HP ProCurve Wireless Access Point 520wl

User Guide - For Software Version 2.4.5

© Copyright 2004, Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number

5990-6056

March 2004

Applicable Products

HP ProCurve Wireless AP 520wl (HP J8133A)

Trademark Credits

Microsoft®, Word®, WordPad®, and Internet Explorer® are US registered trademarks of Microsoft Corporation.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can b obtained from your HP Sales and Service Office or authorized dealer.

Safety Considerations

Prior to the installation and use of this product, review a safety markings and instructions.

Notes and Cautions

NOTE:

A Note indicates important information that help you make better use of your computer.

CAUTION:

A Caution indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

Contents

Regulatory Information

Safety Information viii
Grounding viii
Servicing viii
Accessories viii
Informations concernant la sécurité ix
Hinweise zur Sicherheit x
Considerazioni sulla sicurezza xi
Consideraciones sobre seguridad xii
Safety Information (Japan) xiii
Safety Information (China) xiv
EMC Regulatory Statements xv
Notice for U.S.A. xv
Notice for Canada xv
Notice for European Union xvi
Notice for Japan xvii
Notice for Korea xvii

1 Introducing the 520wl

Wireless Networking Concepts 1-1
Management and Monitoring Capabilities 1-2
HTTP/HTTPS Interface 1-2
Command Line Interface 1-2
SNMP Management 1-2
SNMPv3 Secure Management 1-3
802.11b/g compared to 802.11a Networks 1-4
Feature List 1-4
Cell Size and Coverage Area 1-7
Installation and Initialization 1-8

2 Getting Started

Prerequisites 2-1
Product Package 2-2
AP Cards 2-2
System Requirements 2-2
Hardware Installation 2-3

Initialization 2-6
ScanTool 2-6
Logging into the HTTP Interface 2-8
Setup Wizard 2-9
Download the Latest Software 2-13
Setup your TFTP Server 2-13
Download Updates from your TFTP Server using the Web Interface 2-13
Download Updates from your TFTP Server using the CLI Interface 2-13
Additional Hardware Features 2-14
Installing the AP in a Plenum 2-14
LED Indicators 2-14

3 Status Information

System Status 3-1

4 Advanced Configuration

Configuring the AP Using the HTTP/HTTPS Interface 4-1
System 4-3
Dynamic DNS Support 4-3
Network 4-4
IP Configuration 4-4
DHCP Server 4-5
Link Integrity 4-6
Interfaces 4-7
Operational Mode 4-8
Wireless (802.11a) 4-9
Wireless (802.11b) 4-10
Wireless (802.11b/g) 4-14
Wireless Distribution System (WDS) 4-15
Ethernet 4-16
Management 4-17
Passwords 4-17
IP Access Table 4-17
Services 4-18
Filtering 4-24
Ethernet Protocol 4-24
Static MAC 4-24
Advanced 4-27
TCP/UDP Port 4-27
Alarms 4-28
Groups 4-28
Alarm Host Table 4-31
Syslog 4-31

Bridge 4-32
Spanning Tree 4-32
Storm Threshold 4-33
Intra BSS 4-33
Packet Forwarding 4-33
Security 4-34
Authentication and Encryption Modes 4-34
MAC Access 4-39
Rogue Access Point Detection (RAD) 4-41
RADIUS 4-43
MAC Access Control by way of RADIUS Authentication 4-43
RADIUS Authentication with 802.1x 4-44
RADIUS Accounting 4-46
VLAN/SSID 4-47
VLAN Overview 4-47
VLAN Workgroups and Traffic Management 4-49
Typical User VLAN Configurations 4-49
Typical VLAN Management Configurations 4-50

5 Monitor Information

Accessing Monitor Features 5-1
Version 5-2
ICMP 5-3
IP/ARP Table 5-3
Learn Table 5-4
IAPP 5-4
RADIUS 5-5
Interfaces 5-6
Link Test 5-7
Station Statistics 5-9
Enabling and Viewing Station Statistics 5-9
Refreshing Station Statistics 5-9

6 Commands

Logging into the HTTP Interface 6-1
Introduction to File Transfer via TFTP or HTTP 6-3
TFTP File Transfer Guidelines 6-3
HTTP File Transfer Guidelines 6-3
Image Error Checking during File Transfer 6-3
Update AP via TFTP 6-4
Update AP via HTTP 6-5
Retrieve File via TFTP 6-7
Retrieve File via HTTP 6-8
Reboot 6-10
Reset 6-11
Help Link 6-12

7 Troubleshooting

Troubleshooting Concepts 7-1
Symptoms and Solutions 7-2
Connectivity Issues 7-2
Basic Software Setup and Configuration Problems 7-2
Client Connection Problems 7-4
VLAN Operation Issues 7-4
Active Ethernet (AE) 7-5
Recovery Procedures 7-5
Reset to Factory Default Procedure 7-6
Forced Reload Procedure 7-6
Setting IP Address using Serial Port 7-9
Related Applications 7-11
RADIUS Authentication Server 7-11
TFTP Server 7-11

A Specifications

Software Features A-1
Management Functions A-1
Advanced Bridging Functions A-1
Medium Access Control (MAC) Functions A-2
Security Functions A-2
Network Functions A-2
Advanced Wireless Functions A-3

Hardware Specifications A-3
Physical Specifications A-3
Ethernet Interface A-4
Serial Port Interface A-4
Active Ethernet Interface A-4
HTTP Interface A-4
Radio Specifications A-4
802.11a Channel Frequencies A-4
802.11b Channel Frequencies A-6
802.11g Channel Frequencies A-7
Wireless Communication Range A-7

B ASCII Character Chart

C Command Line Interface (CLI)

General Notes C-1
Prerequisite Skills and Knowledge C-1
Notation Conventions C-1
Important Terminology C-1
Navigation and Special Keys C-2
CLI Error Messages C-2
Command Line Interface (CLI) Variations C-2
Bootloader CLI C-3
CLI Command Types C-4
Operational CLI Commands C-4
Parameter Control Commands C-8
Using Tables & User Strings C-11
Working with Tables C-11
Using Strings C-12
Configuring the AP using CLI commands C-12
Log into the AP using HyperTerminal C-12
Log into the AP using Telnet C-12
Set Basic Configuration Parameters using CLI Commands C-13
Other Network Settings C-17
CLI Monitoring Parameters C-24
Parameter Tables C-24
System Parameters C-26
Network Parameters C-27
Interface Parameters C-30
Management Parameters C-33
Filtering Parameters C-36
Alarms Parameters C-38
Bridge Parameters C-39

Security Parameters C-41
RADIUS Parameters C-42
Rogue Access Point Detection (RAD) Parameters C-44
VLAN/SSID Parameters C-44
Other Parameters C-45

Regulatory Information

Safety Information

Documentation reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product.

WARNING A WARNING in the manual denotes a hazard that can cause injury or death.

CAUTION A CAUTION in the manual denotes a hazard that can damage the equipment.

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazardous conditions and have taken appropriate steps.

Grounding

This product is a safety class I compliant product and has a protective earthing terminal. There must be an uninterruptible safety earth ground from the main power source to the product's power cord or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

Servicing

There are no user-serviceable parts inside this product. Any servicing, adjustment, maintenance or repair must be performed only by service trained personnel.

This product does not have a power switch; it is powered on when the power cord is plugged in.

Accessories

The following accessories are available for this product:

- Wireless 802.11b Access Point Card 150wl
- Wireless 802.11a Access Point Card 160wl
- Wireless 802.11g Access Point Card 170wl
- Wireless Range Extender Antenna 100wl

Regulatory information for these products can be found in the installation instructions included with them.

Informations concernant la sécurité

Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées.

WARNING Dans la documentation, un WARNING indique un danger susceptible d'entraîner des dommages corporels ou la mort.

CAUTION Un texte de mise en garde intitulé CAUTION indique un danger susceptible de causer des dommages à l'équipement.

Ne continuez pas au-delà d'une rubrique WARNING ou CAUTION avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées.

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Cet appareil ne comporte pas de commutateur principal ; la mise sous tension est effectuée par branchement du cordon d'alimentation.

Hinweise zur Sicherheit

Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

WARNING Eine WARNING in der Dokumentation symbolisiert eine Gefahr, die Verletzungen oder sogar Todesfälle verursachen kann.

CAUTION CAUTION in der Dokumentation symbolisiert eine Gefahr, die dis Gerät beschädigen kann.

Fahren Sie nach dem Hinweis WARNING oder CAUTION erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, daß der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfaßt, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, daß die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

Dieses Gerät hat keinen Netzschalter; es wird beim Anschließen des Netzkabels eingeschaltet.

Considerazioni sulla sicurezza

Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso.

WARNING La dicitura WARNINGdenota un pericolo che può causare lesioni o morte.

CAUTION La dicituraCAUTION denota un pericolo che può danneggiare le attrezzature.

Non procedere oltre un avviso di WARNING o di CAUTIONprima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Questo apparato non possiede un commutatore principale; si mette scotto tensione all'inserirsi il cavo d'alimentazione.

Consideraciones sobre seguridad

Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto.

WARNING Una WARNING en la documentación señala un riesgo que podría resultar en lesiones o la muerte.

CAUTION Una CAUTION en la documentación señala un riesgo que podría resultar en averías al equipo.

No proseguir después de un símbolo de WARNING o CAUTION hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación o el juego de cable de alimentación suministrado. Si existe la probabilidad de que la protección a tierra haya sufrido desperfectos, desenchufar el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Este producto no tiene interruptor de potencia; se activa cuando se enchufa el cable de alimentación.

Safety Information (Japan)

安全性の考慮

安全記号

マニュアル参照記号。製品にこの記号がついている場合はマニュアルを参照し、注意事項等をご確認ください。

WARNING　マニュアル中の「WARNING」は人身事故の原因となる危険を示します。

CAUTION　マニュアル中の「CAUTION」は装置破損の原因となる危険を示します。

「WARNING」や「CAUTION」の項は飛ばさないで必ずお読みください。危険性に関する記載事項をよく読み、正しい手順に従った上で次の事項に進んでください。

これは安全性クラスIの製品で保護用接地端子を備えています。主電源から製品の入力配線端子、電源コード、または添付の電源コード・セットまでの間、切れ目のない安全接地が存在することが必要です。もしこの保護回路が損なわれたことが推測されるときは、接地が修復されるまで電源コードを外しておいてください。

LAN ケーブルの接地に関して:

- もし貴社の LAN が複数の配電システムにより電力を受けている領域をカバーしている場合には、それらのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LAN ケーブルは時として危険な過度電圧（例えば雷や、配電設備の電力網での障害）にさらされることがあります。露出した金属部分の取扱いには十分な注意をはらってください。

本製品の内部にはユーザーが修理できる部品はありません。サービス、調整、保守および修理はサービス訓練を受けた専門家におまかせください。

本製品には電源スイッチがありません。電源コードを接続したとき電源入となります。

HP网络产品使用安全手册

使用须知

欢迎使用惠普网络产品，为了您及仪器的安全，请您务必注意如下事项:

1. 仪器要和地线相接，要使用有正确接地插头的电源线，使用中国国家规定 的220V 电源。
2. 避免高温和尘土多的地方，否则易引起仪器内部部件的损坏。
3. 避免接近高温，避免接近直接热源，如直射太阳光、暖气等其它发热体。
4. 不要有异物或液体落入机内，以免部件短路。
5. 不要将磁体放置于仪器附近。

警告

为防止火灾或触电事故，请不要将该机放置于淋雨或潮湿处。

安装

安装辅助管理模块，请参看安装指南。

保修及技术支持

如果您按照以上步骤操作时遇到了困难，或想了解其它产品性能，请按以下 方式与我们联络。

如是硬件故障:

1. 与售出单位或当地维修机构联系。
2. 中国惠普有限公司维修中心地址:
   北京市海淀区知春路49号希格玛大厦
   联系电话: 010-62623888 转 6101
   邮政编码: 100080

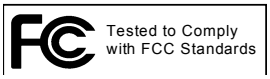
如是软件问题:

1. 惠普用户响应中心热线电话: 010-65645959
2. 传真自动回复系统: 010-65645735

EMC Regulatory Statements

Notice for U.S.A.

Manufacturer's FCC Declaration of Conformity Statement



Product No: J8133A

Manufacturer: Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185 USA

Phone:650-857-1501

For questions regarding this declaration, contact the Product Regulations Manager at the above address or phone number.

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

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

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

The FCC requires the user to be notified that any changes or modifications made to the device that are not expressly approved by the Hewlett-Packard Company may void the user's authority to operate the equipment.

Notice for Canada

This device complies with the limits for a Class B digital device and conforms to Industry Canada standard ICES-003. Cet appareil numérique de la classe B est conforme à la norme ICES-003 de Industry Canada.

Notice for European Union

DECLARATION OF CONFORMITY
according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747-5502
U.S.A.

declares, that the product

Product Name: HP Procurve Wireless Enterprise Access Point 520wl

Product Number(s): J8133A

Regulatory Model: WA1010

Product Options: J8134A, J8136A, J8149A, J8430A

conforms to the following Product Specifications:

Safety: IEC 60950:1991 + A1, A2, A3, A4 / EN 60950:1992 + A1, A2, A3, A4

EMC: EN 55022:1998 / CISPR 22:1997 Class B[1]
EN 55024:1998 / CISPR 24:1997
EN 61000-3-2:1995 +A1, A2 / IEC 61000-3-2:1995 +A2
EN 61000-3-3:1995 Class B / IEC 61000-3-3:1994

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The Product was tested in a typical configuration with 150wl 802.11b Access Point Cards.

Roseville, March 15, 2004

Mike Avery, Regulatory Engineering Mgr.

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen (FAX: + 49-7031-14-3143)

Notice for Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。
取り扱い説明書に従って正しい取り扱いをして下さい。

Notice for Korea

사용자 안내문 (B급 기기)

이 기기는 비업무용으로 전자파장해검정을 받은기기로서, 주거지역에서는 물론 모든 지역에서 사용 할 수 있읍니다.

Regulatory Model Identification Number

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is WA1010. The RMN should not be confused with the marketing name (Wireless Enterprise Access Point 520wl) or the Product Number (J8133A).

Introducing the 520wl

1

In This Chapter

- Wireless Networking Concepts
- Management and Monitoring Capabilities
- 802.11b/g compared to 802.11a Networks
- Installation and Initialization

Wireless Networking Concepts

The 520wl provides wireless access to network infrastructures. As wireless clients move from one coverage cell to another, 520wl units automatically allow client roaming within the same subnet.

To determine the best location for the wireless access point units, we recommend conducting a site survey before placing the devices in their final locations. For information about how to conduct a site survey, contact your local reseller.

Before the 520wl can be configured for your specific networking requirements, it must first be initialized. Initialization consists of setting a static IP address and the appropriate IP mask for the 520wl so that you can recognize it once it is located in your network.

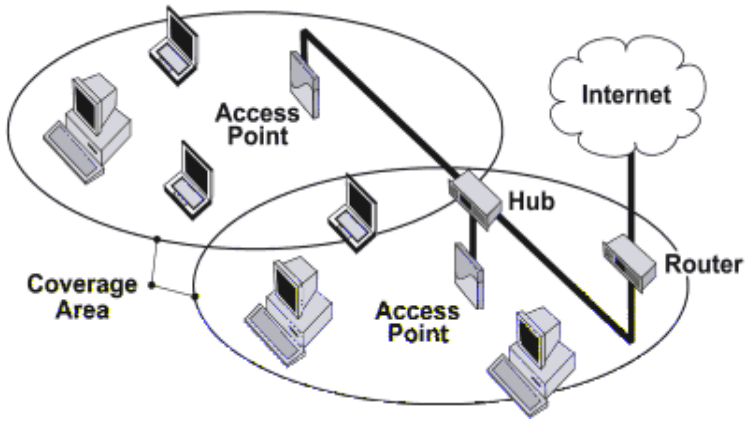


Figure 1-1 Standalone wireless network access infrastructure

The network administrator can configure each unit according to the requirements for the network. The HP ProCurve Wireless Access Point 520wl (hereafter called just “520wl”) functions as a wireless network access point (AP) to data networks. 520wl networks provide:

- Seamless client roaming
- Easy installation and operation
- Over-the-air encryption of data
- High speed network links

For the 520wl to be fully operational, at least one HP ProCurve Wireless AP Card, either the 150wl (802.11b), 160wl (802.11a), or 170wl (802.11g) must be installed.

NOTE:

The AP Cards are not included with your 520wl and must be ordered as separate items.

Management and Monitoring Capabilities

To configure the 520wl for your needs, set your specific network, wireless interface, and bridge parameters. The HTTP (web browser) Interface provides easy configuration and management.

Wireless clients (computers connected to your network through wireless access) use configuration software for network access. Once connected, users can roam from one coverage cell to another while maintaining their connection.

There are four management and monitoring interfaces available to the network administrator to configure and manage the 520wl unit(s) in the network:

1. HTTP/HTTPS Interface
2. Command Line Interface
3. Full SNMP configuration capabilities
4. SNMPv3 Secure Management

HTTP/HTTPS Interface

The HTTP Interface (Web browser Interface) provides easy access to configuration settings and network statistics from any computer in the network. Use the HTTP Interface through your LAN (switch, hub, and so forth), through the Internet, or with a crossover Ethernet cable connected directly to your computer's Ethernet Port.

HTTPS provides an HTTP connection over a Secure Socket Layer. HTTPS is one of two available secure management options on the AP; the other secure management option is SNMPv3. Enabling HTTPS allows the user to access the AP in a secure fashion using Secure Socket Layer (SSL) over port 443. The AP supports SSLv3 with a 128-bit encryption certificate maintained by the AP for secure communications between the AP and the HTTP client. All communications are encrypted using the server and the client-side certificate.

The AP comes with all required SSL files: default certificate, private key and SSL Certificate Passphrase, installed.

Command Line Interface

The Command Line Interface (CLI) represents a set of keyboard commands and parameters used for configuring and managing the 520wl.

Users enter Command Statements, composed of CLI Commands and their associated parameters. Statements may be issued from the keyboard for real time control, or from scripts that automate configuration. For example, when downloading a file, administrators enter the **download** CLI Command along with IP Address, file name, and file type parameters.

- If necessary, use the CLI with your computer serial port to initialize the proper IP address for your network.
- The CLI provides configuration and management access for most generic Telnet and Terminal clients. Use the CLI through your computer serial port, over your LAN, through the Internet, or with a crossover Ethernet cable connected directly to your computer.

Details of the CLI commands used to manage the 520wl device along with syntax and specific parameters names can be found in "Command Line Interface (CLI)."

SNMP Management

In addition to the HTTP and the CLI interfaces, you can also manage and configure a 520wl using the Simple Network Management Protocol (SNMP). This requires an SNMP manager program, like HP Openview or Castlerock's SNMPc.

The 520wl supports several Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Ethernet-like MIB (RFC 1643)
- 802.11 MIB
- Enterprise MIB

HP provides these MIB files on the 520wl CD and through the HP ProCurve website at http://www.hp.com/go/hpprocurve. You need to compile one or more of the above MIBs into your SNMP program's database before you can manage the 520wl. Refer to the documentation that came with your SNMP manager for instructions on how to compile MIBs.

The Enterprise MIB defines the read and read-write objects that can be viewed or configured using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. Refer to the Enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word or WordPad.

SNMPv3 Secure Management

SNMPv3 is one of two available secure management options on the AP; the other secure management option is HTTPS (HTTP connection over Secure Socket Layer). SNMPv3 is based on the existing SNMP framework, but addresses security requirements for device and network management.

The security threats addressed by Secure Management are:

- *Modification of information*: An entity could alter an in-transit message generated by an authorized entity in such a way as to effect unauthorized management operations, including the setting of object values. The essence of this threat is that an unauthorized entity could change any management parameter, including those related to configuration, operations, and accounting.
- *Masquerade*: Management operations that are not authorized for some entity may be attempted by that entity by assuming the identity of an authorized entity.
- *Message stream modification*: SNMP is designed to operate over a connectionless transport protocol. There is a threat that SNMP messages could be reordered, delayed, or replayed (duplicated) to effect unauthorized management operations. For example, a message to reboot a device could be copied and replayed later.
- *Disclosure*: An entity could observe exchanges between a manager and an agent and thereby learns the values of managed objects and learn of notifiable events. For example, the observation of a set command that changes passwords would enable an attacker to learn the new passwords.

To address the security threats listed above, SNMPv3 provides the following when secure management is enabled:

- Authentication: Provides data integrity and data origin authentication.
- Privacy (Encryption): Protects against disclosure of message payload.
- Access Control: Controls and authorizes access to managed objects.

NOTE:

The remainder of this guide describes how to configure a 520wl using the HTTP Web interface or the CLI interface. For information on how to manage devices using SNMP, refer to the documentation that came with your SNMP program. Also, refer to the MIB files for information on the parameters available by way of SNMP.

