabled. WPA Clients Mode is set to Supported/Required. WPA2 Clients Mode is set to Supported/Required. WPA/WPA2 Multicast Cipher is set to WEP/TKIP. WPA/WPA2 Unicast Ciphers can accept TKIP or AES-CCMP. WPA/WPA2 Authentication is set to 802.1X Supported/Required.	The WPA-WPA2 -mixed configuration on the specified VAP radio interface has been changed to the specified state.
Informational	Data Encryption is set to Enabled. WPA2 Clients Mode is set to Disabled. WPA Clients Mode is set to Supported/Required. WPA Multicast Cipher is set to WEP/TKIP. WPA Unicast Cipher can accept TKIP or AES-CCMP/TKIP only. WPA Authentication is set to Pre-Shared Key.	The WPA preshared-key type for the specified VAP radio interface has been updated to the specified type (HEX or alphanumeric) and state.
Informational	Data Encryption is set to Enabled. WPA Clients Mode is set to Disabled. WPA2 Clients Mode is set to Supported/Required. WPA2 Multicast Cipher is set to TKIP/AES-CCMP. WPA2 Unicast Ciphers can accept TKIP or AES-CCMP/AES-CCMP only. WPA2 Authentication is set to Pre-Shared Key.	The WPA2 preshared-key type for the specified VAP radio interface has been updated to the specified type (HEX or alphanumeric) and state.
Informational	Data Encryption is set to Enabled. WPA Clients Mode is set to Supported/Required. WPA2 Clients Mode is set to Supported/Required. WPA/WPA2 Multicast Cipher is set to WEP/TKIP. WPA/WPA2 Unicast Ciphers can accept TKIP or AES-CCMP. WPA/WPA2 Authentication is set to Pre-Shared Key.	The WPA-WPA2 -mixed preshared-key supported/required type for the specified VAP radio interface has been updated to the specified type (HEX or alphanumeric) and state.
Informational	<radio>: Updating key <new-value> used for WEP encryption	The key used for WEP encryption on the 802.11a, 802.11b, or 802.11g interface has been updated to the value displayed in the message.
Informational	<radio>: Updating wpa-clients as <required supported>	The configuration for WPA clients on the 802.11a, 802.11b, or 802.11g interface has been changed to "required" or "supported".
Informational	<radio>: Updating wpa-mode as <dynamic pre-shared-key>	The WPA mode for the specified radio interface has been changed to "dynamic" or "pre-shared key".

Message Level	Message	Explanation
Informational	<radio>: Updating multicast-cipher as <AES TKIP WEP>	The multicast cipher mode for the specified radio interface has been changed to "AES", "TKIP" or "WEP".
Informational	<radio>: Updating wpa-preshared key	The pre-shared key for the specified radio interface has been updated.
Informational	<radio>: Updating wpa-psk-type as alphanumeric hex	The WPA pre-shared key type for the specified radio interface has been changed to alphanumeric or hexadecimal.

Wireless Client

Message Level	Message	Explanation
Warning	Station Failed to <associate reassociate> (invalid mode/state): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point could not associate the client with the specified MAC address due to being in an initialization or scanning state.
Warning	Station Failed to <associate reas-address> (station not authenticated) for Radio <a b/g> VAP <vap-id>	The access point could not associate the client with the specified MAC address due to incomplete authentication.
Warning	Station Failed to <associate reassociate> (internal error): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point failed to associate the client with the specified MAC address due to insufficient memory allocation.
Warning	Station Failed to authenticate (out of sequence frame): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point failed to authenticate a WEP client with the specified MAC address due to a received frame that was not numbered in the correct 802.11 sequence.
Warning	Station Failed to authenticate (unsupported algorithm) for Radio <a b/g> VAP <vap-id>	The access point failed to authenticate the client with the specified MAC address due to a mismatch in WEP shared key settings between the access point and the client.
Warning	Station Failed to authenticate (invalid frame length): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point failed to authenticate the client with the specified MAC address due to a non-standard WEP authentication frame length.
Warning	Station Failed to authenticate (WEP is required on the AP): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point failed to authenticate a WEP client with the specified MAC address due to WEP shared-key authentication being enabled on the client but not on the access point.

Message Level	Message	Explanation
Warning	Station Failed to authenticate (WEP not allowed): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point failed to authenticate a WEP client with the specified MAC address due to WEP shared-key authentication being enabled on the access point but not on the client.
Warning	Station Failed to authenticate (challenge text mismatch): <MAC-address> for Radio <a b/g> VAP <vap-id>	The access point failed to authenticate the client with the specified MAC address due to an incorrect WEP shared key or a corrupted authentication frame.
Notice	Station <MAC-address> has roamed to this access point from access point <IP-of-old-access-point>	The client with the specified MAC address has successfully roamed to this access point from another access point.
Notice	Station roamed to another access point: <MAC-address>	The client with the specified MAC address has successfully roamed from this access point to another access point.
Notice	IAPP Context data for Station <MAC-address> has been sent to access point <IP-of-new-access-point>	IAPP data for the specified client has been sent to the access point to which it is roaming.
Notice	Station Associated: <MAC-address> VAP <vap-id>	The client with the specified MAC address has successfully associated to this access point.
Notice	Station Reassociated: <MAC-address> VAP <vap-id>	The client with the specified MAC address has successfully reassociated to this access point.
Notice	Station Authenticated: <MAC-address> VAP <vap-id>	The client with the specified MAC address has been successfully authenticated.
Notice	Station Forwarding <MAC-address> Encryption key type= <NONE STATIC WEP DYNAMIC WEP WPA-WEP WPA-TKIP WPA-AES>	The client with the specified MAC address is successfully forwarding data to the access point using the specified encryption key.
Notice	Station Roamed to Another Access Point: <MAC-address>	The client with the specified MAC address has roamed from this access point to another access point.
Notice	STA <MAC-address> is deleted: retries exceeded for Radio <a b/g> VAP <vap-id>	The client with the specified MAC address has been removed from the association table due to failed communication after 5 retry attempts.
Notice	STA <MAC-address> is deleted: Inactivity	The client with the specified MAC address has been removed from the association table due to inactivity longer than the idle time interval.

Access Point Management

Message Level	Message	Explanation
Notice	Username and Password : failed	The access point management user name and password were invalid.
Notice	Username and Password : OK	The access point management user name and password were accepted.
Informational	SSH task - terminated SSH session.	A current SSH client session has been terminated.
Informational	SSH task - created SSH session	A new SSH client session has been created.
Informational	SSH task - created SSH session failed	An SSH session failed after three attempts to connect to the SSH server socket.
Informational	SSH task: Enable SSH server	The access point SSH server has been enabled.
Informational	SSH task: Disable SSH server.	The access point SSH server has been disabled.
Informational	SSH task: Set SSH server port to <i><new-port value></i>	The SSH server port has been changed to the specified new port.
Informational	SSH task: Failed to set SSH server port to <i><new-port value></i>	An attempt was made to set the SSH server port to the same value as the default Telnet server port.
Informational	Enable Telnet	The access point Telnet server has been enabled.
Informational	Disable Telnet	The access point Telnet server has been disabled.

SNMP

Message Level	Message	Explanation
Informational	Unauthorized SNMP PDU receipt	An unauthorized SNMP PDU has been received. This message is generated if SNMP v3 is configured on the access point.
Informational	Fail in attempting to read MIB variable because of using an unconfigured SNMP community string	SNMP processes was not able to read the MIB variable because the administrator did not use the correct community string. This message is generated if SNMP v3 is configured on the access point.

Informational	SNMP v3 support: Enable Disable SNMP service and traps	SNMP management access has been enabled or disabled. If it is enabled, SNMP traps can be sent. This message is generated if SNMP v3 is configured on the access point.
---------------	--	---

Syslog

Message Level	Message	Explanation
Error	Syslog : Configuration file version changed	Syslog settings were found in a configuration file of a previous version. The settings have been reset to default values.
Informational	Syslog : TCP connection fail, Drop message <message>	The TCP connection with the syslog server failed and the specified message was not sent.
Informational	Syslog : Can't connect to syslog server <IP-address>	The access point cannot connect to the specified syslog server.