802.11b/g compared to 802.11a Networks

The 520wl supports 802.11 wireless connectivity through the use of 802.11a-compliant 5 GHz, 802.11b-compliant 2.4 GHz, and 802.11g-compliant 2.4 GHz radio technology. The IEEE 802.11a standard adds support for a high-speed wireless physical layer in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard requires support for data rates of 6, 12, 24, and 54 Mbps. The 520wl supports the following data rates: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s. The IEEE 802.11b standard supports wireless physical layer 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 Mbits/s.

The new IEEE 802.11g standard adds support for a high-speed wireless physical layer in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard requires support for data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

The 520wl can be used with any combination of 802.11a, 802.11b, and 802.11g AP Cards. You can have an 802.11a and an 802.11b or 802.11g card present in the 520wl at the same time and 2.4 GHz and 5 GHz clients will be supported simultaneously. Note however that only one 802.11a card with antenna adapter can be plugged into the 520wl at one time.

Feature List

The IEEE standards that govern wireless communications are different for the 2.4 GHz band and the 5 GHz band. The table below compares the software features supported for each type of card in the 520wl:

Feature	2.4 GHz (802.11b)	2.4 GHz (802.11g)	5 GHz (802.11a)	Comments
Number of stations per AP	up to 250	up to 128	up to 128	This information corresponds to a cas where no encryption is enabled. For more information about the number of stations supported when using different types of encryption, please see the table “Number of Stations per BSS” located in appendix A.
HTTP/HTTPS Server	yes	yes	yes	
Telnet / CLI	yes	yes	yes	
SNMP/SNMPv3 support	yes	yes	yes	
VLAN Support (16 User VLANs)	no	yes	no	
Emergency Reset to Default Configuration	yes	yes	yes	
DHCP Client	yes	yes	yes	
DHCP Server	yes	yes	yes	
TFTP	yes	yes	yes	
RADIUS Mac-based Access Control	yes	yes	yes	
Fallback to Primary RADIUS Server	yes	yes	yes	
RADIUS Session Timeout	yes	yes	yes	
RADIUS Multiple MAC Address Formats	yes	yes	yes	
RADIUS DNS Host Name Support	yes	yes	yes	
RADIUS Start/Stop Accounting	yes	yes	yes	
802.1X (EAP-MD5, EAP-TLS and EAP-TTLS)	yes	yes	yes	
802.1d bridging	yes	yes	yes	
MAC Access Control Table	yes	yes	yes	
Protocol Filtering	yes	yes	yes	
Multicast/Broadcast Storm Filtering	yes	yes	yes	
Proxy ARP	yes	yes	yes	
Roaming	yes	yes	yes	
Link Integrity	yes	yes	yes	
Automatic Channel Select	yes	yes	yes	
WEP	yes	yes	yes	Key lengths supported for 802.11b: 64-bit and 128-bit Key lengths supported for 802.11a and 802.11g: 64-bit, 128-bit, and 152-bit (Note: Some products refer to 64-bit as “40-bit”, 128-bit as “104-bit”, and 152-bit as “128-bit”.)
WEP Plus (Weak Key Avoidance)[1]	yes	no	no	
WDS Relay	yes	yes	yes	
Remote Link Test[1]	yes	no	no	
Medium Density Distribution[1]	yes	no	no	
Distance between APs	yes	no	no	

Feature	2.4 GHz (802.11b)	2.4 GHz (802.11g)	5 GHz (802.11a)	Comments
Closed System	yes	yes	yes	
Interference Robustness	yes	no	no	
Load Balancing[1]	yes	no	no	
AP List[1]	yes	no	no	No client support for 802.11a
SpectraLink VoIP Support	yes	no	no	
Blocking Intra BSS Clients	yes	yes	yes	
Packet Forwarding	yes	yes	yes	
TCP/UDP Port Filtering	yes	yes	yes	
Dynamic Frequency Selection	N/A	N/A	yes	A user cannot manually select a channel for products sold in Europe; these products require automatic channel selection using Dynamic Frequency Selection (DFS).
Per User Per Session Encryption	no	yes	yes	In conjunction with 802.1x or WPA[2]
Syslog Messaging	yes	no	yes	
Turbo Mode	no	no	yes	Turbo mode provides twice the data rate of standard 802.11a mode; not available in all countries.
Monitoring Station Statistics	yes	yes	yes	
Secure Socket Layer (SSL)	yes	yes	yes	
Rogue AP Detection Support	no	yes	yes	
TX Power Control	no	yes	no	
Auto Configuration	yes	yes	yes	
Multiple Authentication Server Support	yes	yes	yes	
Dynamic Domain Name Service (DDNS)	yes	yes	yes	
AP System Naming Convention	yes	yes	yes	
WiFi Protected Access (WPA)	no	yes	no	

[1] This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150WL. In addition, this feature will only give information for ORiNOCO/Agere/Lucent based clients.

[2] WPA is supported only in the HP ProCurve Wireless 802.11g AP Card 170WL.

The following table provides detailed information on the differences between the 802.11a and 802.11b/g feature sets.

	2.4 GHz (802.11b)	2.4 GHz (802.11g)	5 GHz (802.11a)
Physical Layer Type (Modulation Type)	DSSS (Direct Sequence Spread Spectrum)	ODFM (Orthogonal Frequency Division Multiplexing)	ODFM (Orthogonal Frequency Division Multiplexing)
Auto Channel Select (ACS)	Enable (default) Disable Note: If your country has channel restrictions the ACS feature on the 150wl card should be disabled and you should configure an appropriate channel for your country manually. Use the table below and the *HP ProCurve Wireless Products Regulatory and Radio Approvals Booklet* to determine which channels you can use in your country.	Enable (default) Disable Note: If your country has channel restrictions the ACS feature on the 170wl card should be disabled and you should configure an appropriate channel for your country manually. Use the table below and the *HP ProCurve Wireless Products Regulatory and Radio Approvals Booklet* to determine which channels you can use in your country.	Enable (default) Disable Note: A user cannot manually select a channel for products sold in Europe; these products require automatic channel selection using DFS. See "Dynamic Frequency Selection (DFS)."
Frequency Channel	1 - 2.412 GHz 2 - 2.417 GHz 3 - 2.422 GHz (default FCC, ETSI, Japan) 4 - 2.427 GHz 5 - 2.432 GHz 6 - 2.437 GHz 7 - 2.442 GHz 8 - 2.447 GHz 9 - 2.452 GHz 10 - 2.457 GHz 11 - 2.462 GHz 12 - 2.467 GHz (ETSI countries only) 13 - 2.472 GHz 14 - 2.484 GHz (Japan only) For France, channels 10-13 only	1 - 2.412 GHz 2 - 2.417 GHz 3 - 2.422 GHz 4 - 2.427 GHz 5 - 2.432 GHz 6 - 2.437 GHz 7 - 2.442 GHz 8 - 2.447 GHz 9 - 2.452 GHz 10 - 2.457 GHz (default FCC, ETSI, Japan) 11 - 2.462 GHz 12 - 2.467 GHz (ETSI countries only) 13 - 2.472 GHz 14 - 2.484 GHz (Japan only) For France, channels 10-13 only Channel 14 is only available when using the .11b only mode.	36 - 5.180 GHz 40 - 5.200 GHz 44 - 5.220 GHz 48 - 5.240 GHz 52 - 5.260 GHz (default FCC) 56 - 5.280 GHz 60 - 5.300 GHz 64 - 5.320 GHz Channels 36-64 are valid for products in the FCC regulatory domain. The following channels are available in Europe: 36 - 5.180 GHz (default) 40 - 5.200 GHz 44 - 5.220 GHz 48 - 5.240 GHz The following channels are available in Japan: 34 - 5.170 GHz (default) 38 - 5.190 GHz 42 - 5.210 GHz 46 - 5.230 GHz For Turbo mode (not available in all countries), the following channels are available: 42 - 5.210 GHz 50 - 5.250 GHz 58 - 5.290 GHz
Regulatory Domain	USA (FCC) Canada (DOC) Europe (ETSI) France (FR) Japan (MKK)	USA (FCC) Canada (DOC) Europe (ETSI) France (FR) Japan (MKK)	USA (FCC) Canada (DOC) Europe (ETSI) Japan (MKK)

continued on the next page

	2.4 GHz (802.11b)	2.4 GHz (802.11g)	5 GHz (802.11a)
Transmit Rate	1 Mbps 2 Mbps 5.5 Mbps 11 Mbps	6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps	0 - Auto Fallback (default) 6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps For Turbo mode (not available in all countries): 0 - Auto Fallback (default) 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 72 Mbps 96 Mbps 108 Mbps
Distance Between APs	large (default) medium small minicell microcell	large (default) medium small	N/A
Multicast Rate	1 Mbps 2 Mbps (default) 5.5 Mbps 11 Mbps Available options depend on **Distance Between APs** setting	N/A	N/A
Interference Robustness	Enable (default) Disable		N/A
Closed System	Enable Disable (default)	Enable Disable (default)	Enable Disable (default)
Load Balancing	Enable (default) Disable		N/A
Medium Density Distribution	Enable (default) Disable		N/A

Cell Size and Coverage Area

The coverage area achieved with the 2.4 GHz card type is larger than that of a 5 GHz card. The transmit rate is higher in the smaller (5 GHz) cell than the larger (2.4 GHz cell). The following illustrations depict the difference in cell sizes and the way that cell size affects coverage area.

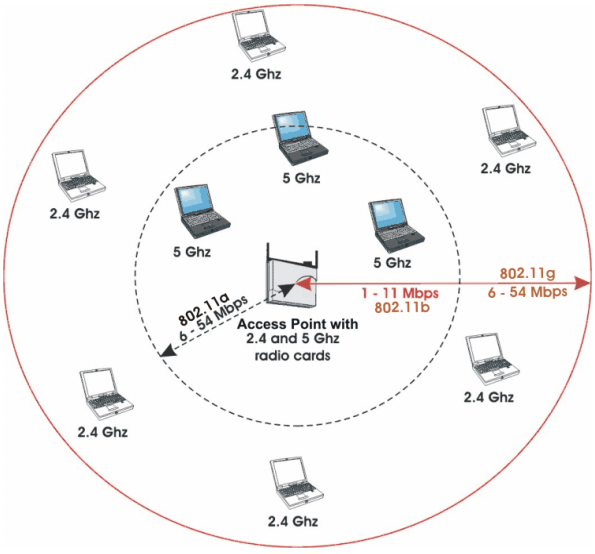


Figure 1-2 Cell Size and Coverage Area

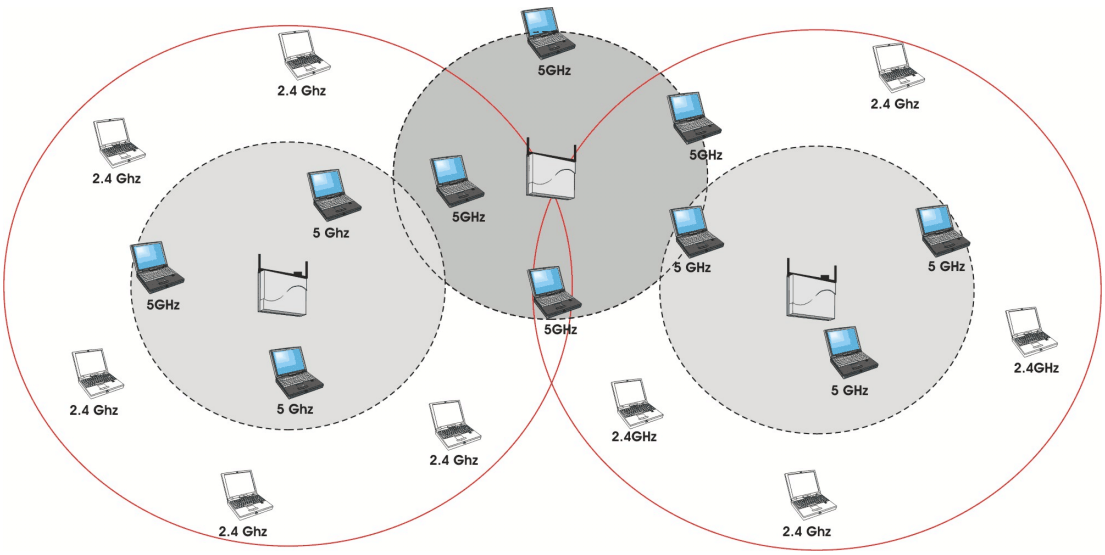


Figure 1-3 802.11a compared to 802.11b/g Coverage Area

Installation and Initialization

The 520wl is designed to support both 2.4 GHz (IEEE 802.11b), 2.4 GHz (IEEE 802.11g), and 5 GHz (IEEE 802.11a) AP Cards. The HP ProCurve Wireless 802.11a Access Point Kit 160wl has an antenna adapter which snaps into place on the existing wall mounting bracket. Because of the antenna adapter, only one 160wl card can be installed in the AP. The second slot can be populated with an HP ProCurve Wireless Access Point card 150wl (802.11b), or 170wl (802.11g).

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements the following antenna installation and device operating configurations must be satisfied:

a. For configurations using the integral antenna the separation distance between the antenna(s) and any person's body (including hands, wrists, feet, and ankles) must be at least 2.5 cm (1 inch).

b. For configurations using an approved external antenna the separation distance between the antenna and any person's body (including hands, wrists, feet, and ankles) must be at least 20 cm (8 inches).

The transmitter shall not be collocated with other transmitters or antennas.

Getting Started

2

In This Chapter

- Prerequisites
- Product Package
- System Requirements
- Hardware Installation
- Hardware Installation
- Initialization
- Download the Latest Software
- Additional Hardware Features

Prerequisites

Before installing an AP, you need to gather certain network information. The following section identifies the information you need.

Network Name (SSID of the wireless cards)	You must assign the Access Point a Network Name before wireless users can communicate with it. The clients also need the same Network Name. This is not the same as the System Name, which applies only to the Access Point. The network administrator typically provides the Network Name.
AP's IP Address	If you do not have a DHCP server on your network, then you need to assign the Access Point an IP address that is valid on your network.
HTTP Password	Each Access Point requires a read/write password to access the web interface. The default password is "public".
CLI Password	Each Access Point requires a read/write password to access the CLI interface. The default password is "public".
SNMP Read Password	Each Access Point requires a password to allow get requests from an SNMP manager. The default password is "public".
SNMP Read-Write Password	Each Access Point requires a password to allow get and set requests from an SNMP manager. The default password is "public".
SNMPv3 Authentication Password	If Secure Management is enabled, each Access Point requires a password for sending authenticated SNMPv3 messages. The default password is "public".
SNMPv3 Privacy Password	If Secure Management is enabled, each Access Point requires a password when sending encrypted SNMPv3 data. The default password is "public".
Security Settings	You need to determine what security features you will enable on the Access Point.
Authentication Method	A primary authentication server may be configured; a back-up authentication server is optional. The network administrator typically provides this information.
Authentication Server Shared Secret	This is a password shared between the Access Point and the RADIUS authentication server (so both passwords must be the same), and is typically provided by the network administrator.
Authentication Server Authentication Port	This is a port number (default is 1812) and is typically provided by the network administrator.
Client IP Address Pool Allocation Scheme	The Access Point can automatically provide IP addresses to clients as they sign on. The network administrator typically provides the IP Pool range.
DNS Server IP Address	The network administrator typically provides this IP Address.

Product Package

Each AP comes with the following:

- One mounting plate
- Mounting hardware
- Metal faceplate for APs mounted in a plenum environment
- AP cover
- Processor module
- Power supply
- AC power cord
- One Installation CD-ROM that contains the following:
  - Software Installation Wizard
  - ScanTool
  - TFTP software
  - HTML Help
  - This user's guide in PDF format
- One *Unit Installation Quick Start Guide* - foldout

If any of these items are missing or damaged, contact your reseller or see the support document that came with your AP for contact information.

AP Cards

APs can be fitted with different radio type AP Cards. AP Cards are available for 802.11a, 802.11b, and 802.11g.

System Requirements

To begin using an AP, you must have the following minimum requirements:

- A 10Base-T Ethernet or 100Base-TX Fast Ethernet switch or hub.
- At least one radio card designed for the AP: an HP ProCurve Wireless 802.11a Access Point Kit 160wl, 802.11b Access Point card 150wl, or 802.11g Access Point card 170wl.
- At least one of the following IEEE 802.11-compliant devices:
  - An 802.11a client device if you have an HP ProCurve Wireless 802.11a Access Point Kit 160wl
  - An 802.11b or 802.11g client device if you have an HP ProCurve Wireless Access Point card 150wl (802.11b) or 170wl (802.11g)
- A computer that is connected to the same IP network as the AP and has one of the following Web browsers installed:
  - Microsoft Internet Explorer 6 with Service Pack 1 or later and patch Q323308
  - Netscape 6.1 or later

  (The computer is required to configure the AP using the HTTP interface.)

Hardware Installation

Follow these steps to install your AP:

1. Clip the power supply into the mounting bracket.
2. Plug the AC power cord into the power supply.

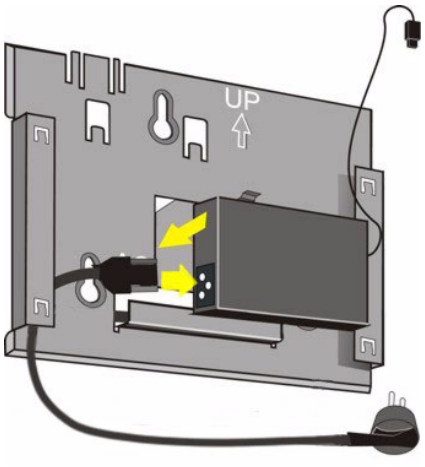


Figure 2-1 Install the power supply

3. Slide the AP module onto the mounting bracket. Ensure it is properly seated. It mounts over the power supply.
4. Plug the DC connector from the power supply into the top of the AP module.

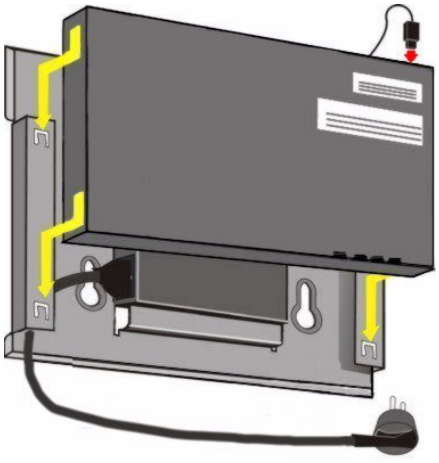


Figure 2-2 Insert module in mounting bracket and attach power connector

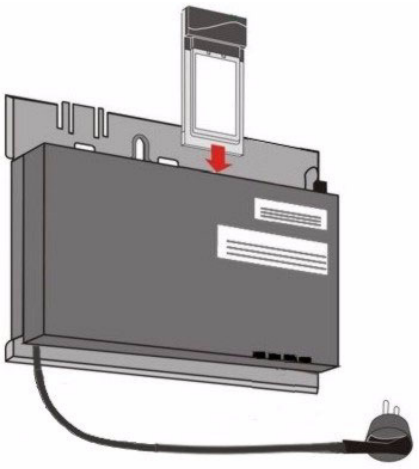


Figure 2-3 Slide an AP Card into the AP

5. Slide an AP Card (not included in the kit) into slot A or B of the AP.
6. Connect the unit to a power source, such as a wall outlet.
7. Wait for the power LED to turn green before proceeding.

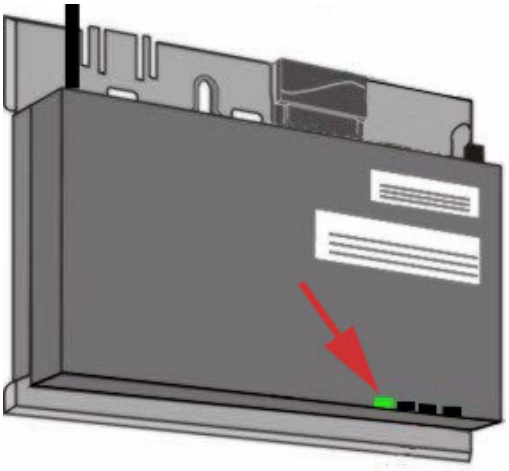


Figure 2-4 Power LED turns green when the unit is operational

8. Conduct a Site Survey to determine the best location for your device.
9. Once you have chosen a final location for your unit, mount the bracket and the processor module and place the cover onto the unit as shown.