DHCP

Message Level	Message	Explanation
Informational	DHCP Client : Send Discover	The access point has sent a DHCP discover message.
Informational	DHCP Client : Receive Offer from <address>	The access point has received a configuration offer from the specified DHCP server.
Informational	DHCP Client : Send Request, Request IP = <IP-address>	The access point has sent a request to the DHCP server to use the offered IP address.
Informational	DHCP Client : Receive Nak	The access point has received a reject message from the DHCP server in response to a client request.
Informational	DHCP Client : Receive Ack from <address>, Lease time = <duration>	The access point has received an accept message from the specified DHCP server to use the offered IP address for a specified duration.

Message Level	Message	Explanation
Informational	DHCP Client : Send Decline	The access point has sent a decline message in response to an offer from the DHCP server.
Informational	DHCP Client : Send Release	The access point has sent a release message to the DHCP server for the current IP configuration.

Appendix C

Country Channel Allocations

Note: Check with your local Regulatory and Safety agencies to determine if the channels presented in this appendix are approved for your location.

Channel Numbers

Available 802.11a (5 GHz) channel numbers and center frequencies.

5.150 - 5.250 GHz (UNII-low band)	5.250 - 5.350 GHz (UNII-middle band)	5.470 - 5.725 GHz (ETSI)	5.725 - 5.850 GHz (UNII-high band)
36 – 5.180 GHz 40 – 5.200 GHz 44 – 5.220 GHz 48 – 5.240 GHz Japan/Argentina 34 – 5.170 GHz 38 – 5.190 GHz 42 – 5.210 GHz 46 – 5.230 GHz			149 – 5.745 GHz 153 – 5.765 GHz 157 – 5.785 GHz 161 – 5.805 GHz 165 – 5.825 GHz 169 – 5.845 GHz

Available 802.11a (5 GHz) turbo mode channel numbers and center frequencies.

5.150 - 5.250 GHz (UNII-low band)	5.250 - 5.350 GHz (UNII-middle band)	5.470 - 5.725 GHz (ETSI)	5.725 - 5.850 GHz (UNII-high band)
42 – 5.210 GHz			152 – 5.760 GHz 160 – 5.800 GHz

Available 802.11b/g (2.4 GHz) channel numbers and center frequencies.

2.400 - 2.4835 GHz (2.497 GHz in Japan)	
1 – 2.412 GHz	8 – 2.447 GHz
2 – 2.417 GHz	9 – 2.452 GHz
3 – 2.422 GHz	10 – 2.457 GHz
4 – 2.427 GHz	11 – 2.462 GHz
5 – 2.432 GHz	12 – 2.467 GHz
6 – 2.437 GHz	13 – 2.472 GHz
7 – 2.442 GHz	14 – 2.484 GHz (Japan 802.11b only)

Channel Settings by Country

The countries listed in the following table do not allow user configuration of the Country Code. The Country Code is preset for access points shipped to these countries and it is prohibited to change the setting.

Country (Code)	802.11a (5 GHz)		802.11g (2.4 GHz)		802.11b (2.4 GHz)	
	Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
Canada (CA)	36-48 149-165 Turbo Mode 42 152-160	149-165 Turbo Mode 152-160	1-11	1-11	1-11	1-11
United States (US)	36-48 149-165 Turbo Mode 42 152-160	149-165 Turbo Mode 152-160	1-11	1-11	1-11	1-11
Japan (JP)	34-46	None	1-13	1-13	1-14	1-14
Taiwan (TW)	149-161 Turbo Mode 152	149-161 Turbo Mode 152	1-11	1-11	1-11	1-11
New Zealand (NZ)	36-48 149-169	149-169	1-13	1-13	1-13	1-13

The countries listed in the following table allow user configuration of the Country Code. For access points shipped to these countries, the Country Code is set to the default setting of "99." The country code must be set to the country in which the access point is to be used.

Note: Outdoor channels in the table marked with an asterisk (*) indicate that either local regulations do not explicitly specify the channels for use or that local regulations are unknown.

Country (Code)	802.11a (5 GHz)		802.11g (2.4 GHz)		802.11b (2.4 GHz)	
	Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
Albania (AL)	None	None	1-13	1-13*	1-13	1-13*
Algeria (DZ)	None	None	1-13	1-13*	1-13	1-13*
Argentina (AR)	34-46	None	None	None	1-13	1-13
Armenia (AM)	36-48	36-48*	1-13	1-13*	1-13	1-13*
Australia (AU)	36-48 149-161 Turbo Mode 42 152-160	149-161 Turbo Mode 152-160	1-13	1-13	1-13	1-13
Austria (AT)	36-48	None	1-13	1-13	1-13	1-13
Azerbaijan (AZ)	36-48	36-48*	1-13	1-13*	1-13	1-13*
Bahrain (BH)	36-48 149-161	None	1-13	None	1-13	None
Belarus (BY)	None	None	1-13	1-13*	1-13	1-13*
Belgium (BE)	36-48	None	1-13	13	1-13	13
Belize (BZ)	149-165	149-165*	1-13	1-13*	1-13	1-13*
Bolivia (BO)	149-165	149-165*	1-13	1-13*	1-13	1-13*
Brazil (BR)	149-165	149-165	None	None	1-13	1-13
Brunei Darussalam (BN)	149-165	149-165*	1-13	1-13*	1-13	1-13*
Bulgaria (BG)	36-48	None	1-13	1-13	1-13	1-13
Chile (CL)	149-165 Turbo Mode 152-160	None	1-13	None	1-13	1-13
China (CN)	149-165	149-165	1-13	1-13	1-13	1-13
Colombia (CO)	36-48 149-161	149-161	1-11	1-11	1-11	1-11
Costa Rica (CR)	None	None	1-13	1-13*	1-13	1-13*
Croatia (HR)	36-48	None	1-13	1-13	1-13	1-13
Cyprus (CY)	36-48	None	1-13	1-13	1-13	1-13
Czech Republic (CZ)	36-48	None	1-13	1-13	1-13	1-13
Denmark (DK)	36-48	None	1-13	1-13	1-13	1-13

Country (Code)	802.11a (5 GHz)		802.11g (2.4 GHz)		802.11b (2.4 GHz)	
	Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
Dominican Republic (DO)	36-48 149-165 Turbo Mode 42 152-160	36-48* 149-165* Turbo Mode 42 152-160	1-11	1-11*	1-11	1-11*
Ecuador (EC)	149-165	149-165	None	None	1-13	1-13
Egypt (EG)	None	None	1-13	1-13	1-13	1-13
Estonia (EE)	36-48	None	1-13	1-13	1-13	1-13
Finland (FI)	36-48	None	1-13	1-13	1-13	1-13
France (FR)	36-48	None	1-13	1-7	1-13	1-7
Georgia (GE)	36-48	36-48*	1-11	1-11*	1-11	1-11*
Germany (DE)	36-48	None	1-13	1-13	1-13	1-13
Greece (GR)	None	None	1-13	None	1-13	None
Guatemala (GT)	36-48 149-165 Turbo Mode 42 152-160	36-48* 149-165* Turbo Mode 42 152-160	1-11	1-11*	1-11	1-11*
Hong Kong (HK)	36-48 149-165 Turbo Mode 42 152-160	149-165 Turbo Mode 152-160	1-11	1-11	1-11	1-11
Hungary (HU)	36-48	None	1-13	1-13	1-13	1-13
Iceland (IS)	36-48	None	1-13	1-13	1-13	1-13
India (IN)	149-161	149-161	1-13	None	1-13	None
Indonesia (ID)	None	None	1-13	1-13*	1-13	1-13*
Iran (IR)	149-165	149-165*	1-13	1-13*	1-13	1-13*
Ireland (IE)	36-48	None	1-13	1-13	1-13	1-13
Israel (IL)	None	None	5-7	5-7	5-7	5-7
Italy (IT)	36-48	None	1-13	None	1-13	None
Jordan (JO)	36-48 149-161	None	1-13	None	1-13	None
Kazakhstan (KZ)	None	None	1-13	1-13*	1-13	1-13*