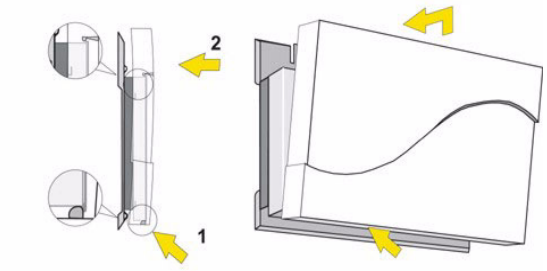


Figure 2-5 Final Installation with Cover

10. Connect one end of an Ethernet cable to the AP's Ethernet port. The other end of the cable should not be connected to any other device until after the installation is complete.
    - Use a straight-through Ethernet cable to connect the AP to a hub, switch, or patch panel.
    - Use a cross-over Ethernet cable to connect to a single computer.
11. Configure and test the unit. See Initialization for details.
12. Download the latest software to the unit, if necessary. HP provides access point software updates through the HP ProCurve website at http://www.hp.com/go/hpprocurve. See Download the Latest Software for details.

Initialization

HP provides two tools to simplify the initialization and configuration of an AP:

- ScanTool
- Setup Wizard

ScanTool is included on the Installation CD; the Setup Wizard launches automatically the first time you access the HTTP interface.

NOTE

These initialization instructions describe how to configure an AP over an Ethernet connection using ScanTool and the HTTP interface. If you want to configure the unit over the serial port, see Setting IP Address using Serial Port for information on how to access the CLI over a serial connection and Command Line Interface (CLI) for a list of supported commands.

ScanTool

ScanTool is a software utility that is included on the 520wl CD and through the HP ProCurve website at http://www.hp.com/go/hpprocurve. ScanTool allows you to find the IP address of an Access Point by referencing the MAC address in a Scan List, or to assign an IP address if one has not been assigned.

The tool automatically detects the Access Points installed on your network, regardless of IP address, and lets you configure each unit's IP settings. In addition, you can use ScanTool to download new software to an AP that does not have a valid software image installed (see Client Connection Problems).

To access the HTTP interface and configure the AP, the AP must be assigned an IP address that is valid on its Ethernet network. By default, the AP is configured to obtain an IP address automatically from a network Dynamic Host Configuration Protocol (DHCP) server during boot-up. If your network contains a DHCP server, you can run ScanTool to find out what IP address the AP has been assigned. If your network does not contain a DHCP server, the Access Point's IP address defaults to 10.0.0.1. In this case, you can use ScanTool to assign the AP a static IP address that is valid on your network.

ScanTool Instructions

Follow these steps to install ScanTool, initialize the Access Point, and perform initial configuration:

1. Locate the unit's Ethernet MAC address and write it down for future reference. The MAC address is printed on the product label. Each unit has a unique MAC address, which is assigned at the factory.
2. Confirm that the AP is connected to the same LAN subnet as the computer that you will use to configure the AP.
3. Power up, reboot, or reset the AP.
   – Result: The unit requests an IP Address from the network DHCP server.
4. Insert the Installation CD into the CD-ROM drive of the computer that you will use to configure the AP.
   – Result: The installation program will launch automatically.
5. Follow the on-screen instructions to install the Access Point software and documentation.

NOTE

The Installation program supports the following operating systems:

- Windows 98SE
- Windows 2000
- Windows NT
- Windows ME
- Windows XP

6. After the software has been installed, double-click the **ScanTool** icon on the Windows desktop to launch the program (if the program is not already running).
   – Result: ScanTool scans the subnet and displays all detected Access Points. The ScanTool's ***Scan List*** screen appears, as shown in the following example.

NOTE

If your computer has more than one network adapter installed, you will be prompted to select the adapter that you want ScanTool to use before the ***Scan List*** appears. If prompted, select an adapter and click **OK**. You can change your adapter setting at any time by clicking the **Select Adapter** button on the ***Scan List*** screen. Note that the ***ScanTool Network Adapter Selection*** screen will not appear if your computer only has one network adapter installed.

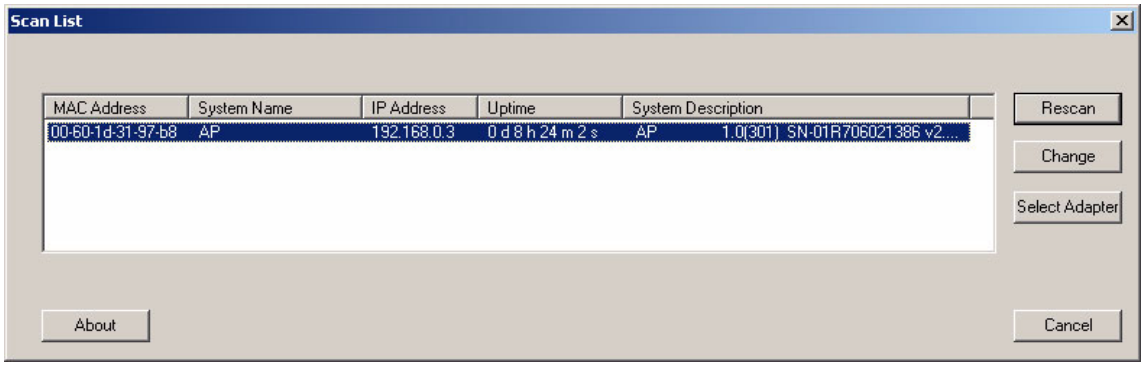


Figure 2-6 Scan List

7. Locate the MAC address of the AP you want to initialize within the Scan List.

NOTE

If your Access Point does not show up in the Scan List, click the **Rescan** button to update the display. If the unit still does not appear in the list, see Troubleshooting for suggestions. After rebooting an Access Point, it may take up to five minutes for the unit to appear in the Scan List.

8. Do one of the following:
   - If the AP has been assigned an IP address by a DHCP server on the network, write down the IP address and click **Cancel** to close ScanTool. Proceed to Setup Wizard for information on how to access the HTTP interface using this IP address.
   - If the AP has not been assigned an IP address (in other words, the unit is using its default IP address, 10.0.0.1), follow these steps to assign it a static IP address that is valid on your network:
     1. Highlight the entry for the AP you want to configure.
     2. Click the **Change** button.

     — Result: the ***Change*** screen appears.

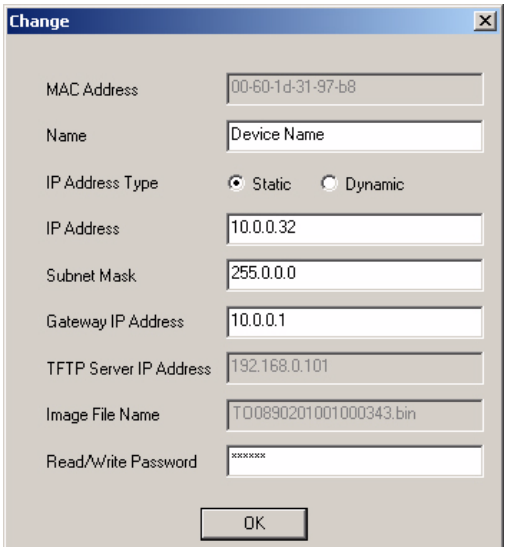


Figure 2-7 Scan Tool Change Screen

3. Set **IP Address Type** to **Static**.
4. Enter a static **IP Address** for the AP in the field provided. You must assign the unit a unique address that is valid on your IP subnet. Contact your network administrator if you need assistance selecting an IP address for the unit.
5. Enter your network's **Subnet Mask** in the field provided.
6. Enter your network's **Gateway IP Address** in the field provided.
7. Enter the SNMP Read/Write password in the **Read/Write Password** field (for new units, the default SNMP Read/Write password is "public").

NOTE

The TFTP Server IP Address and Image File Name fields are only available if ScanTool detects that the AP does not have a valid software image installed. See Client Connection Problems.

8. Click **OK** to save your changes.
   — Result: The Access Point will reboot automatically and any changes you made will take effect.
9. When prompted, click **OK** a second time to return to the ***Scan List*** screen.
10. Click **Cancel** to close the ScanTool.
11. Proceed to Setup Wizard for information on how to access the HTTP interface.

Logging into the HTTP Interface

Once the AP has a valid IP Address and an Ethernet connection, you may use your web browser to monitor network statistics.

The Command Line Interface (CLI) also provides a method for viewing network statistics using Telnet or a serial connection. This section covers only use of the HTTP interface. For more information about viewing network statistics with the CLI, refer to Command Line Interface (CLI).

Follow these steps to monitor an AP's operating statistics using the HTTP interface:

1. Open a Web browser on a network computer.

NOTE

The HTTP interface supports the following Web browser:

- Microsoft Internet Explorer 6 with Service Pack 1 or later
- Netscape 6.1 or later

2. If necessary, disable the Internet proxy settings. For Internet Explorer users, follow these steps:
   – Select **Tools > Internet Options...**.
   – Click the **Connections** tab.
   – Click **LAN Settings...**.
   – If necessary, remove the check mark from the **Use a proxy server** box.
   – Click **OK** twice to save your changes and return to Internet Explorer.
3. Enter the Access Point's IP address in the browser's **Address** field and press **Enter**.
   – Result: The AP ***Enter Network Password*** screen appears.
4. Enter the HTTP password in the **Password** field and click **OK**. Leave the **User Name** field blank. (By default, the HTTP password is "public").
   – Result: The ***System Status*** screen appears.

Figure 2-8 Enter Network Password Screen

Setup Wizard

The first time you connect to an AP's HTTP interface, the Setup Wizard launches automatically. The Setup Wizard provides step-by-step instructions for how to configure the Access Point's basic operating parameter, such as Network Name, IP parameters, system parameters, and management passwords.

Setup Wizard Instructions

The first time you logon to the AP HTTP interface, the Setup Wizard launches. Follow these steps to access the Access Point's HTTP interface and launch the Setup Wizard:

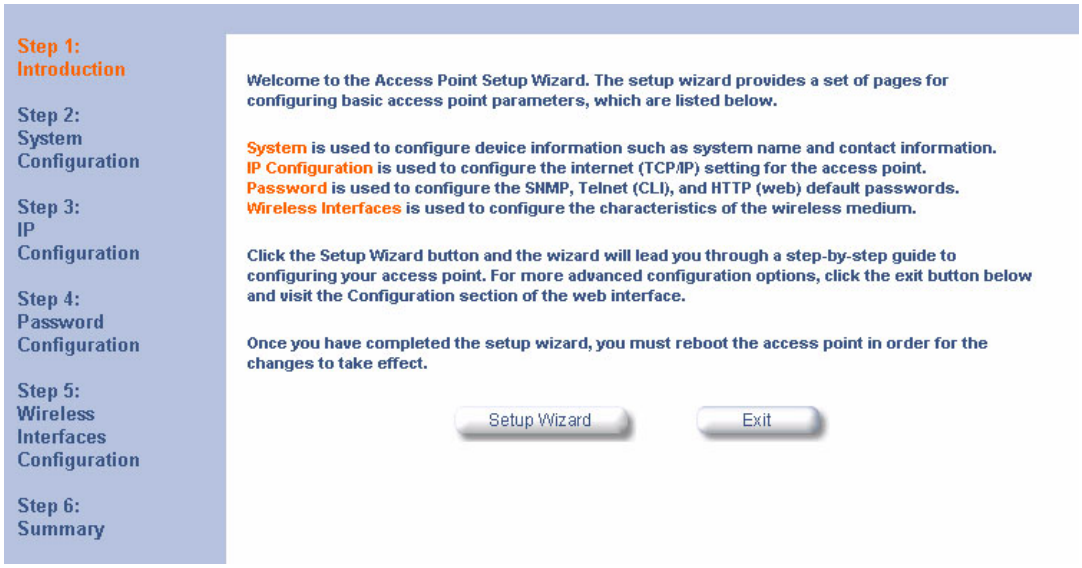


Figure 2-9 Setup Wizard

5. Click **Setup Wizard** to begin. If you want to configure the AP without using the Setup Wizard, click **Exit** and see Advanced Configuration.

   The Setup Wizard supports the following navigation options:

   - **Save & Next Button:** Each Setup Wizard screen has a **Save & Next** button. Click this button to submit any changes you made to the unit's parameters and continue to the next page. The instructions below describe how to navigate the Setup Wizard using the **Save & Next** buttons.

- **Navigation Panel:** The Setup Wizard provides a navigation panel on the left-hand side of the screen. Click the link that corresponds to the parameters you want to configure to be taken to that particular configuration screen. Note that clicking a link in the navigation panel will not submit any changes you made to the unit's configuration on the current page.
- **Exit:** The navigation panel also includes an **Exit** option. Click this link to close the Setup Wizard at any time.

CAUTION

If you exit from the Setup Wizard, any changes you submitted (by clicking the **Save & Next** button) up to that point will be saved to the unit but will not take effect until it is rebooted.

6. Configure the System Configuration settings and click **Save & Next**. See System for more information.
7. Configure the Access Point's Basic IP address settings, if necessary, and click **Save & Next**. See Basic IP Parameters for more information.
8. Assign the AP new passwords to prevent unauthorized access and click **Save & Next**. Each management interface has its own password:
   - SNMP Read Password
   - SNMP Read-Write Password
   - SNMPv3 Authentication Password
   - SNMPv3 Privacy Password
   - CLI Password
   - HTTP (Web) Password

   By default, each of these passwords is set to "public". See Passwords for more information.
9. Configure the basic wireless interface settings and click **Save & Next**.
   - The following options are available for an 802.11a AP:
     - **Network Name (SSID):** Enter a Network Name (between 2 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well.
     - **Auto Channel Select:** By default, the AP scans the area for other Access Points and selects the best available communication channel, either a free channel (if available) or the channel with the least amount of interference. Remove the check mark to disable this option. Note that you cannot disable Auto Channel Select for 802.11a products in Europe (see Dynamic Frequency Selection (DFS) for details).
     - **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency. Available Channels vary based on regulatory domain. See 802.11a Channel Frequencies. Note that you cannot manually set the channel for 802.11a products in Europe (see Dynamic Frequency Selection (DFS) for details).
     - **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the AP. Choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback. The Auto Fallback feature allows the AP to select the best transmit rate based on the cell size.
     - **WEP Encryption:** Place a check mark in the box provided to enable WEP encryption. See WEP Encryption for more information.
     - **Set Encryption Key 1:** If you enabled Encryption, configure an Encryption Key. This key is used to encrypt and decrypt data between the AP and its wireless clients. Enter the number of characters that correspond to the desired key size, as described below:
       - Enter 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart) to use 64-bit encryption.
       - Enter 26 hexadecimal characters or 13 ASCII characters to use 128-bit encryption.
       - Enter 32 hexadecimal characters or 16 ASCII characters to use 152-bit encryption.
   - The following options are available for an 802.11b AP:
     - **Network Name (SSID):** Enter a Network Name (between 2 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well.
     - **Auto Channel Select:** By default, the AP scans the area for other Access Points and selects the best available communication channel, either a free channel (if available) or the channel with the least amount of interference. Remove the check mark to disable this option. If you are setting up a Wireless Distribution System (WDS), it must be disabled. See Wireless Distribution System (WDS) for more information.

— **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's operating channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency (unless you are setting up a WDS). Available Channels vary based on regulatory domain. See 802.11b Channel Frequencies.

— **Distance Between APs:** Set to **Large**, **Medium**, **Small**, **Microcell**, or **Minicell** depending on the site survey for your system. The distance value is related to the **Multicast Rate** (described next). In general, a larger distance between APs means that your clients operate a slower data rates (on average). See Distance Between APs for more information.

- **Multicast Rate:** Sets the rate at which Multicast messages are sent. This value is related to the **Distance Between APs** parameter (described previously). The table below displays the possible Multicast Rates based on the Distance between APs. See Multicast Rate for more information.

Distance between APs	Multicast Rate
Large	1 and 2 Mbits/sec
Medium	1, 2, and 5.5 Mbits/sec
Small	1, 2, 5.5 and 11 Mbits/sec
Minicell	1, 2, 5.5 and 11 Mbits/sec
Microcell	1, 2, 5.5 and 11 Mbits/sec

- **WEP Encryption:** Place a check mark in the box provided to enable WEP encryption. See WEP Encryption for more information.
- **Set Encryption Key 1:** If you enabled Encryption, configure an Encryption Key. This key is used to encrypt and decrypt data between the AP and its wireless clients. Enter the number of characters that correspond to the desired key size, as described below:
  - Enter 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart) to use 64-bit encryption.
  - Enter 26 hexadecimal characters (0-9 and A-F) or 13 ASCII characters to use 128-bit encryption.

- The following options are available for an 802.11b/g AP:
  - **Operational Mode:** An 802.11b/g wireless interface can be configured to operate in the following modes:
    - 802.11b mode only
    - 802.11g mode only
    - 802.11g-wifi mode (Although this is a valid option, the .11g AP Card is not Wi-Fi certified.)
    - 802.11b/g mode (default)
  - **Network Name (SSID):** Enter a Network Name (between 2 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well.
  - **Auto Channel Select:** By default, the AP scans the area for other Access Points and selects the best available communication channel, either a free channel (if available) or the channel with the least amount of interference. Remove the check mark to disable this option.
  - **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency. Available Channels vary based on regulatory domain. See 802.11g Channel Frequencies.
  - **Transmit Rate:** Select a specific transmit rate for the AP. The values available depend on the Operational Mode. Auto Fallback is the default setting; it allows the AP to select the best transmit rate based on the cell size.
    - For 802.11b only -- Auto Fallback, 1, 2, 5.5, 11 Mbits/sec.
    - For 802.11g only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/sec.
    - For 802.11b/g and 802.11g-wifi-- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec.
  - **WEP Encryption:** Place a check mark in the box provided to enable WEP encryption. See WEP Encryption for more information.
  - **Set Encryption Key 1:** If you enabled Encryption, configure an Encryption Key. This key is used to encrypt and decrypt data between the AP and its wireless clients. Enter the number of characters that correspond to the desired key size, as described below:
    - Enter 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart) to use 64-bit encryption.
    - Enter 26 hexadecimal characters or 13 ASCII characters to use 128-bit encryption.
    - Enter 32 hexadecimal characters or 16 ASCII characters to use 152-bit encryption.

NOTE

Additional advanced settings are available in the ***Wireless Interface Configuration*** screen. See Wireless (802.11a), Wireless (802.11b), or Wireless (802.11b/g) for details. See Security for more information on security features.

10. Review the configuration summary. If you want to make any additional changes, use the navigation panel on the left-hand side of the screen to return to an earlier screen. After making a change, click **Save & Next** to save the change and proceed to the next screen.
11. When finished, click **Reboot** on the Summary screen to restart the AP and apply your changes.

Download the Latest Software

HP periodically releases updated software for the AP on its Web site at http://www.hp.com/go/hpprocurve. HP recommends that you check the Web site for the latest updates after you have installed and initialized the unit.

Three types of files can be downloaded to the AP from a TFTP server:

- image (AP software image or kernel)
- config (configuration file)
- bspBl (BSP/Bootloader firmware file)

Setup your TFTP Server

A Trivial File Transfer Protocol (TFTP) server allows you to transfer files across a network. You can upload files from the AP for backup or copying, and you can download the files for configuration and AP Image upgrades. The TFTP server software is located on the installation CD-ROM.

NOTE

If a TFTP server is not available in the network, you can perform similar file transfer operations using the HTTP interface.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP address, the proper AP Image file name, and that the TFTP server is operational.
- **Make sure the TFTP server is configured to both Transmit and Receive files, with no automatic shutdown or time-out.**

Download Updates from your TFTP Server using the Web Interface

1. Download the latest software from http://www.hp.com/go/hpprocurve.
2. Copy the latest software updates to your TFTP server.
3. In the Web Interface, click the **Commands** button and select the **Download** tab.
4. Enter the IP address of your TFTP server in the field provided.
5. Enter the **File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.
6. Select the **File Type** from the drop-down menu (use *Img* for software updates).
7. Select **Download & Reboot** from the **File Operation** drop-down menu.
8. Click **OK**.
9. The Access Point will reboot automatically when the download is complete.

Download Updates from your TFTP Server using the CLI Interface

1. Download the latest software from http://www.hp.com/go/hpprocurve.
2. Copy the latest software updates to your TFTP server.
3. Open the CLI interface by way of Telnet or a serial connection.
4. Enter the CLI password when prompted.
5. Enter the command: **download <tftpaddr> <filename> img**
   – Result: The download will begin. Be patient while the image is downloaded to the Access Point.
6. When the download is complete, type **reboot 0** and press **Enter**.

NOTE

See Command Line Interface (CLI) for more information.

Additional Hardware Features

- Installing the AP in a Plenum
- LED Indicators

Installing the AP in a Plenum

In an office building, plenum is the space between the structural ceiling and the tile ceiling that is provided to help air circulate. Many companies also use the plenum to house communication equipment and cables. However, these products and cables must comply with certain safety requirements, such as Underwriter Labs (UL) Standard 2043: “Standard for Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces”.

The AP has been certified under UL Standard 2043 and can be installed in the plenum only when the following conditions apply:

- The unit's plastic cover has been removed.
- The power supply of the Access Point has been removed.
- There are two 802.11b or 11g cards in the cards slots.