Country (Code)	802.11a (5 GHz)		802.11g (2.4 GHz)		802.11b (2.4 GHz)	
	Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
(North) Korea (KP)	149-161	149-161*	1-13	1-13*	1-13	1-13*
Korea Republic (KR)	149-161	149-161	1-13	1-13	1-13	1-13
Kuwait (KW)	None	None	1-13	1-13	1-13	1-13
Latvia (LV)	None	None	1-13	1-13*	1-13	1-13*
Lebanon (LB)	None	None	1-13	1-13	1-13	1-13
Liechtenstein (LI)	36-48	None	1-13	1-13	1-13	1-13
Lithuania (LT)	36-48	None	1-13	1-13	1-13	1-13
Luxembourg (LU)	36-48	None	1-13	1-13	1-13	1-13
Macau (MO)	36-48 149-165	36-48* 149-165*	1-13	1-13*	1-13	1-13*
Macedonia (MK)	None	None	1-13	1-13*	1-13	1-13*
Malaysia (MY)	149-169	149-169	1-13	1-13	1-13	1-13
Malta (MT)	36-48	None	1-13	1-13	1-13	1-13
Mexico (MX)	36-48 149-165 Turbo Mode 42 152	149-165 Turbo Mode 152	1-11	None	1-11	None
Monaco (MC)	36-48	36-48*	1-13	1-13*	1-13	1-13*
Morocco (MA)	None	None	1-13	1-13	1-13	1-13
Netherlands (NL)	36-48	None	1-13	1-13	1-13	1-13
Norway (NO)	36-48	None	1-13	1-13	1-13	1-13
Oman (OM)	None	None	1-13	1-13*	1-13	1-13*
Pakistan (PK)	None	None	1-13	1-13*	1-13	1-13*
Panama (PA)	36-48 149-165 Turbo Mode 42 152-160	36-48* 149-165* Turbo Mode 42 152-160	1-11	1-11*	1-11	1-11*
Peru (PE)	149-165	149-165	1-13	1-13	1-13	1-13
Philippines (PH)	149-169 Turbo Mode 152-160	149-169 Turbo Mode 152-160	1-13	1-13	1-13	1-13

Country (Code)	802.11a (5 GHz)		802.11g (2.4 GHz)		802.11b (2.4 GHz)	
	Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
Poland (PL)	36-48	None	1-13	1-13	1-13	1-13
Portugal (PT)	36-48	None	1-13	1-13	1-13	1-13
Puerto Rico (PR)	36-48 149-165 Turbo Mode 42 152-160	36-48* 149-165* Turbo Mode 42 152-160	1-11	1-11*	1-11	1-11*
Qatar (QA)	None	None	1-13	1-13*	1-13	1-13*
Romania (RO)	None	None	1-13	1-13	1-13	1-13
Russia (RU)	None	None	1-13	1-13	1-13	1-13
Saudi Arabia (SA)	None	None	1-13	1-13	1-13	1-13
Singapore (SG)	36-48 149-165	36-48 149-165	1-13	1-13	1-13	1-13
Slovak Republic (SK)	36-48	None	1-13	1-13	1-13	1-13
Slovenia (SI)	36-48	None	1-13	1-13	1-13	1-13
South Africa (ZA)	36-48	None	1-13	1-13	1-13	1-13
Spain (ES)	36-48	None	1-13	None	1-13	None
Sweden (SE)	36-48	None	1-13	1-13	1-13	1-13
Switzerland (CH)	36-48	None	1-13	1-13	1-13	1-13
Syria (SY)	None	None	1-13	1-13*	1-13	1-13*
Thailand (TH)	149-169	149-169	1-13	None	1-13	None
Turkey (TR)	36-48	None	1-13	1-13	1-13	1-13
Ukraine (UA)	None	None	1-13	1-13*	1-13	1-13*
United Arab Emirates (AE)	None	None	1-13	1-13	1-13	1-13
United Kingdom (GB)	36-48	None	1-13	1-13	1-13	1-13
Uruguay (UY)	149-165	149-165	1-13	1-13	1-13	1-13
Uzbekistan (UZ)	36-48 149-165 Turbo Mode 42 152-160	36-48 149-165 Turbo Mode 42 152-160	1-11	1-11	1-11	1-11