  OR
- There is one 802.11b card and the other card slot is protected with the metal faceplate provided in your kit.

NOTE

The HP ProCurve Wireless 802.11a Access Point Kit160wl is not approved in accordance with UL-2043 for use in a plenum. The Access Point using a power supply, should not be plenum mounted. Use Active Ethernet to power the units mounted in a plenum environment.

Installing/Removing the Metal Faceplate

When using only one card in the AP mounted in a plenum environment, remove the plastic cover. Place the top edge of the faceplate under the front ridge of the metal enclosure. Snap the faceplate in the empty card slot in the AP.

CAUTION

Do not drop the faceplate into the card slot in the AP.

To install a second radio card, the faceplate must be removed. Gently pry the faceplate off using the tab on the faceplate.

LED Indicators

The AP has four LED indicators, which exhibit the following behavior:

Power	Ethernet	PC Card A	PC Card B	Indication
Green	Green flash with data activity	Green flash with data activity	Green flash with data activity	Normal Operation
Amber	Red	Amber	Amber	Rebooting/Power On Self Test (POST)
Amber	n/a (not applicable)	n/a	n/a	Missing or bad AP Image if amber after reboot
Red	Red	n/a	n/a	Power On Self Test (POST) running
n/a	n/a	Red	Red	PC Card incompatible on indicated interface
n/a	n/a	Red	Red	PC Card failure on indicated interface
Green	n/a	Amber	Amber	Indicated interface in Administrative State

n/a	n/a	Off	Off	PC Card not present

Related Topics

The Setup Wizard helps you configure the basic AP settings required to get the unit up and running. The AP supports many other configuration and management options. The remainder of this user guide describes these options in detail.

- See Advanced Configuration for information on configuration options that are available within the Access Point's HTTP interface.
- See Monitor Information for information on the statistics displayed within the Access Point's HTTP interface.
- See Commands for information on the commands supported by the Access Point's HTTP interface.
- See Troubleshooting for troubleshooting suggestions.
- See Command Line Interface (CLI) for information on the CLI interface and for a list of CLI commands.

Status Information

3

System Status

System Status is the first screen to appear each time you connect to the HTTP interface. You can also return to this screen by clicking the **Status** button.

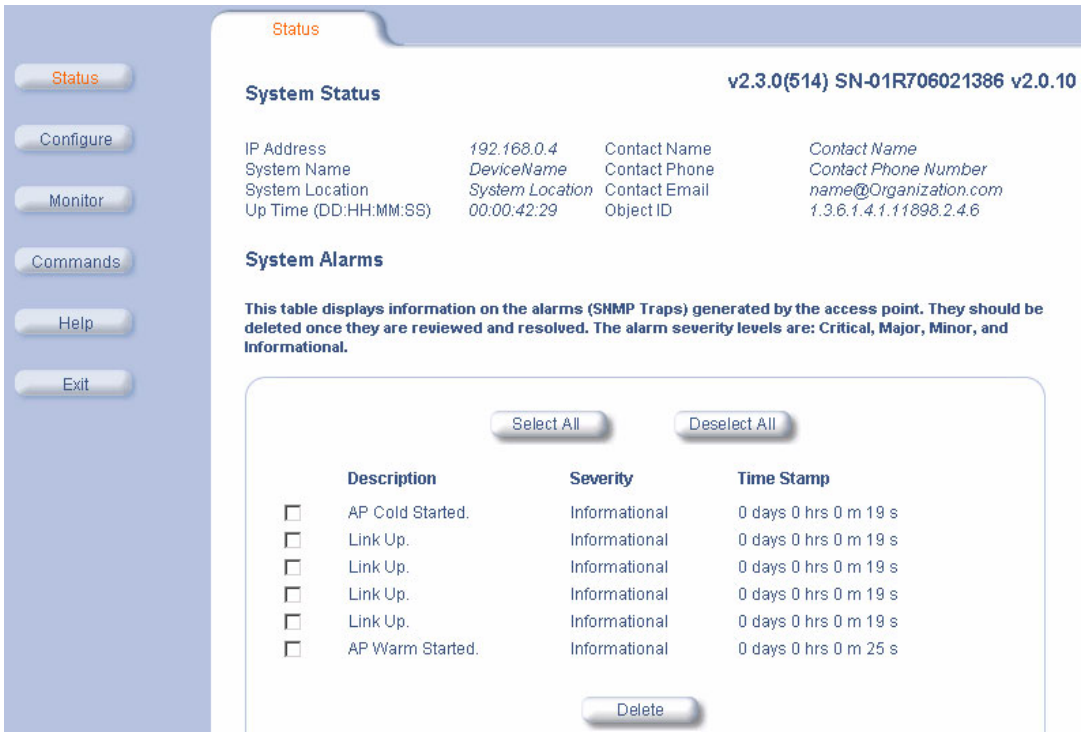


Figure 3-1 System Status Screen

Each section of the ***System Status*** screen provides the following information:

- **System Status:** This area provides system level information, including the unit's IP address and contact information. See System for information on these settings.
- **System Alarms:** System traps (if any) appear in this area. Each trap identifies a specific severity level: Critical, Major, Minor, and Informational. See Alarms for a list of possible alarms.

Advanced Configuration

4

In This Chapter

- Configuring the AP Using the HTTP/HTTPS Interface.
- System: Configure specific system information such as system name and contact information.
- Network: Configure IP settings, DNS client, DHCP server, and Link Integrity.
- Interfaces: Configure the Access Point's interfaces: Wireless and Ethernet. Also describes configuring a Wireless Distribution System (WDS).
- Management: Configure the Access Point's management Passwords, IP Access Table, and Services such as configuring secure or restricted access to the AP by way of SNMPv3, HTTPS, or CLI. Set up Automatic Configuration for Static IP.
- Filtering: Configure Ethernet Protocol filters, Static MAC Address filters, Advanced filters, and Port filters.
- Alarms: Configure the Alarm (SNMP Trap) Groups, the Alarm Host Table, and the Syslog features.
- Bridge: Configure the Spanning Tree Protocol, Storm Threshold protection, Intra BSS traffic, and Packet Forwarding.
- Security: Configure security features such as MAC Access Control, WPA, WEP Encryption, and 802.1x. Configure Rogue Access Point Detection (RAD) and define the Scan Interval.
- RADIUS: Configure RADIUS features such as RADIUS Access Control and Accounting.
- VLAN/SSID: Configure VLAN IDs and SSIDs.

Configuring the AP Using the HTTP/HTTPS Interface

Follow these steps to configure an Access Point's operating settings using the HTTP/HTTPS interface:

1. Open a Web browser on a network computer.

NOTE

The HTTP interface supports the following Web browser:

- Microsoft Internet Explorer 6 with Service Pack 1 or later
- Netscape 6.1 or later

2. If necessary, disable the Internet proxy settings. For Internet Explorer users, follow these steps:
   - Select **Tools > Internet Options...**.
   - Click the **Connections** tab.
   - Click **LAN Settings...**.
   - If necessary, remove the check mark from the **Use a proxy server** box.
   - Click **OK** twice to save your changes and return to Internet Explorer.
3. Enter the Access Point's IP address in the browser's **Address** field and press **Enter**.
   - Result: The ***Enter Network Password*** screen appears.
4. Enter the HTTP password in the **Password** field and click **OK**. Leave the **User Name** field blank. (By default, the HTTP password is "public").
   - Result: The ***System Status*** screen appears.

Figure 4-1 Enter Network Password Screen

5. Click the **Configure** button located on the left-hand side of the screen.

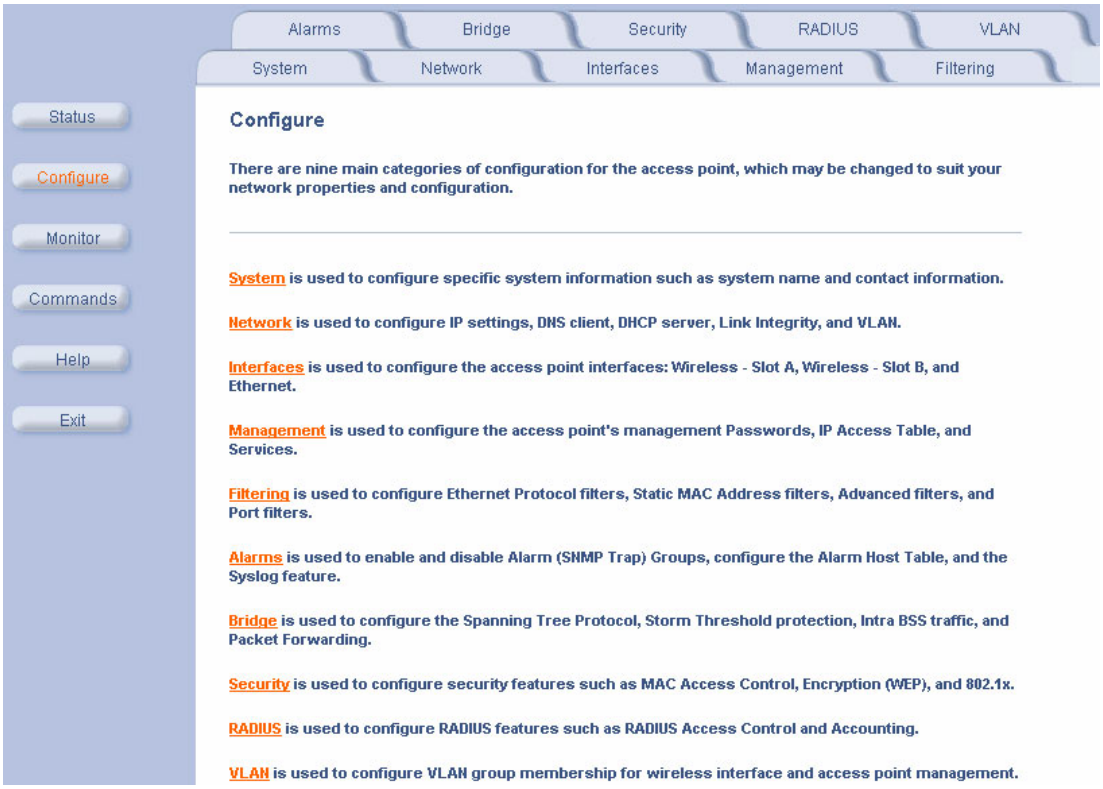


Figure 4-2 Configure Main Screen

6. Click the tab that corresponds to the parameter you want to configure. For example, click **Network** to configure the Access Point's TCP/IP settings. The parameters contained in each of the configuration categories are described later in this chapter.
7. Configure the Access Point's parameters as necessary. After changing a configuration value, click **OK** to save the change.
8. Reboot the Access Point for all of the changes to take effect.

System

You can configure and view the following parameters within the ***System Configuration*** screen:

- **Name:** The name assigned to the AP. Refer to the Dynamic DNS Support and Access Point System Naming Convention sections for rules on naming the AP.
- **Location:** The location where the AP is installed.
- **Contact Name:** The name of the person responsible for the AP.
- **Contact Email:** The email address of the person responsible for the AP.
- **Contact Phone:** The telephone number of the person responsible for the AP.
- **Object ID:** This is a read-only field that displays the Access Point's MIB definition; this information is useful if you are managing the AP using SNMP.
- **Ethernet MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's Ethernet interface. The MAC address is assigned at the factory.
- **Descriptor:** This is a read-only field that reports the Access Point's name, serial number, current image software version, and current bootloader software version.
- **Up Time:** This is a read-only field that displays how long the Access Point has been running since its last reboot.

Dynamic DNS Support

DNS is a distributed database mapping the user readable names and IP addresses (and more) of every registered system on the Internet. Dynamic DNS is a lightweight mechanism which allows for modification of the DNS data of host systems whose IP addresses change dynamically. Dynamic DNS is usually used in conjunction with DHCP for assigning meaningful names to host systems whose IP addresses change dynamically.

Access Points provide DDNS support by adding the host name (option 12) in DHCP Client messages, which is used by the DHCP server to dynamically update the DNS server.

Access Point System Naming Convention

The Access Point's system name is used as its host name. In order to prevent Access Points with default configurations from registering similar host names in DNS, the default system name of the Access Point is uniquely generated. Access Points generate unique system names by appending the last 3 bytes of the Access Point's MAC address to the default system name.

The system name must be compliant with the encoding rules for host name as per DNS RFC 1123. The DNS host name encoding rules are:

- Characters have to alphanumeric or hyphen.
- The name cannot start or end with a hyphen.
- The name cannot start with a digit.
- The number of characters has to be 63 or less. (Currently the system name length is limited to 32 bytes).

Image upgrades could cause the system to boot with an older system name format that is not DNS compliant. To prevent problems with dynamic DNS after an image upgrade, the system name will automatically be converted to a DNS compliant system name.

The rules of conversion of older system names are:

- If the length is greater than 63 then the string is truncated. (This will not happen since the system name is anyway limited to 32 bytes)
- All invalid characters at the beginning or end of the string are replaced with the character 'X'.
- All other invalid characters are replaced with hyphens.

Network

The Network category contains three sub-categories.

- IP Configuration
- DHCP Server
- Link Integrity

IP Configuration

You can configure and view the following parameters within the ***IP Configuration*** screen:

NOTE

You must reboot the Access Point in order for any changes to the Basic IP or DNS Client parameters take effect.

Basic IP Parameters

- **IP Address Assignment Type:** Set this parameter to **Dynamic** to configure the Access Point as a Dynamic Host Configuration Protocol (DHCP) client; the Access Point will obtain IP settings from a network DHCP server automatically during boot-up. If you do not have a DHCP server or if you want to manually configure the Access Point's IP settings, set this parameter to **Static**.
- **IP Address:** The Access Point's IP address. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current IP address. The Access Point will default to 10.0.0.1 if it cannot obtain an address from a DHCP server.
- **Subnet Mask:** The Access Point's subnet mask. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the unit's current subnet mask. The subnet mask will default to 255.0.0.0 if the unit cannot obtain one from a DHCP server.
- **Gateway IP Address:** The IP address of the Access Point's gateway. When IP Address Assignment Type is set to Dynamic, this field is read-only and reports the IP address of the unit's gateway. The gateway IP address will default to 10.0.0.2 if the unit cannot obtain an address from a DHCP server.

DNS Client

If you prefer to use host names to identify network servers rather than IP addresses, you can configure the AP to act as a Domain Name Service (DNS) client. When this feature is enabled, the Access Point contacts the network's DNS server to translate a host name to the appropriate network IP address. You can use this DNS Client functionality to identify RADIUS servers by host name. See RADIUS for details.

- **Enable DNS Client:** Place a check mark in the box provided to enable DNS client functionality. Note that this option must be enabled before you can configure the other DNS Client parameters.
- **DNS Primary Server IP Address:** The IP address of the network's primary DNS server.
- **DNS Secondary Server IP Address:** The IP address of a second DNS server on the network. The Access Point will attempt to contact the secondary server if the primary server is unavailable.
- **DNS Client Default Domain Name:** The default domain name for the Access Point's network (for example, "proxim.com"). Contact your network administrator if you need assistance setting this parameter.

Advanced

- **Default TTL (Time to Live):** Time to Live (TTL) is a field in an IP packet that specifies how long in seconds the packet can remain active on the network. The Access Point uses the default TTL for packets it generates for which the transport layer protocol does not specify a TTL value. This parameter supports a range from 0 to 65535. By default, TTL is 64.

DHCP Server

If your network does not have a DHCP Server, you can configure the AP as a DHCP server to assign dynamic IP addresses to Ethernet nodes and wireless clients.

CAUTION

Make sure there are no other DHCP servers on the network and do not enable the DHCP server without checking with your network administrator first, as it could bring down the whole network. Also, the AP must be configured with a static IP address before enabling this feature.

When the DHCP Server functionality is enabled, you can create one or more IP address pools from which to assign addresses to network devices.

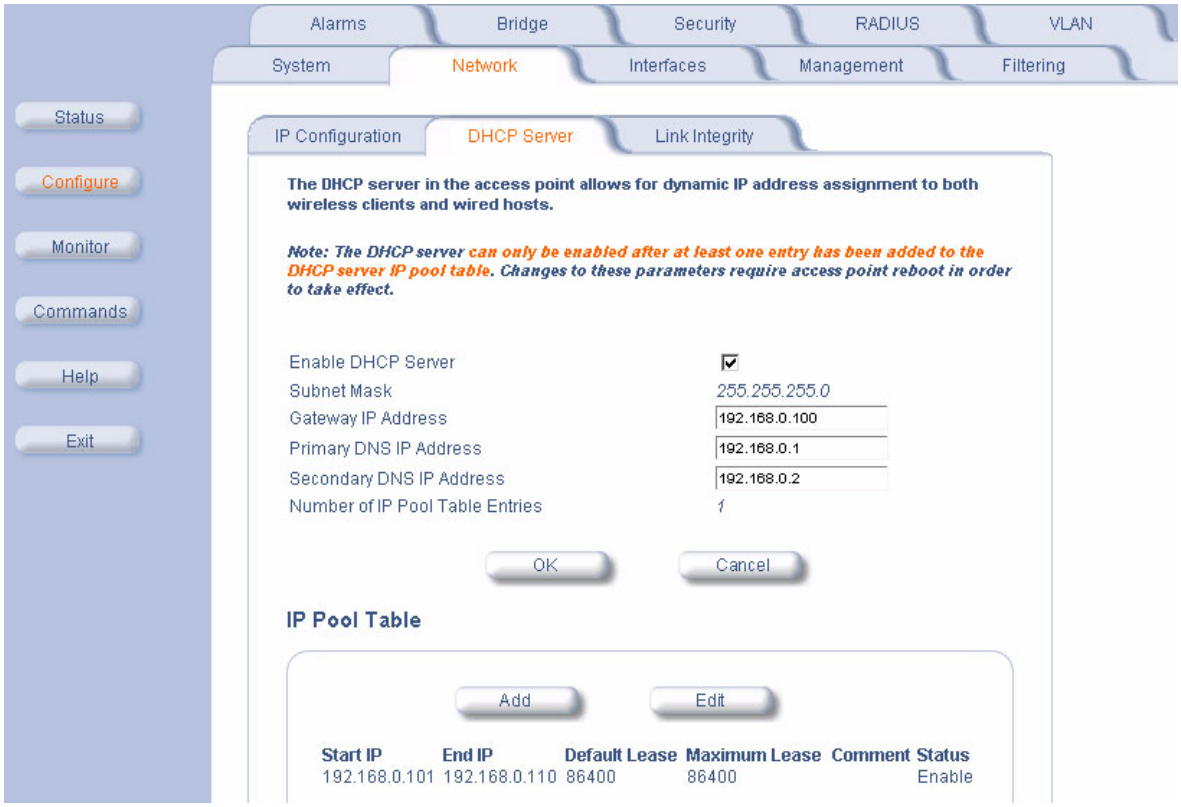


Figure 4-3 DHCP Server Configuration Screen

You can configure and view the following parameters within the ***DHCP Server Configuration*** screen:

- **Enable DHCP Server:** Place a check mark in the box provided to enable DHCP Server functionality.

NOTE

You cannot enable the DHCP Server functionality unless there is at least one IP Pool Table Entry configured.

- **Subnet Mask:** This field is read-only and reports the Access Point's current subnet mask. DHCP clients that receive dynamic addresses from the AP will be assigned this same subnet mask.
- **Gateway IP Address:** The AP will assign the specified address to its DHCP clients.
- **Primary DNS IP Address:** The AP will assign the specified address to its DHCP clients.
- **Secondary DNS IP Address:** The AP will assign the specified address to its DHCP clients.
- **Number of IP Pool Table Entries:** This is a read-only field that reports the number of IP address pools currently configured.
- **IP Pool Table Entry:** This entry specifies a range of IP addresses that the AP can assign to its wireless clients. Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  - **Start IP Address**
  - **End IP Address**
  - **Default Lease Time (optional):** The default time value for clients to retain the assigned IP address. DHCP automatically renews IP Addresses without client notification. This parameter supports a range between 0 and 86400 seconds. The default is 86400 seconds.
  - **Maximum Lease Time (optional):** The maximum time value for clients to retain the assigned IP address. DHCP automatically renews IP Addresses without client notification. This parameter supports a range between 0 and 86400 seconds. The default is 86400 seconds.
  - **Comment (optional)**
  - **Status:** IP Pools are enabled upon entry in the table. You can also disable or delete entries by changing this field's value.

NOTE

You must reboot the Access Point before changes to any of these DHCP server parameters take effect.

Link Integrity

The Link Integrity feature checks the link between the AP and the nodes on the Ethernet backbone. These nodes are listed by IP address in the Link Integrity IP Address Table. The AP periodically pings the nodes listed within the table. If the AP loses network connectivity (that is, the ping attempts fail), the AP disables its wireless interface until the connection is restored. This forces the unit's wireless clients to switch to another Access Point that still has a network connection. Note that this feature does not affect WDS links (if applicable).

You can configure and view the following parameters within the ***Link Integrity Configuration*** screen:

- **Enable Link Integrity:** Place a check mark in the box provided to enable Link Integrity.
- **Poll Interval (milliseconds):** The interval between link integrity checks. Range is 500 - 15000 ms in increments of 500 ms; default is 500 ms.
- **Poll Retransmissions:** The number of times a poll should be retransmitted before the link is considered down. Range is 0 to 255; default is 5.
- **Target IP Address Entry:** This entry specifies the IP address of a host on the network that the AP will periodically poll to confirm connectivity. The table can hold up to five entries. By default, all five entries are set to 0.0.0.0. Click **Edit** to update one or more entries. Each entry contains the following field:
  - **Target IP Address**
  - **Comment (optional)**
  - **Status:** Set this field to **Enable** to specify that the Access Point should poll this device. You can also disable an entry by changing this field's value to **Disable**.

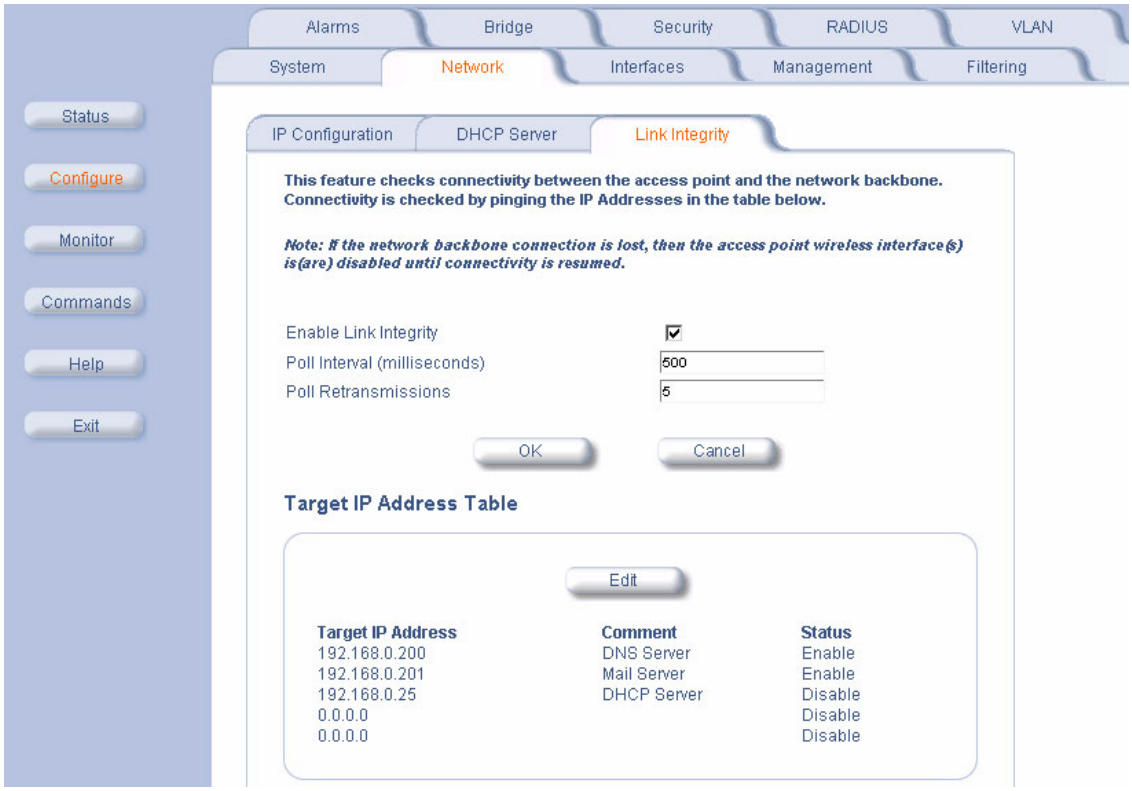


Figure 4-4 Link Integrity Configuration Screen

Interfaces

From the **Interfaces** tab, you configure the Access Point's operational mode, power control settings, wireless interface settings and Ethernet settings. You may also configure a Wireless Distribution System for AP-to-AP communications.

For the wireless interface configuration, refer to the wireless parameters below that correspond to your radio type.

- Operational Mode
- Wireless (802.11a)
- Wireless (802.11b)
- Wireless (802.11b/g)
- Wireless Distribution System (WDS)
- Ethernet

Operational Mode

You can configure and view the following parameters within the ***Operational Mode*** screen.

- **Operational Mode**: the mode of communication between the wireless clients and the Access Point:
  - 802.11b only
  - 802.11g only
  - 802.11bg
  - 802.11a (default)
  - 802.11g-wifi (Although this is a valid option, the .11g AP Card is not Wi-Fi certified.)

TX Power Control

The TX Power Control feature lets the user configure the transmit power level of the card in the AP at one of four levels:

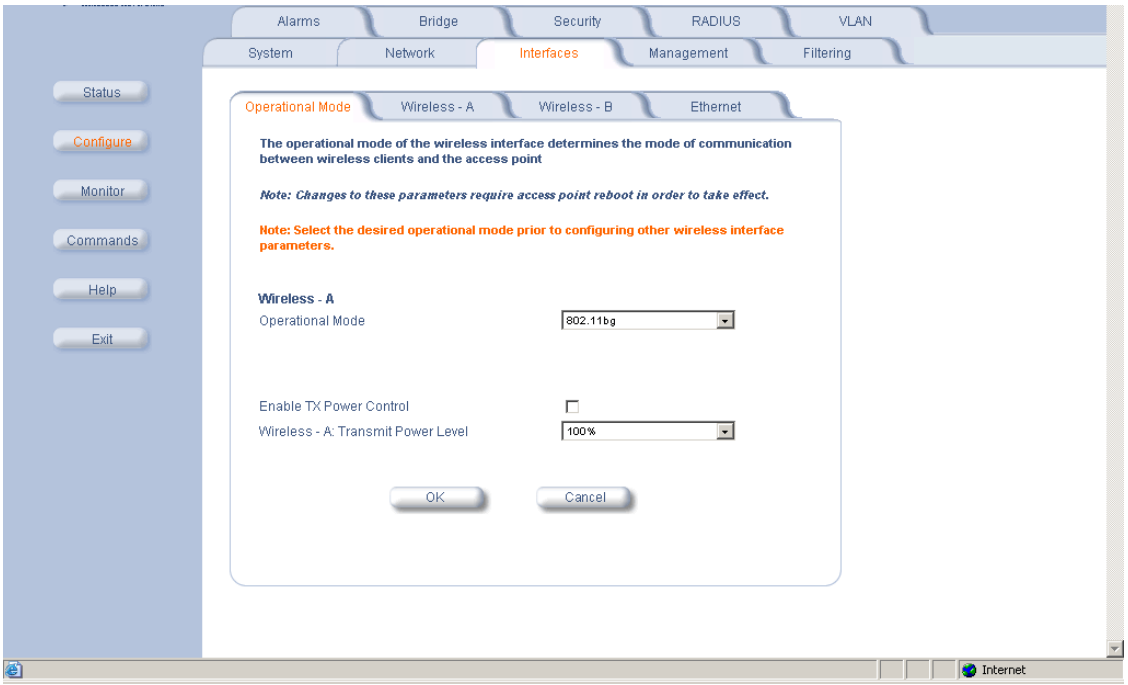
- 100% of the maximum transmit power level of the card
- 50%
- 25%
- 12.5%

NOTE

TX Power Control is only supported on the HP ProCurve Wireless 802.11g AP Card 170wl.

Configuring TX Power Control

1. Click **Configure > Interfaces > Operational Mode**.
2. Select **Enable Transmit Power Control**.
3. Select the transmit power level for interface A from the Wireless-A: Transmit Power Level drop-down menu.Select the transmit power level for interface B from the Wireless-B: Transmit Power Level drop-down menu.
4. Click **OK**.



Wireless (802.11a)

You can configure and view the following parameters within the ***Wireless Interface Configuration*** screen for an 802.11a AP:

NOTE

You must reboot the Access Point before any changes to these parameters take effect.

- **Physical Interface Type:** For an 802.11a AP, this field reports: “802.11a (OFDM 5 GHz).” OFDM stands for Orthogonal Frequency Division Multiplexing; this is the name for the radio technology used by 802.11a devices.
- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point’s wireless interface. The MAC address is assigned at the factory.
- **Regulatory Domain:** Reports the regulatory domain for which the AP is certified. Not all features or channels are available in all countries. The available regulatory domains include:
  - FCC - U.S./Canada, Mexico, and Australia
  - ETSI - Europe and the United Kingdom
  - MKK: Japan
  - SG: Singapore
  - ASIA: China, Hong Kong, and South Korea
  - TW: Taiwan
- **Network Name (SSID):** Enter a Network Name (between 2 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well.
- **Auto Channel Select:** The AP scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled. See 802.11a Channel Frequencies for a list of Channels.

NOTE

You cannot disable Auto Channel Select for 802.11a products in Europe (see Dynamic Frequency Selection (DFS) for details).

- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point’s current operating Channel. When Auto Channel Select is disabled, you can specify the Access Point’s channel. If you decide to manually set the unit’s Channel, ensure that nearby devices do not use the same frequency. Available Channels vary based on regulatory domain. See 802.11a Channel Frequencies. Note that you cannot manually set the channel for 802.11a products in Europe (see Dynamic Frequency Selection (DFS) for details).
- **Transmit Rate:** Use the drop-down menu to select a specific transmit rate for the AP. Choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, and Auto Fallback. Auto Fallback is the default setting; it allows the AP unit to select the best transmit rate based on the cell size.
- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) is used with clients that have power management enabled. DTIM should be left at 1, the default value, if any clients have power management enabled. This parameter supports a range between 1 and 255.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See RTS/CTS Medium Reservation for more information.
- **Closed System:** Check this box to allow only clients configured with the Access Point’s specific Network Name to associate with the Access Point. When enabled, a client configured with the Network Name “ANY” cannot connect to the AP. This option is disabled by default.

Dynamic Frequency Selection (DFS)

802.11a APs sold in Europe use a technique called Dynamic Frequency Selection (DFS) to automatically select an operating channel. During boot-up, the AP scans the available frequency and selects a channel that is free of interference. If the AP subsequently detects interference on its channel, it automatically reboots and selects another channel that is free of interference.

DFS only applies to 802.11a APs used in Europe (i.e., units whose regulatory domain is set to ETSI). The European Telecommunications Standard Institute (ETSI) requires that 802.11a devices use DFS to prevent interference with radar systems and other devices that already occupy the 5 GHz band.

If you are using an 802.11a AP in Europe, keep in mind the following:

- DFS is not a configurable parameter. It is always enabled and cannot be disabled.
- You cannot manually select the device's operating channel; you must let DFS select the channel.
- You cannot configure the **Auto Channel Select** option. Within the HTTP interface, this option always appears enabled.

RTS/CTS Medium Reservation

The 802.11 standard supports optional RTS/CTS communication based on packet size. Without RTS/CTS, a sending radio listens to see if another radio is already using the medium before transmitting a data packet. If the medium is free, the sending radio transmits its packet. However, there is no guarantee that another radio is not transmitting a packet at the same time, causing a collision. This typically occurs when there are hidden nodes (clients that can communicate with the Access Point but are out of range of each other) in very large cells.

When RTS/CTS occurs, the sending radio first transmits a Request to Send (RTS) packet to confirm that the medium is clear. When the receiving radio successfully receives the RTS packet, it transmits back a Clear to Send (CTS) packet to the sending radio. When the sending radio receives the CTS packet, it sends the data packet to the receiving radio. The RTS and CTS packets contain a reservation time to notify other radios (including hidden nodes) that the medium is in use for a specified period. This helps to minimize collisions. While RTS/CTS adds overhead to the radio network, it is particularly useful for large packets that take longer to resend after a collision occurs.

RTS/CTS Medium Reservation is an advanced parameter and supports a range between 0 and 2347 bytes. When set to 2347 (the default setting), the RTS/CTS mechanism is disabled. When set to 0, the RTS/CTS mechanism is used for all packets. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. You should not need to enable this parameter for most networks unless you suspect that the wireless cell contains hidden nodes.

Wireless (802.11b)

You can configure and view the following parameters within the ***Wireless Interface Configuration*** screen for an 802.11b AP:

NOTE

You must reboot the Access Point before any changes to these parameters take effect.

- **Physical Interface Type:** For 802.11b AP, this field reports: "802.11b (DSSS 2.4 GHz)." DSSS stands for Direct Sequence Spread Spectrum; this is the name for the radio technology used by 802.11b devices.
- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's wireless interface. The MAC address is assigned at the factory.
- **Regulatory Domain:** Reports the regulatory domain for which the AP is certified. Not all features or channels are available in all countries. The available regulatory domains include:
  - FCC - U.S./Canada, Mexico, and Australia
  - ETSI - Most of Europe, including the United Kingdom and some Eastern block countries
  - MKK - Japan
  - IL - Israel
- **Network Name (SSID):** Enter a Network Name (between 2 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well.
- **Auto Channel Select:** The AP scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled; see 802.11b Channel Frequencies for a list of Channels. However, if you are setting up a Wireless Distribution System (WDS), it must be disabled. See Wireless Distribution System (WDS) for more information.
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's operating channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency (unless you are setting up a WDS). Available Channels vary based on regulatory domain. See 802.11b Channel Frequencies.

- **Distance Between APs:** Set to **Large**, **Medium**, **Small**, **Microcell**, or **Minicell** depending on the site survey for your system. By default, this parameter is set to **Large**. The distance value is related to the **Multicast Rate** (described next). In general, a larger distance between APs means that your clients operate a slower data rates (on average). See Distance Between APs for more information.
- **Multicast Rate:** Sets the rate at which Multicast messages are sent. This value is related to the Distance Between APs parameter (described previously). The table below displays the possible Multicast Rates based on the Distance between APs setting. By default, this parameter is set to 2 Mbits/sec. See Multicast Rate for more information.

Distance between APs	Multicast Rate
Large	1 and 2 Mbits/sec
Medium	1, 2, and 5.5 Mbits/sec
Small	1, 2, 5.5 and 11 Mbits/sec
Minicell	1, 2, 5.5 and 11 Mbits/sec
Microcell	1, 2, 5.5 and 11 Mbits/sec

- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) is used with clients that have power management enabled. DTIM should be left at 1, the default value, if any clients have power management enabled. This parameter supports a range between 1 and 255.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See RTS/CTS Medium Reservation for more information.
- **Interference Robustness:** Enable this option if other electrical devices in the 2.4 GHz frequency band (such as a microwave oven or a cordless phone) may be interfering with the wireless signal. The AP will automatically fragment large packets into multiple smaller packets when interference is detected to increase the likelihood that the messages will be received in the presence of interference. The receiving radio reassembles the original packet once all fragments have been received. This option is disabled by default.
- **Closed System:** Check this box to allow only clients configured with the Access Point's specific Network Name to associate with the Access Point. When enabled, a client configured with the Network Name "ANY" cannot connect to the AP. This option is disabled by default.
- **Load Balancing:** Enable this option so clients can evaluate which Access Point to associate with, based on current AP loads. This feature is enabled by default; it helps distribute the wireless load between APs. This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150wl. In addition, this feature will only give information for ORiNOCO/Agere/Lucent based clients.
- **Medium Density Distribution:** When enabled, the Access Point automatically notifies wireless clients of its **Distance Between APs**, **Interference Robustness**, and **RTS/CTS Medium Reservation** settings. This feature is enabled by default and allows clients to automatically adopt the values used by its current Access Point (even if these values differ from the client's default values or from the values supported by other Access Points). This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150wl. In addition, this feature will only give information for ORiNOCO/Agere/Lucent based clients.

Distance Between APs

Distance Between APs defines how far apart (physically) your AP devices are located, which in turn determines the size of your cell. Cells of different sizes have different capacities and, therefore, suit different applications. For instance, a typical office has many stations that require high bandwidth for complex, high-speed data processing. In contrast, a typical warehouse has a few forklifts requiring low bandwidth for simple transactions. This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150wl.

Cell capacities are compared in the following table, which shows that small cells suit most offices and large cells suit most warehouses:

Small Cell	Large Cell
Physically accommodates few stations	Physically accommodates many stations
High cell bandwidth per station	Lower cell bandwidth per station
High transmit rate	Lower transmit rate

Coverage

The number of Access Points in a set area determines the network coverage for that area. A large number of Access Points covering a small area is a high-density cell. A few Access Points, or even a single unit, covering the same small area would result in a low-density cell, even though in both cases the actual area did not change — only the number of Access Points covering the area changed.

In a typical office, a high density area consists of a number of Access Points installed every 20 feet and each Access Point generates a small radio cell with a diameter of about 10 feet. In contrast, a typical warehouse might have a low density area consisting of large cells (with a diameter of about 90 feet) and Access Points installed every 200 feet.

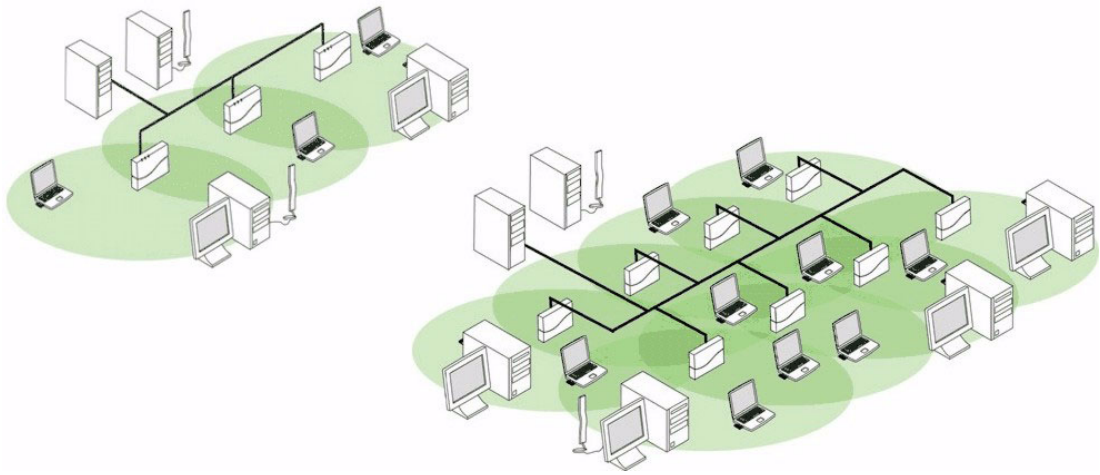


Figure 4-5 Low Density vs. Ultra High Density Network

The Distance Between Cells parameter supports five values: Large, Medium, Small, Minicell, and Microcell.

CAUTION

The distance between APs should not be approximated. It is calculated by means of a manual Site Survey, in which an AP is set up and clients are tested throughout the area to determine signal strength and coverage, and local limits such as physical interference are investigated. From these measurements the appropriate cell size and density is determined, and the optimum distance between APs is calculated to suit your particular business requirements. Contact your reseller for information on how to conduct a Site Survey.

Multicast Rate

The multicast rate determines the rate at which broadcast and multicast packets are transmitted by the Access Point to the wireless network. Stations that are closer to the Access Point can receive multicast packets at a faster data rate than stations that are farther away from the AP. Therefore, you should set the Multicast Rate based on the size of the Access Point's cell. For example, if the Access Point's cell is very small (that is, Distance Between APs is set to Microcell), you can expect that all stations should be able to successfully receive multicast packets at 11 MBits/sec so you can set Multicast Rate to 11 Mbits/sec. However, if the Access Point's cell is large, you need to accommodate stations that may not be able to receive multicast packets at the higher rates; in this case, you should set Multicast Rate to 1 or 2 Mbits/sec.