Country (Code)	802.11a (5 GHz)		802.11g (2.4 GHz)		802.11b (2.4 GHz)	
	Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
Venezuela (VE)	149-165	149-165	1-13	1-13	1-13	1-13
Vietnam (VN)	None	None	1-13	1-13*	1-13	1-13*

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key

Broadcast keys are sent to stations using 802.1x dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and eaves dropping.

Extensible Authentication Protocol (EAP)

An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1x port authentication and a RADIUS authentication server to provide “mutual authentication” between a client, the access point, and the a RADIUS server

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

IEEE 802.11a

A wireless standard that supports high-speed communications in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard supports data rates of 6, 12, 24, and 54 Mbps.

IEEE 802.11b

A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g

A wireless standard that supports wireless communications in the 2.4 GHz band using supports high-speed communications in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

Inter Access Point Protocol (IAPP)

A protocol that specifies the wireless signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM/ allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

RADIUS

A logon authentication protocol that uses software running on a central server to control access to the network.

Roaming

A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the infrastructure network.

RTS Threshold

Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Temporal Key Integrity Protocol (TKIP)

A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

Wi-Fi Protected Access

WPA employs 802.1x as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA Pre-shared Key (PSK)

PSK can be used for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access.

Numerics

802.11a 6-4
802.11g 6-4
802.1X
 intrusion detection 17-3

A

AAA *See* TACACS+
ACL 9-10
ADC 2-1
AES 22-5
authentication 19-1, 22-8
 configuring 19-1, 22-8
 MAC address 19-3, 19-6
 type 22-1
Authentication, Authorization, and Accounting *See*
 TACACS+

B

banners 9-15
beacon
 interval 21-6, 21-21
 rate 21-8, 21-21
block station 17-5
blocking a MAC address 17-4
BOOTP 8-2, 8-3

C

channel 21-6, 21-20
clear all MAC entries 19-4
Clear To Send *See* CTS
CLI 4-1
 command modes 4-4
command line interface *See* CLI
community name, configuring 10-3

community string 10-3, 10-7
configuration, IP address setup without ADC 2-2
console port
 required settings 2-2
country code
 configuring 6-2
CTS 21-11, 21-22

D

default settings 2-6
device status, displaying 24-1
DHCP 8-1, 8-2, 8-3, 8-4
DNS 8-3, 8-4
Domain Name Server *See* DNS
DTIM 21-8, 21-21

E

EAP 22-4
encryption 22-1, 22-4, 22-9
event logs 12-4
Extensible Authentication Protocol *See* EAP

F

factory defaults
 restoring 6-7
filter 18-1, 19-3
 address 19-1, 19-3
 between wireless clients 18-3, 18-6
 local bridge 18-3, 18-6
 local or remote 19-1, 19-4
 management access 18-3, 18-6
 protocol types 18-3, 18-7
 VLANs 21-20, 23-4, 23-5
firmware
 displaying version 24-2
fragmentation 21-8

G

gateway address 2-3, 4-2, 8-2, 8-4

H

hardware version, displaying 24-2, 24-3
hidden SSID 21-7, 21-20
HTTP, secure server 9-8
HTTPS 9-8