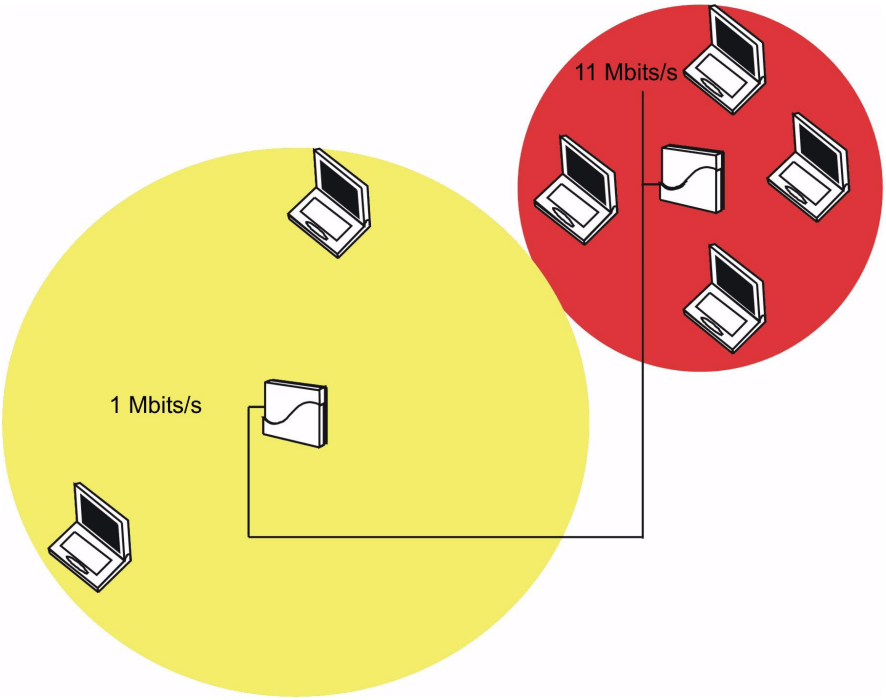


Figure 4-6 1 Mbits/s and 11 Mbits/s Multicast Rates

NOTE

There is an inter-dependent relationship between the Distance between APs and the Multicast Rate. In general, larger systems operate at a lower average transmit rate. The variation between Multicast Rate and Distance Between APs is presented in the following table:

	1.0 Mbit/s	2.0 Mbits/s	5.5 Mbits/s	11 Mbits/s
Large	yes	yes		
Medium	yes	yes	yes	
Small	yes	yes	yes	yes
Minicell	yes	yes	yes	yes
Microcell	yes	yes	yes	yes

The Distance Between APs **must be set before** the Multicast Rate, because when you select the Distance Between APs, the appropriate range of Multicast values automatically populates the drop-down menu. This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150wl.

Wireless (802.11b/g)

You can configure the following radio parameters for an 802.11b/g AP:

NOTE

You must reboot the Access Point before any changes to these parameters take effect.

- **Operational Mode:** An 802.11b/g wireless interface can be configured to operate in the following modes:
  - **802.11b mode only:** The radio uses the 802.11b standard only.
  - **802.11g mode only:** The radio is optimized to communicate with 802.11g devices. This setting will provide the best results if this radio interface will only communicate with 802.11g devices.
  - **802.11b/g mode:** This is the default mode. Use this mode if you want to support a mix of 802.11b and 802.11g devices.
  - **802.11g-wifi:** This mode was developed for Wi-Fi compliance testing purposes. It is similar to 802.11g only mode. (Although this is a valid option, the .11g AP Card is not Wi-Fi certified.)

  In general, you should use either 802.11g only mode (if you want to support 802.11g devices only) or 802.11b/g mode to support a mix of 802.11b and 802.11g devices.
- **Physical Interface Type:** Depending on the Operational Mode, this field reports:
  - For 802.11b mode only: "802.11b (CCK/DSSS 2.4 GHz)"
  - For 802.11g and 802.11g-wifi modes: "802.11g (OFDM/DSSS 2.4 GHz)"
  - For 802.11b/g mode: "802.11b/g (ERP-CCK/DSSS/OFDM 2.4 GHz)"

  OFDM stands for Orthogonal Frequency Division Multiplexing; this is the name for the radio technology used by 802.11a devices. DSSS stands for Direct Sequence Spread Spectrum; this is the name for the radio technology used by 802.11b devices.
- **MAC Address:** This is a read-only field that displays the unique MAC (Media Access Control) address for the Access Point's wireless interface. The MAC address is assigned at the factory.
- **Regulatory Domain:** Reports the regulatory domain for which the AP is certified. Not all features or channels are available in all countries. The available regulatory domains include:
  - FCC - U.S./Canada, Mexico, and Australia
  - ETSI - Europe, including the United Kingdom, China, and South Korea
  - MKK - Japan
  - IL - Israel
- **Network Name (SSID):** Enter a Network Name (between 2 and 31 characters long) for the wireless network. You must configure each wireless client to use this name as well.
- **Auto Channel Select:** The AP scans the area for other Access Points and selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. By default this feature is enabled; see 802.11g Channel Frequencies for a list of Channels.
- **Frequency Channel:** When Auto Channel Select is enabled, this field is read-only and displays the Access Point's current operating channel. When Auto Channel Select is disabled, you can specify the Access Point's operating channel. If you decide to manually set the unit's channel, ensure that nearby devices do not use the same frequency (unless you are setting up a WDS). Available Channels vary based on regulatory domain. See 802.11g Channel Frequencies.
- **Transmit Rate:** Select a specific transmit rate for the AP. The values available depend on the Operational Mode. Auto Fallback is the default setting; it allows the AP to select the best transmit rate based on the cell size.
  - For 802.11b only -- Auto Fallback, 1, 2, 5.5, 11 Mbits/sec
  - For 802.11g only -- Auto Fallback, 6, 9, 12, 18, 24, 36, 48, 54 Mbits/sec
  - For 802.11b/g and 802.11g-wifi -- Auto Fallback, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbits/sec
- **DTIM Period:** The Deferred Traffic Indicator Map (DTIM) is used with clients that have power management enabled. DTIM should be left at 1, the default value, if any clients have power management enabled. This parameter supports a range between 1 and 255.
- **RTS/CTS Medium Reservation:** This parameter affects message flow control and should not be changed under normal circumstances. Range is 0 to 2347. When set to a value between 0 and 2347, the Access Point uses the RTS/CTS mechanism for packets that are the specified size or greater. When set to 2347 (the default setting), RTS/CTS is disabled. See RTS/CTS Medium Reservation for more information.

- **Closed System:** Check this box to allow only clients configured with the Access Point's specific Network Name to associate with the Access Point. When enabled, a client configured with the Network Name "ANY" cannot connect to the AP. This option is disabled by default.

Wireless Distribution System (WDS)

A Wireless Distribution System (WDS) creates a link between two 802.11a, 802.11b, or 802.11b/g APs over their radio interfaces. This link relays traffic from one AP that does not have Ethernet connectivity to a second AP that has Ethernet connectivity. WDS allows you to configure up to six (6) point-to-point links between Access Points.

In the WDS Example below, AP 1 and AP 2 communicate over a WDS link (represented by the blue line). This link provides Client 1 with access to network resources even though AP 1 is not directly connected to the Ethernet network. Packets destined for or sent by the client are relayed between the Access Points over the WDS link. If 802.1q VLAN tagged packets travel through a WDS link, tags are maintained for all traffic coming from either the wired or wireless side of the network.

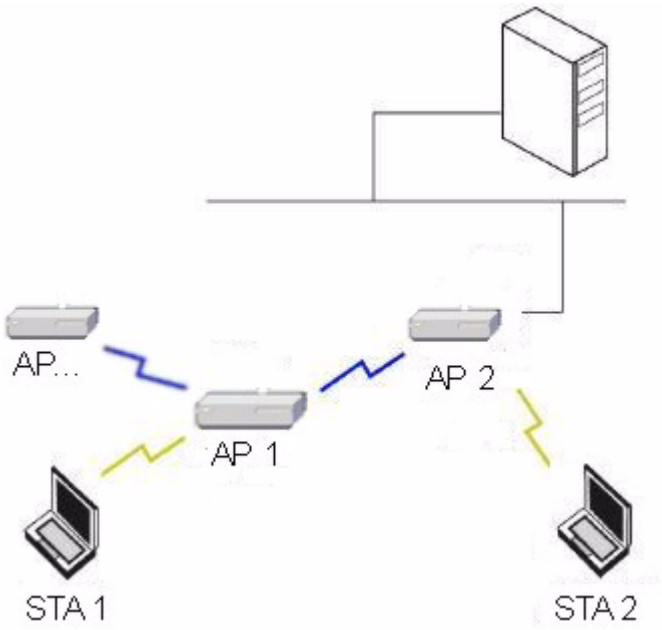


Figure 4-7 WDS Example

Bridging WDS

Each WDS link is mapped to a logical WDS port on the AP. WDS ports behave like Ethernet ports rather than like standard wireless interfaces: on a BSS port, an Access Point learns by association and from frames; on a WDS or Ethernet port, an Access Point learns from frames only. When setting up a WDS, keep in mind the following:

- The WDS link shares the communication bandwidth with the clients. Therefore, while the maximum data rate for the Access Point's cell is still 11 Mb for 802.1b and 54Mb for 802.11a and 802.11g, client throughput will decrease when the WDS link is active.
- If there is no partner MAC address configured in the WDS table, the WDS port remains disabled.
- Each WDS port on a single AP should have a unique partner MAC address. Do not enter the same MAC address twice in an AP's WDS port list.
- Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.
- Each Access Point that is a member of the WDS must have the same network domain.
- Each Access Point that is a member of the WDS must have the same WEP Encryption settings. WDS does not use 802.1x. Therefore, if you want to encrypt the WDS link, you must configure each Access Point to use WEP encryption (either WEP encryption only or Mixed Mode), and each Access Point must have the same Encryption Key(s). See Security.

- If your network does not support spanning tree, be careful to avoid creating network loops between APs. For example, creating a WDS link between two Access Points connected to the same Ethernet network will create a network loop (if spanning tree is disabled). For more information, refer to the Spanning Tree section.

WDS Setup Procedure

NOTE

You must disable Auto Channel Select to create a WDS. Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.

To setup a wireless backbone follow the steps below for each AP that you wish to include in the Wireless Distribution System.

1. Confirm that Auto Channel Select is disabled.
2. Write down the MAC Address of the radio that you wish to include in the Wireless Distribution System.
3. Open the ***Wireless Interface Configuration*** screen.
4. Scroll down to the **Wireless Distribution System** heading.
5. Click the **Edit** button to update the Wireless Distribution System (WDS) Table.
6. Enter the MAC Address that you wrote down in Step 2 in one of the **Partner MAC Address** field of the Wireless Distribution Setup window.
7. Set the **Status** of the device to **Enable**.
8. Click **OK**.
9. Reboot the AP.

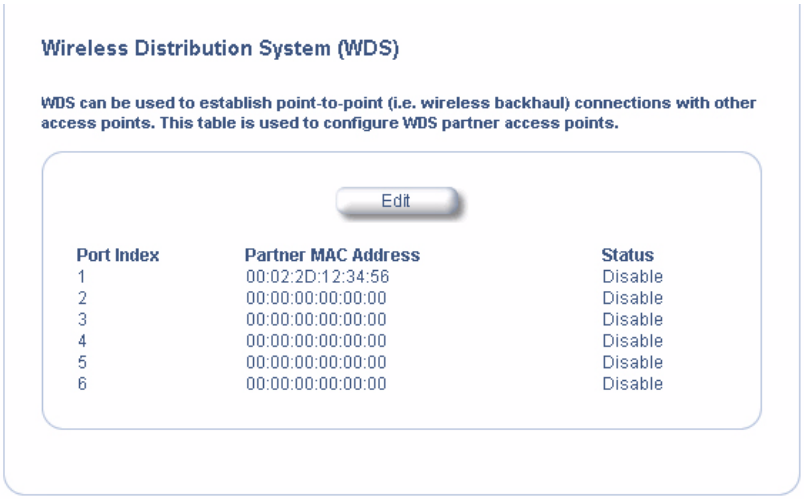


Figure 4-8 WDS Configuration

NOTE

To set up a Wireless Distribution System (WDS) with 802.1x, set each Access Point's 802.1x Security Mode to Mixed and assign each unit in the WDS the same Encryption Key 1. See Security.

Ethernet

Select the desired speed and transmission mode from the drop-down menu. Half-duplex means that only one side can transmit at a time and full-duplex allows both sides to transmit. When set to auto-duplex, the AP negotiates with its switch or hub to automatically select the highest throughput option supported by both sides.

For best results, HP recommends that you configure the Ethernet setting to match the speed and transmission mode of the device the Access Point is connected to (such as a hub or switch). If in doubt, leave this setting at its default, **auto-speed-auto-duplex**. Choose between:

- 10 Mbit/s - half duplex, full duplex, or auto duplex
- 100 Mbit/s - half duplex or full duplex
- auto speed - half duplex or auto duplex

Management

The Management category contains three sub-categories.

- Passwords
- IP Access Table
- Services

Passwords

You can configure the following passwords:

- **SNMP Read Password:** The password for read access to the AP using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is “public”.
- **SNMP Read/Write Password:** The password for read and write access to the AP using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is “public”.
- **SNMPv3 Authentication Password:** The password used when sending authenticated SNMPv3 messages. Enter a password in both the **Password** field and the **Confirm** field. The default password is “public”. Password length is recommended to be at least 8 characters. Secure Management (Services tab) must be enabled to configure SNMPv3.
- **SNMPv3 Privacy Password:** The password used when sending encrypted SNMPv3 data. Enter a password in both the **Password** field and the **Confirm** field. The default password is “public”. Password length is recommended to be at least 8 characters. Secure Management (Services tab) must be enabled to configure SNMPv3.
- **Telnet (CLI) Password:** The password for the CLI interface (by way of serial or Telnet). Enter a password in both the **Password** field and the **Confirm** field. The default password is “public”.
- **HTTP (Web) Password:** The password for the Web browser HTTP interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is “public”.

NOTE

For security purposes HP recommends changing ALL PASSWORDS from the default “public” immediately, to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the Reset to Factory Default Procedure.

IP Access Table

The Management IP Access table limits in-band management access to the IP addresses or range of IP addresses specified in the table. This feature applies to all management options (SNMP, HTTP, and Telnet). To configure this table, click **Add** and set the following parameters:

- **IP Address:** Enter the IP Address for the management station.
- **IP Mask:** Enter a mask that will act as a filter to limit access to a range of IP Addresses based on the IP Address you already entered.
  - The IP mask 255.255.255.255 would authorize the single station defined by the IP Address to configure the Access Point. The AP would ignore commands from any other IP address. In contrast, the IP mask 255.255.255.0 would allow any device that shares the first three octets of the IP address to configure the AP. For example, if you enter an IP address of 10.20.30.1 with a 255.255.255.0 subnet mask, any IP address between 10.20.30.1 and 10.20.30.254 will have access to the AP’s management interfaces.
- **Comment:** Enter an optional comment, such as the station name.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** pull-down menu.

Services

You can configure the following management services:

NOTE

You must reboot the Access Point if you change the HTTP Port or Telnet Port.

Secure Management

Secure Management allows the use of encrypted and authenticated communication protocols such as SNMPv3, and Secure Socket Link (SSL), to manage the Access Point.

- **Enable Secure Management:** Enables the further configuration of HTTPS Access, and SNMPv3. After enabling Secure Management, you can choose to configure HTTPS (SSL) access on the Services tab, and configure SNMPv3 passwords on the Passwords tab.

SNMP Settings

- **SNMP Interface Bitmask:** Configure the interface or interfaces (**Ethernet**, **Wireless**, **All Interfaces**) from which you will manage the AP by way of SNMP. You can also select **Disabled** to prevent a user from accessing the AP by way of SNMP.

HTTP Access

- **HTTP Interface Bitmap:** Configure the interface or interfaces (**Ethernet**, **Wireless**, **All Interfaces**) from which you will manage the AP by way of the Web interface. For example, to allow Web configuration by way of the Ethernet network only, set **HTTP Interface Bitmask** to **Ethernet**. You can also select **Disabled** to prevent a user from accessing the AP from the Web interface.
- **HTTP Port:** Configure the HTTP port from which you will manage the AP by way of the Web interface. By default, the HTTP port is 80.
- **Enable HTTP Setup Wizard:** The Setup Wizard appears automatically the first time you access the HTTP interface. If you exited out of the Setup Wizard and want to relaunch it, enable this option, click **OK**, and then close your browser or reboot the AP. The Setup Wizard will appear the next time you access the HTTP interface.

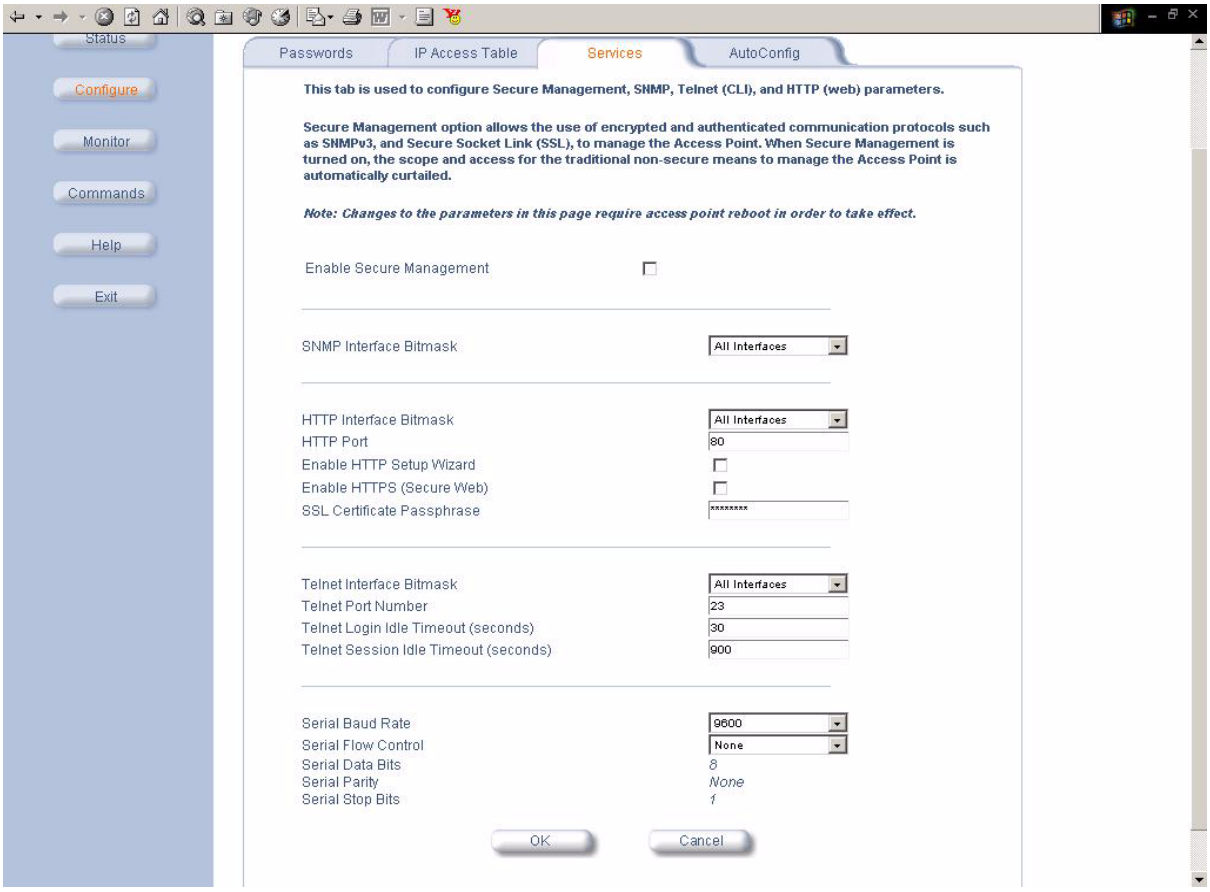


Figure 4-9 Management Services Configuration Screen

HTTPS Access (Secure Socket Layer)

The user can access the AP in a secure fashion using Secure Socket Layer (SSL) over port 443. The AP supports SSLv3 with a 128-bit encryption certificate maintained by the AP for secure communications between the AP and the HTTP client. All communications are encrypted using the server and the client-side certificate. The AP comes pre-installed with all required SSL files: default certificate and private key installed.

Configuring Secure Socket Layer (SSL)

After enabling SSL, the only configurable parameter is the SSL passphrase.

If you decide to upload a new certificate and private key (using TFTP or HTTP File Transfer), you need to change the SSL Certificate Passphrase for the new SSL files.

- **Enable HTTPS (Secure Web):** Check this box to enable SSL on the AP.

NOTE

You need to reboot the AP after enabling or disabling SSL for the changes to take effect.

- **SSL Certificate Passphrase:** Specifies the SSL Passphrase to use if Enable HTTPS has been checked. The user must change the SSL passphrase when uploading a new certificate/private key pair, which will have a corresponding passphrase.

Accessing the AP through the HTTPS interface

The user should use a SSL intelligent browser to access the AP through the HTTPS interface. After configuring SSL, access the AP using **https://** followed by the AP's management IP address.

Telnet Configuration Settings

- **Telnet Interface Bitmask:** Select the interface (**Ethernet**, **Wireless**, **All Interfaces**) from which you can manage the AP by way of telnet. This parameter can also be used to Disable telnet management.
- **Telnet Port:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select).
- **Login Idle Timeout (seconds):** Enter the number of seconds the system will wait for a login attempt. The AP terminates the session when it times out. The range is 1 to 300 seconds; the default is 30 seconds.
- **Session Idle Timeout (seconds):** Enter the number of seconds the system will wait during a session while there is no activity. The AP will terminate the session on timeout. The range is 1 to 36000 seconds; the default is 900 seconds.