I

IAPP 18-1, 18-6
IEEE 802.11a 21-1
 configuring interface 6-4, 21-1
 maximum data rate 21-9, 21-11, 21-21
 radio channel 21-6, 21-20
IEEE 802.11b 21-1
IEEE 802.11f 18-1, 18-6
IEEE 802.11g 21-1
 configuring interface 6-4, 21-23
 maximum data rate 21-9, 21-11, 21-29
 radio channel 21-6, 21-28
IEEE 802.1x 5-6, 5-7, 22-4
 configuring 19-1, 19-7, 22-21
intrusion detection 17-1
IP address
 BOOTP/DHCP 8-2, 8-3
 configuring 2-3, 8-1, 8-2, 8-3
IP address setup without ADC 2-2

L

load balancing 21-31
log
 messages 12-1, 12-3
 server 12-1, 12-3
log-in
 Web interface 3-1
login
 CLI 4-1
logon authentication
 RADIUS client 5-6, 19-6

M

MAC address, authentication 19-3, 19-6
main menu 3-3
maximum data rate 21-9, 21-11, 21-21, 21-29
 802.11a interface 21-9, 21-11, 21-21
 802.11g interface 21-9, 21-11, 21-29
message of the day 9-15
messages, syslog B-1, C-1
multicast cipher 22-22

O

open system 22-1

P

password
 configuring 9-1
 management 9-1
pre-shared key
 intrusion detection 17-4
problems, troubleshooting A-1
PSK 22-5

R

radio channel
 802.11a interface 21-6, 21-20
 802.11g interface 21-6, 21-28
RADIUS 15-1, 22-4
RADIUS, logon authentication 5-6, 19-6
rate limit
 Ethernet 20-2
 wireless 6-12
Remote Authentication Dial-in User Service *See* **RADIUS**
Request to Send *See* **RTS**
reset 6-7
resetting the access point 6-7
restarting the system 6-7
RJ-45 port
 configuring duplex mode 20-3
 configuring speed 20-3
RTS
 threshold 21-11, 21-22

S

Secure Socket Layer *See* **SSL**
security, options 22-1
session key 19-7, 22-21
shared key 22-9, 22-12
Simple Network Time Protocol *See* **SNTP**
SNMP 10-1
 community name 10-3
 community string 10-3
 enabling traps 10-2, 10-7
 trap destination 10-4, 10-7
 trap manager 10-4, 10-7
SNTP 13-1, 13-3, 13-6
 enabling client 13-1, 13-3
 server 13-3, 13-6
software
 displaying version 24-1, 24-2
SSID 21-2, 21-6, 21-7, 21-12, 21-14, 21-20, 21-26, 21-28, 22-1, 24-5
ssid 5-10
SSID prioritization 5-13, 26-1

- SSID, hidden 21-7, 21-20
- SSL 9-8
- startup files, setting 7-3
- static MAC authentication
 - intrusion detection 17-4
- station status 24-5, 24-8
- status
 - displaying device status 24-1
 - displaying station status 24-5, 24-8
- syslog messages B-1, C-1
- system clock, setting 13-1, 13-2
- system log
 - enabling 12-1, 12-2
 - server 12-1, 12-3

T

- TACACS+ 16-1
- Telnet
 - for managenet access 4-1
- Temporal Key Integrity Protocol *See* TKIP
- time zone 13-4, 13-6
- TKIP 22-4
- transmit power, configuring 21-12, 21-21
- trap destination 10-4, 10-7
- trap manager 10-4, 10-7
- troubleshooting A-1

U

- user name, manager 9-2, 9-4
- user password 9-4
- user passwords 9-2

V

- VLAN
 - configuration 21-20, 23-3, 23-4, 23-5
 - management ID 23-2
 - native ID 21-20, 23-4, 23-5

W

- Web interface
 - access requirements 3-1
 - configuration buttons 3-3
 - home page 3-2
 - menu list 3-3
- WEP 22-4, 22-9
 - configuring 22-4, 22-9, 22-12, 22-16, 22-20
 - shared key 22-9, 22-12
- Wi-Fi Protected Access *See* WPA
- Wired Equivalent Protection *See* WEP
- WPA 22-4
 - pre-shared key 22-16
- WPA, pre-shared key *See* PSK