Serial Configuration Settings

The serial port interface on the AP is enabled at all times. See Setting IP Address using Serial Port for information on how to access the CLI interface by way of the serial port. You can configure and view following parameters:

– **Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.

– **Flow Control:** Select either **None** (default) or **Xon/Xoff** (software controlled) data flow control.

NOTE

To avoid potential problems when communicating with the AP through the serial port, HP recommends that you leave the Flow Control setting at None (the default value).

- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

NOTE

The serial port bit configuration is commonly referred to as **8N1**.

Advanced Configuration

Automatic Configuration

The Automatic Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Automatic Configuration is disabled by default. The configuration process for Automatic Configuration varies depending on whether the AP is configured for dynamic or static IP.

When an AP is configured for dynamic IP, the Configuration filename and the TFTP server IP address are contained in the DHCP response when the AP gets its IP address dynamically from the DHCP server. When configured for static IP, these parameters are instead configured in the AP interface.

After setting up automatic configuration you must reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If Syslog is configured, a Syslog message will appear indicating the success or failure of the Automatic Configuration.

Set up Automatic Configuration for Static IP

Perform the following procedure to enable and set up Automatic Configuration when you have a static IP address for the TFTP server.

1. Click **Configure** > **Management** > **AutoConfig**.
   The Automatic Configuration Screen appears.
2. Check **Enable Auto Configuration**.
3. Enter the **Configuration Filename**.
4. Enter the IP address of the TFTP server in the **TFTP Server Address** field.

NOTE

The default filename is “config”. The default TFTP IP address is “10.0.0.2”.

5. Click **OK** to save the changes.
6. Reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If a Syslog server was configured, the following messages can be observed on the Syslog server:

- AutoConfig for Static IP
- TFTP server address and configuration filename
- AutoConfg Successful

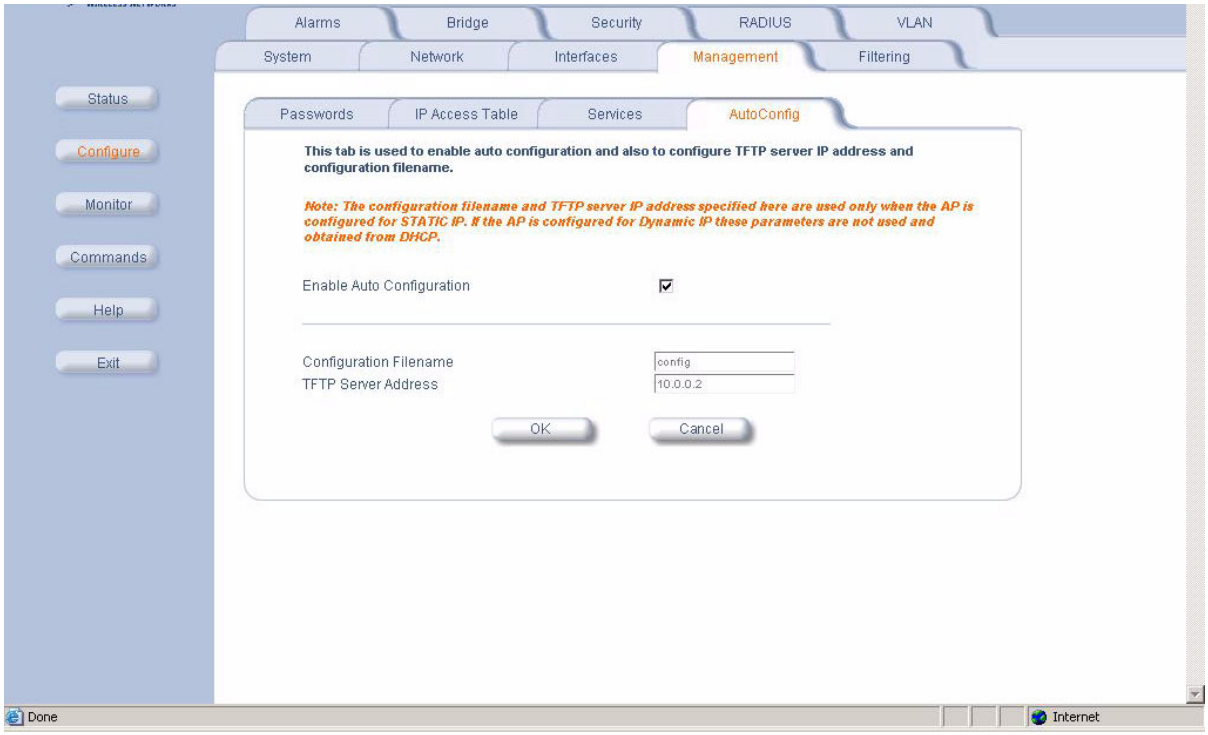


Figure 4-10 Automatic Configuration Screen

Set up Automatic Configuration for Dynamic IP

Perform the following procedure to enable and set up Automatic Configuration when you have a dynamic IP address for the TFTP server by way of DHCP.

The Configuration filename and the TFTP server IP address are contained in the DHCP response when the AP gets its IP address dynamically from the DHCP server. A Syslog server address is also contained in the DHCP response, allowing the AP to send Auto Configuration success and failure messages to a Syslog server.

NOTE

The configuration filename and TFTP server IP address are configured only when the AP is configured for Static IP. If the AP is configured for Dynamic IP these parameters are not used and obtained from DHCP.

1. Click **Configure** > **Management** > **AutoConfig**.
   The Automatic Configuration Screen appears.
2. Check **Enable Auto Configuration**.

When the AP is Configured with Dynamic IP, the DHCP server should be configured with the TFTP Server IP address ("Boot Server Host Name", option 66) and Configuration file ("Bootfile name", option 67) as follows:

3. **Select DHCP Server** > **DHCP Option** > **Scope**.
   The DHCP Options: Scope Screen appears.

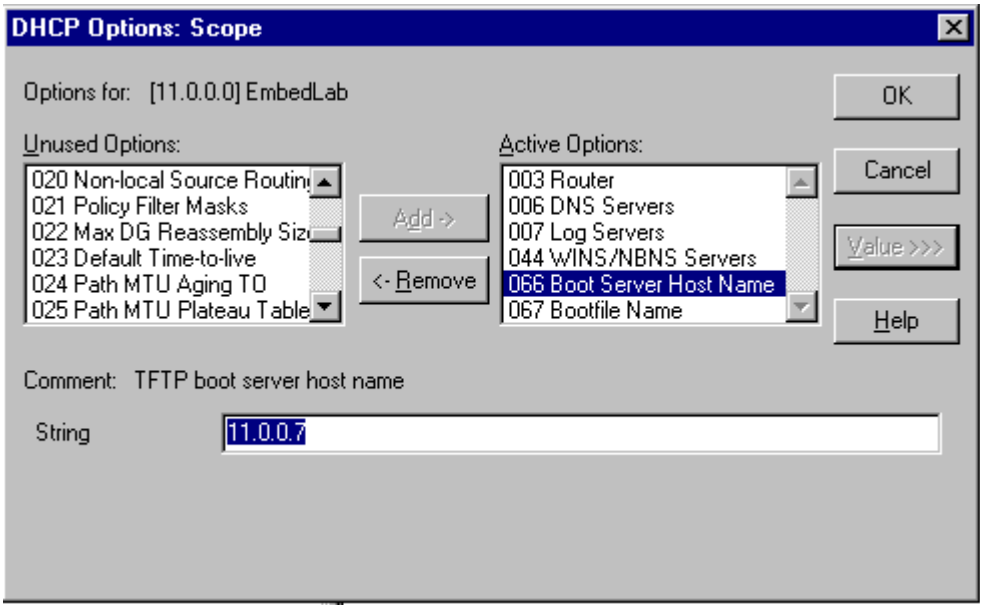


Figure 4-11 DHCP Options: Setting the Boot Server Host Name

4. Add the Boot Server Hostname and Boot Filename parameters to the Active Options list.
5. Set the value of the Boot Server Hostname Parameter to the hostname or IP Address of the TFTP server. For example: 11.0.0.7.

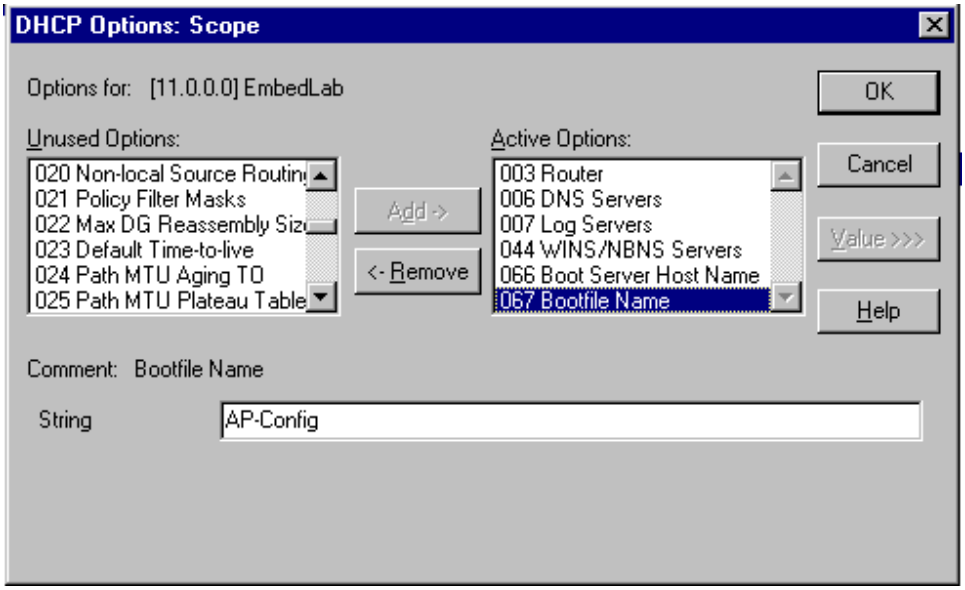


Figure 4-12 DHCP Options: Setting the Bootfile Name

6. Set the value of the Bootfile Name parameter to the Configuration filename. For example: AP-Config
7. If using Syslog, set the Log server IP address (option 7, Log Servers).
8. Reboot the AP. When the AP reboots it receives the new configuration information and must reboot one additional time. If a Syslog server was configured, the following messages can be observed on the Syslog server:

- AutoConfig for Dynamic IP
- TFTP server address and configuration filename
- AutoConfg Successful

Filtering

The Access Point's Packet Filtering features help control the amount of traffic exchanged between the wired and wireless networks. There are four sub-categories under the Filtering heading.

- Ethernet Protocol
- Static MAC
- Advanced
- TCP/UDP Port

Ethernet Protocol

The Ethernet Protocol Filter blocks or forwards packets based on the Ethernet protocols they support.

Follow these steps to configure the Ethernet Protocol Filter:

1. Select the interface or interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
   - **Ethernet:** Packets are examined at the Ethernet interface
   - **Wireless:** Packets are examined at the Wireless interface
   - **All Interfaces:** Packets are examined at both interfaces
   - **Disabled:** The filter is not used
2. Select the **Filter Operation Type**.
   - If set to **Passthru**, only the enabled Ethernet Protocols listed in the Filter Table will pass through the bridge.
   - If set to **Block**, the bridge will block enabled Ethernet Protocols listed in the Filter Table.
3. Configure the **Ethernet Protocol Filter Table**. This table is pre-populated with existing Ethernet Protocol Filters, however, you may enter additional filters by specifying the appropriate parameters.
   - To add an entry, click **Add**, and then specify the **Protocol Number** and a **Protocol Name**.
     - **Protocol Number:** Enter the protocol number. See http://www.iana.org/assignments/ethernet-numbers for a list of protocol numbers.
     - **Protocol Name:** Enter related information, typically the protocol name.
   - To edit or delete an entry, click **Edit** and change the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.
   - An entry's status must be enabled in order for the protocol to be subject to the filter.

Static MAC

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. When this feature is properly configured, the AP can block traffic between wired devices and wireless devices based on MAC address.

For example, you can set up a Static MAC filter to prevent wireless clients from communicating with a specific server on the Ethernet network. You can also use this filter to block unnecessary multicast packets from being forwarded to the wireless network.

NOTE

The Static MAC Filter is an advanced feature. You may find it easier to control wireless traffic by way of other filtering options, such as Ethernet Protocol Filtering.

Each static MAC entry contains the following fields:

- **Wired MAC Address**
- **Wired Mask**
- **Wireless MAC Address**
- **Wireless Mask**
- **Comment:** This field is optional.

Each MAC Address or Mask is comprised of 12 hexadecimal digits (0-9, A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (0 or 1).)

Taken together, a MAC Address/Mask pair specifies an address or a range of MAC addresses that the AP will look for when examining packets. The AP uses Boolean logic to perform an "AND" operation between the MAC Address and

the Mask at the bit level. However, for most users, you do not need to think in terms of bits. It should be sufficient to create a filter using only the hexadecimal digits 0 and F in the Mask (where 0 is any value and F is the value specified in the MAC address). A Mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a Mask of FF:FF:FF:FF:FF:FF applies only to the specified MAC Address.

For example, if the MAC Address is 00:20:A6:12:54:C3 and the Mask is FF:FF:FF:00:00:00, the AP will examine the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the Mask is FF:FF:FF:FF:FF:FF, the AP will only look for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, you can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters. Which parameters to configure depends upon the traffic that you want block:

– To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC Address and Wired Mask (leave the Wireless MAC Address and Wireless Mask set to all zeros).
– To prevent all traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC address and Wireless Mask (leave the Wired MAC Address and Wired Mask set to all zeros).
– To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

To create an entry, click **Add** and enter the appropriate MAC addresses and Masks to setup a filter. The entry is enabled automatically when saved. To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.

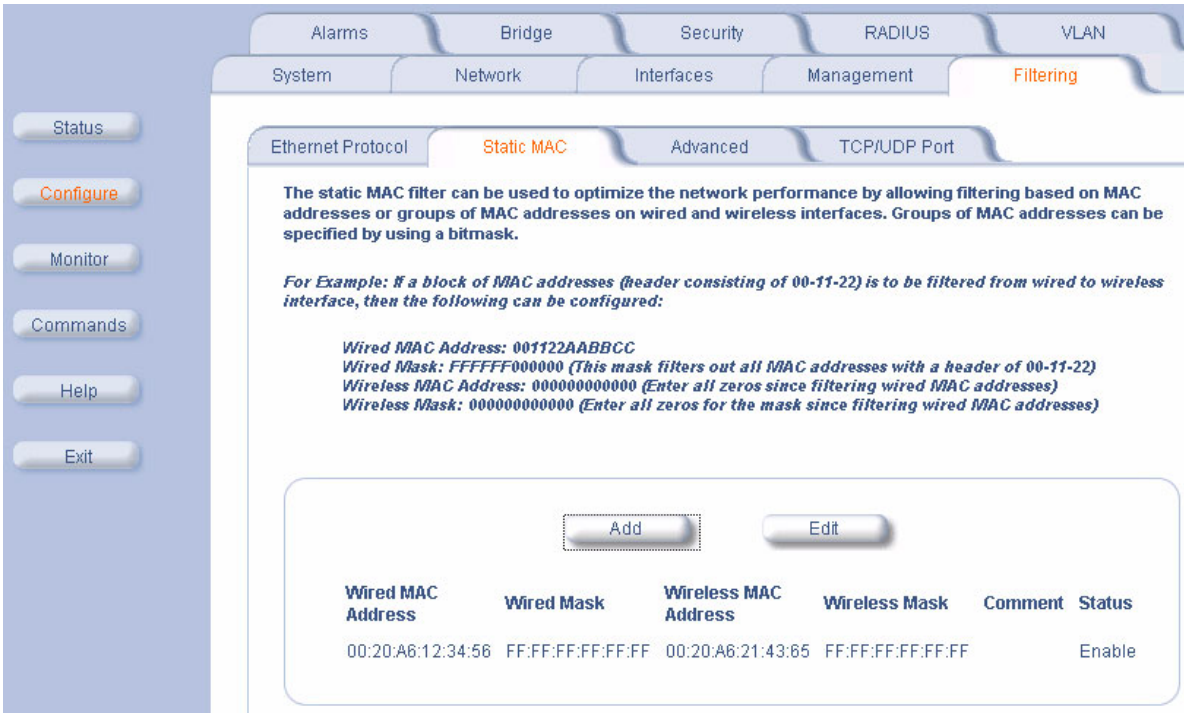


Figure 4-13 Static MAC Configuration Screen

Static MAC Filter Examples

Consider a network that contains a wired server and three wireless clients. The MAC address for each unit is as follows:

– Wired Server: 00:40:F4:1C:DB:6A
– ireless Client 1: 00:02:2D:51:94:E4
– Wireless Client 2: 00:02:2D:51:32:12
– Wireless Client 3: 00:20:A6:12:4E:38

Prevent Two Specific Devices from Communicating

Configure the following settings to prevent the Wired Server and Wireless Client 1 from communicating:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: Traffic between the Wired Server and Wireless Client 1 is blocked. Wireless Clients 2 and 3 can still communicate with the Wired Server.

Prevent Multiple Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Server.

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:00:00:00

Result: When a logical “AND” is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Server and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Server since it has a different prefix (00:20:A6).

Prevent All Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent all three Wireless Clients from communicating with Wired Server 1.

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The Access Point blocks all traffic between Wired Server 1 and all wireless clients.

Prevent A Wireless Device From Communicating With the Wired Network

Configure the following settings to prevent Wireless Client 3 from communicating with any device on the Ethernet.

- **Wired MAC Address:** 00:00:00:00:00:00
- **Wired Mask:** 00:00:00:00:00:00
- **Wireless MAC Address:** 00:20:A6:12:4E:38
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: The Access Point blocks all traffic between Wireless Client 3 and the Ethernet network.

Prevent Messages Destined for a Specific Multicast Group from Being Forwarded to the Wireless LAN

If there are devices on your Ethernet network that use multicast packets to communicate and these packets are not required by your wireless clients, you can set up a Static MAC filter to preserve wireless bandwidth. For example, if routers on your network use a specific multicast address (such as 01:00:5E:00:32:4B) to exchange information, you can set up a filter to prevent these multicast packets from being forwarded to the wireless network:

- **Wired MAC Address:** 01:00:5E:00:32:4B
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The Access Point does not forward any packets that have a destination address of 01:00:5E:00:32:4B to the wireless network.

Advanced

You can configure the following advanced filtering options:

- **Enable Proxy ARP:** Place a check mark in the box provided to allow the Access Point to respond to Address Resolution Protocol (ARP) requests for wireless clients. When enabled, the AP answers ARP requests for wireless stations without actually forwarding them to the wireless network. If disabled, the Access Point will bridge ARP requests for wireless clients to the wireless LAN.
- **Enable IP/ARP Filtering:** Place a check mark in the box provided to allow IP/ARP filtering based on the IP/ARP Filtering Address and IP Mask. Leave the box unchecked to prevent filtering. If enabled, you should also configure the IP/ARP Filtering Address and IP/ARP IP Mask.
  - **IP/ARP Filtering Address:** Enter the Network filtering IP Address.
  - **IP/ARP IP Mask:** Enter the Network Mask IP Address.

The following protocols are listed in the Advanced Filter Table:

- **Deny IPX RIP**
- **Deny IPX SAP**
- **Deny IPX LSP**
- **Deny IP Broadcasts**
- **Deny IP Multicasts**

The AP can filter these protocols in the wireless-to-Ethernet direction, the Ethernet-to-wireless direction, or in both directions. Click **Edit** and use the **Status** field to Enable or Disable the filter.

TCP/UDP Port

Port-based filtering enables you to control wireless user access to network services by selectively blocking TCP/UDP protocols through the AP. A user specifies a Protocol Name, Port Number, Port Type (TCP, UDP, or TCP/UDP), and filtering interfaces (Wireless only, Ethernet only, all interfaces, or no interfaces) in order to block access to services, such as Telnet and FTP, and traffic, such as NETBIOS and HTTP.

For example, an AP with the following configuration would discard frames received on its Ethernet interface with a UDP destination port number of 137, effectively blocking NETBIOS Name Service packets.

Protocol Type (TCP/UDP)	Destination Port Number	Protocol Name	Interface	Status (Enable/Disable)
UDP	137	NETBIOS Name Service	Ethernet	Enable

Adding TCP/UDP Port Filters

1. Place a check mark in the box labeled **Enable TCP/UDP Port Filtering**.
2. Click **Add** under the ***TCP/UDP Port Filter Table*** heading.
3. In the ***TCP/UDP Port Filter Table***, enter the Protocol Names to filter.
4. Set the destination Port Number (a value between 0 and 65535) to filter. See the IANA Web site at http://www.iana.org/assignments/port-numbers for a list of assigned port numbers and their descriptions.
5. Set the Port Type for the protocol: **TCP**, **UDP**, or both (**TCP/UDP**).
6. Set the **Interface** to filter:
   - Wireless
   - Ethernet
   - All interfaces
   - No interfaces
7. Click **OK**.

Editing TCP/UDP Port Filters

1. Click **Edit** under the ***TCP/UDP Port Filter Table*** heading.
2. Make any changes to the Protocol Name or Port Number for a specific entry, if necessary.
3. In the row that defines the port, set the **Status** to **Enable**, **Disable**, or **Delete**, as appropriate.
4. Select **OK**.

Alarms

This category has three sub-categories.

- Groups
- Alarm Host Table
- Syslog

Groups

There are seven alarm groups that can be enabled or disabled by way of the Web interface. Place a check mark in the box provided to enable a specific group. Remove the check mark from the box to disable the alarms. Alarm Severity Levels vary.

- **Configuration Alarm**

Trap Name	Description
oriTrapDNSIPNotConfigured	This traps is generated when the DNS IP Address has not been configured. Severity Level: Major

- **Security Alarms**

Trap Name	Description
oriTrapAuthenticationFailure	This trap is generated when a client authentication failure occurs. The authentication failures can range from: - MAC Access Control Table - RADIUS MAC Authentication - 802.1x Authentication specifying the EAP-Type Severity Level: Major
oriTrapUnauthorizedManagerDetected	This trap is generated when an unauthorized manager has attempted to view and/or modify parameters. Severity Level: Major

- **Wireless Alarms**

Trap Name	Description
oriTrapWLCNotPresent	When you start the AP, this trap is generated when a wireless interface/card is not present in the AP. Severity Level: Informational
oriTrapWLCFailure	This trap is generated when a general failure occurs with the wireless interface/card. Severity Level: Critical
oriTrapWLCRemoval	This trap is generated when the wireless interface/card has been removed from the device. Severity Level: Critical
oriTrapWLCIncompatibleFirmware	This trap is generated when the firmware of the wireless interface/card is incompatible with the AP. Severity Level: Critical
oriTrapWLCVoltageDiscrepancy	The dual-radio AP supports 3.3 V and 5 V wireless cards. This trap is generated when a wireless interface/card using a different voltage is inserted in the AP. Severity Level: Critical
oriTrapWLCIncompatibleVendor	This trap is generated when an incompatible wireless vendor card is inserted or present in the AP. Severity Level: Critical
oriTrapWLCFirmwareDownloadFailure	This trap is generated when a failure occurs during the firmware download process of the wireless interface/card. Severity Level: Critical

- **Operational Alarms**

Trap Name	Description
oriTrapWatchDogTimerExpired	This trap is generated when the software watch dog timer expires. This indicates that a problem has occurred with one or more software modules and the AP will reboot automatically. Trap Severity Level: Critical
oriTrapRADIUSServerNotResponding	This trap is generated when no response is received from the RADIUS server(s) for authentication requests sent from the RADIUS client in the AP. Trap Severity Level: Major
oriTrapModuleNotInitialized	This trap is generated when a certain software or hardware module is not initialized or fails to initialize. Trap Severity Level: Major
oriTrapDeviceRebooting	This trap is generated when the AP is rebooting. Trap Severity Level: Informational
oriTrapTaskSuspended	This trap is generated when a software task in the AP is suspended. Trap Severity Level: Critical
oriTrapBootPFailed	In bootloader mode, this trap is generated when the AP does not receive a response from the BootP server. The result is that the Access Point reverts to its static IP configuration and you will need to set reset configuration options. Trap Severity Level: Major
oriTrapDHCPFailed	In operational mode, this trap is generated when the AP does not receive a response from the DHCP server. The result is that the Access Point reverts to its static IP configuration and you will need to set reset configuration options. Trap Severity Level: Major

- **FLASH Memory Alarms**

Trap Name	Description
oriTrapFlashMemoryEmpty	This trap is generated when an error occurs while downloading a file to the AP and no data is present in the flash memory. Severity Level: Informational
oriTrapFlashMemoryCorrupted	This trap is generated when an error occurs while downloading a file to the AP and the data in the flash memory is invalid or corrupted. Severity Level: Critical

- **TFTP Alarms**

Trap Name	Description
oriTrapTFTPFailedOperation	This trap is generated when a failure occurs during a TFTP upload or download operation. Severity Level: Major
oriTrapTFTPOperationInitiated	This trap is generated when a TFTP upload or download operation is started. Severity Level: Informational
oriTrapTFTPOperationCompleted	This trap is generated when a TFTP operation is complete (upload or download). Severity Level: Informational

- **Image Alarms**

Trap Name	Description
oriTrapZeroSizeImage	This trap is generated when a zero size image is loaded on the AP. Trap Severity Level: Major
oriTrapInvalidImage	This trap is generated when an invalid image is loaded in the Access Point. Trap Severity Level: Major
oriTrapImageTooLarge	This trap is generated when the image loaded in the AP exceeds the size limitation of the flash memory. Trap Severity Level: Major
oriTrapIncompatibleImage	This trap is generated when an incompatible image is loaded in the AP. Trap Severity Level: Major

In addition, the AP supports these standard traps, which are always enabled:

- **RFC 1215-Trap**

Trap Name	Description
coldStart	The AP has been turned on or rebooted. Trap Severity Level: Informational
linkUp	The AP's Ethernet interface link is up (working). Trap Severity Level: Informational
linkDown	The AP's Ethernet interface link is down (not working). Trap Severity Level: Informational

- **Bridge MIB (RFC 1493) Alarms**

Trap Name	Description
newRoot	This trap indicates that the AP has become the new root in the Spanning Tree network. Trap Severity Level: Informational
topologyChange	This trap is sent by the AP when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. This trap is not sent if a newRoot trap is sent for the same transition. Trap Severity Level: Informational

All these alarm groups correspond to System Alarms that are displayed in the System Status screen, including the traps that are sent by the AP to the SNMP managers specified in the Alarm Host Table.

Severity Levels

There are three severity levels for system alarms:

- Critical
- Major
- Informational

Critical alarms will often result in severe disruption in network activity or an automatic reboot of the AP.

Major alarms are usually activated due to a breach in the security of the system. Clients cannot be authenticated or an attempt at unauthorized access into the AP has been detected.

Informational alarms are there to provide the network administrator with some general information about the activities the AP is performing.

Alarm Host Table

To add an entry and enable the AP to send SNMP trap messages to a Trap Host, click **Add**, and then specify the IP Address and Password for the Trap Host.

- **IP Address:** Enter the Trap Host IP Address.
- **Password:** Enter the password in the **Password** field and the **Confirm** field.
- **Comment:** Enter an optional comment, such as the alarm (trap) host station name.

To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.

Syslog

The Syslog messaging system enables the AP to transmit event messages to a central server for monitoring and troubleshooting. The AP can send messages to one Syslog server (it cannot send messages to more than one Syslog server). The access point logs “Session Start (Log-in)” and “Session Stop (Log-out)” events for each wireless client as an alternative to RADIUS accounting.

See RFC 3164 at http://www.rfc-editor.org for more information on the Syslog standard.

Figure 4-14 Syslog Configuration Screen

Setting Syslog Event Notifications

Syslog Events are logged according to the level of detail specified by the administrator. Logging only urgent system messages will create a far smaller, more easily read log then a log of every event the system encounters. Determine which events to log by selecting a priority defined by the following scale:

Event	Priority	Description
LOG_EMERG	0	system is unusable
LOG_ALERT	1	action must be taken immediately
LOG_CRIT	2	critical conditions
LOG_ERR	3	error conditions
LOG_WARNING	4	warning conditions
LOG_NOTICE	5	normal but significant condition
LOG_INFO	6	informational
LOG_DEBUG	7	debug-level messages

Configuring Syslog Event Notifications

You can configure the following Syslog settings from the HTTP interface:

- **Enable Syslog:** Place a check mark in the box provided to enable system logging.
- **Syslog Port Number:** This field is read-only and displays the port number (514) assigned for system logging.
- **Syslog Lowest Priority Logged:** The AP will send event messages to the Syslog server that correspond to the selected priority and above. For example, if set to 6, the AP will transmit event messages labeled priority 0 to 6 to the Syslog server(s). This parameter supports a range between 1 and 7; 6 is the default.
- **Syslog Host Table:** This table specifies the IP addresses of a network servers that the AP will send Syslog messages to. Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  - **IP Address:** Enter the IP Address for the management host.
  - **Comment:** Enter an optional comment such as the host name.
  - **Status:** The entry is enabled automatically when saved (so the Status field is only visible when editing an entry). You can also disable or delete entries by changing this field's value.

Bridge

The AP is a bridge between your wired and wireless networking devices. As a bridge, the functions performed by the AP include:

- MAC address learning
- Forward and filtering decision making
- Spanning Tree protocol used for loop avoidance

Once the AP is connected to your network, it learns which devices are connected to it and records their MAC addresses in the Learn Table. The table can hold up to 10,000 entries. To view the Learn Table, click on the **Monitor** button in the Web interface and select the Learn Table tab.

The **Bridge** tab has four sub-categories.

- Spanning Tree
- Storm Threshold
- Intra BSS
- Packet Forwarding

Spanning Tree

A Spanning Tree is used to avoid redundant communication loops in networks with multiple bridging devices. Bridges do not have any inherent mechanism to avoid loops, because having redundant systems is a necessity in certain networks. However, redundant systems can cause Broadcast Storms, multiple frame copies, and MAC address table instability problems.

Complex network structures can create multiple loops within a network. The Spanning Tree configuration blocks certain ports on AP devices to control the path of communication within the network, avoiding loops and following a spanning tree structure.

For more information on Spanning Tree protocol, please see Section 8.0 of the IEEE 802.1d standard. The Spanning Tree configuration options are advanced settings. HP recommends that you leave these parameters at their default values unless you are familiar with the Spanning Tree protocol.

Storm Threshold

Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by:

- Specifying a maximum number of frames per second as received from a single network device (identified by its MAC address).
- Specifying an absolute maximum number of messages per port.

The Storm Threshold parameters allow you to specify a set of thresholds for each port of the AP, identifying separate values for the number of broadcast messages/second and Multicast messages/second.

When the number of frames for a port or identified station exceeds the maximum value per second, the AP will ignore all subsequent messages issued by the particular network device, or ignore all messages of that type.

– **Address Threshold:** Enter the maximum allowed number of packets per second.
– **Ethernet Threshold:** Enter the maximum allowed number of packets per second.
– **Wireless Threshold:** Enter the maximum allowed number of packets per second.

Intra BSS

The wireless clients (or *subscribers*) that associate with a certain AP form the Basic Service Set (BSS) of a network infrastructure. By default, wireless subscribers in the same BSS can communicate with each other. However, some administrators (such as wireless public spaces) may wish to block traffic between wireless subscribers that are associated with the same AP to prevent unauthorized communication and to conserve bandwidth. This feature enables you to prevent wireless subscribers within a BSS from exchanging traffic.

Although this feature is generally enabled in public access environments, Enterprise LAN administrators use it to conserve wireless bandwidth by limiting communication between wireless clients. For example, this feature prevents peer-to-peer file sharing or gaming over the wireless network.

To block Intra BSS traffic, set **Intra BSS Traffic Operation** to **Block**.

To allow Intra BSS traffic, set **Intra BSS Traffic Operation** to **Passthru**.

Packet Forwarding

The Packet Forwarding feature enables you to redirect traffic generated by wireless clients that are all associated to the same AP to a single MAC address. This filters wireless traffic without burdening the AP and provides additional security by limiting potential destinations or by routing the traffic directly to a firewall. You can redirect to a specific port (Ethernet or WDS) or allow the bridge's learning process (and the forwarding table entry for the selected MAC address) to determine the optimal port.

NOTE

The gateway to which traffic will be redirected should be a node on the Ethernet network. It should not be a wireless client.

Configuring Interfaces for Packet Forwarding

Configure your AP to forward packets by specifying interface port(s) to which packets are redirected and a destination MAC address.

1. Within the ***Packet Forwarding Configuration*** screen, check the box labeled **Enable Packet Forwarding**.
2. Specify a destination **Packet Forwarding MAC Address**. The AP will redirect all unicast, multicast, and broadcast packets received from wireless clients to the address you specify.
3. Select a **Packet Forwarding Interface Port** from the drop-down menu. You can redirect traffic to:
   – Ethernet
   – A WDS connection (see Wireless Distribution System (WDS) for details)
   – Any (traffic is redirected to a port based on the bridge learning process)
4. Click **OK** to save your changes.

Security

The AP provides several security features to protect your network from unauthorized access.

- Authentication and Encryption Modes
- MAC Access
- Rogue Access Point Detection (RAD)

Authentication and Encryption Modes

The AP supports the following Security features:

- WEP Encryption: The original encryption technique specified by the IEEE 802.11 standard.
- 802.1x Authentication: An IEEE standard for client authentication.
- Wi-Fi Protected Access (WPA): A new standard that provides improved encryption security over WEP.

WEP Encryption

The IEEE 802.11 standards specify an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on an 802.11 network using an Encryption Key (also known as a WEP Key).

When Encryption is enabled, two 802.11 devices must have the same Encryption Keys and both devices must be configured to use Encryption in order to communicate. If one device is configured to use Encryption but a second device is not, then the two devices will not communicate, even if both devices have the same Encryption Keys.

- An 802.11b AP supports 64-bit and 128-bit encryption:
  - For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart).
  - For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.
- An 802.11a or 802.11b/g AP supports 64-bit, 128-bit, and 152-bit encryption:
  - For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart).
  - For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.
  - For 152-bit encryption, an encryption key is 32 hexadecimal characters or 16 ASCII characters.

NOTE

64-bit encryption is sometimes referred to as 40-bit encryption; 128-bit encryption is sometimes referred to as 104-bit encryption.

802.1x Authentication

IEEE 802.1x is a standard that provides a means to authenticate and authorize network devices attached to a LAN port. A port in the context of IEEE 802.1x is a point of attachment to the LAN, either a physical Ethernet connection or a wireless link to an Access Point. 802.1x requires a RADIUS server and uses the Extensible Authentication Protocol (EAP) as a standards-based authentication framework, and supports automatic key distribution for enhanced security. The EAP-based authentication framework can easily be upgraded to keep pace with future EAP types.

Popular EAP types include:

- EAP-Message Digest 5 (MD5): Username/Password-based authentication; does not support automatic key distribution
- EAP-Transport Layer Security (TLS): Certificate-based authentication (a certificate is required on the server and each client); supports automatic key distribution
- EAP-Tunneled Transport Layer Security (TTLS): Certificate-based authentication (a certificate is required on the server; a client's username/password is tunneled to the server over a secure connection); supports automatic key distribution
- PEAP - Protected EAP with MS-CHAP v2: Secure username/password-based authentication; supports automatic key distribution

Different servers support different EAP types and each EAP type provides different features. Refer to the documentation that came with your RADIUS server to determine which EAP types it supports.

NOTE

The AP supports the following EAP types when Authentication Mode is set to **802.1x** or **WPA**: EAP-TLS, PEAP, and EAP-TTLS. When Authentication Mode is set to Mixed, the AP supports the following EAP types: EAP-TLS, PEAP, EAP-TLLS, and EAP-MD5 (MD5 does not support automatic key distribution; therefore, if you choose this method you need to manually configure each client with the network's encryption key).

Authentication Process

There are three main components in the authentication process. The standard refers to them as:

1. supplicant (client PC)
2. authenticator (Access Point)
3. authentication server (RADIUS server)

When using Authentication Mode is set to 802.1x, WPA, or Mixed mode (802.1x and WEP), you need to configure your RADIUS server for authentication purposes.

Prior to successful authentication, an unauthenticated client PC cannot send any data traffic through the AP device to other systems on the LAN. The AP inhibits all data traffic from a particular client PC until the client PC is authenticated. Regardless of its authentication status, a client PC can always exchange 802.1x messages in the clear with the AP (the client begins encrypting data after it has been authenticated).

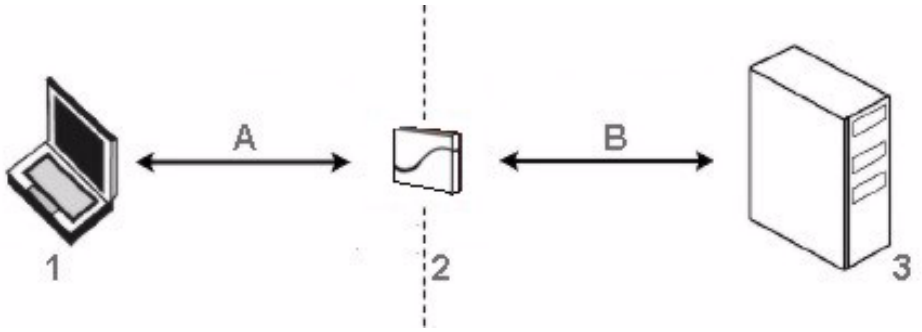


Figure 4-15 RADIUS Authentication Illustrated

The AP acts as a pass-through device to facilitate communications between the client PC and the RADIUS server. The AP (2) and the client (1) exchange 802.1x messages using an EAPOL (EAP Over LAN) protocol (A). Messages sent from the client station are encapsulated by the AP and transmitted to the RADIUS (3) server using EAP extensions (B).

Upon receiving a reply EAP packet from the RADIUS, the message is typically forwarded to the client, after translating it back to the EAPOL format. Negotiations take place between the client and the RADIUS server. After the client has been successfully authenticated, the client receives an Encryption Key from the AP (if the EAP type supports automatic key distribution). The client uses this key to encrypt data after it has been authenticated.

For 802.11a and 802.11b/g clients that communicate with an AP, each client receives its own unique encryption key; this is known as Per User Per Session Encryption Keys.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a security standard designed by the Wi-Fi Alliance in conjunction with the Institute of Electrical and Electronics Engineers (IEEE). WPA is a sub-set of the forthcoming IEEE 802.11i security standard, currently in draft form. (IEEE 802.11i is also referred to as "WPA2" and will be available in 2004.)

NOTE

For Dual-radio APs: WPA is available for APs an HP ProCurve Wireless 802.11g AP Card 170wl only.

WPA is a replacement for Wired Equivalent Privacy (WEP), the encryption technique specified by the original 802.11 standard. WEP has several vulnerabilities that have been widely publicized. WPA addresses these weaknesses and provides a stronger security system to protect wireless networks.

WPA provides the following new security measures not available with WEP:

- Improved packet encryption using the Temporal Key Integrity Protocol (TKIP) and the Michael Message Integrity Check (MIC).
- Per-user, per-session dynamic encryption keys:
  - Each client uses a different key to encrypt and decrypt unicast packets exchanged with the AP
  - A client's key is different for every session; it changes each time the client associates with an AP
  - The AP uses a single global key to encrypt broadcast packets that are sent to all clients simultaneously
  - Encryption keys change periodically based on the **Re-keying Interval** parameter
  - WPA uses 128-bit encryption keys
- Dynamic Key distribution
  - The AP generates and maintains the keys for its clients
  - The AP securely delivers the appropriate keys to its clients
- Client/server mutual authentication
  - 802.1x
  - Pre-shared key (for networks that do not have an 802.1x solution implemented)

NOTE

For more information on WPA, see the Wi-Fi Alliance Web site at http://www.wi-fi.org.

The AP supports two WPA authentication modes:

- **WPA:** The AP uses 802.1x to authenticate clients. You should only use an EAP that supports mutual authentication and session key generation, such as EAP-TLS, EAP-TTLS, and PEAP. See 802.1x Authentication for details.
- **WPA-PSK (Pre-Shared Key):** For networks that do not have 802.1x implemented, you can configure the AP to authenticate clients based on a Pre-Shared Key. This is a shared secret that is manually configured on the AP and each of its clients. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).

Configuring Security Settings

You can configure each wireless interface to operate in one of the following Security modes:

1. No Security: This is the default setting for an AP.
2. Enable WEP Encryption: The AP and clients use the same static WEP keys to encrypt data.
3. Enable 802.1x Security: The AP uses the 802.1x standard to communicate with a RADIUS server and authenticate clients. The AP generates and distributes dynamic, per user WEP Keys to each client following successful authentication.
4. Enable Mixed Mode (802.1x and WEP Encryption): The AP uses 802.1x Mode for clients that support 802.1x (and have an 802.1x supplicant application installed). The AP uses static WEP Encryption for clients that do not use 802.1x.
5. Enable WPA Mode: The AP uses 802.1x to communicate with a RADIUS server and authenticate clients. The AP generates and distributes dynamic, per user encryption keys (based on the Temporal Key Integrity Protocol (TKIP)) to each client following successful authentication. WPA mode provides message integrity checking to guard against replay type attacks. This mode is not available for all radio types.
6. Enable WPA-PSK Mode: The AP uses a Pre-shared Key (manually configured on both the AP and the clients) to authenticate clients. The AP generates and distributes dynamic, per user encryption keys (based on TKIP) to each client following successful authentication. This mode is for customers who want to use WPA but do not have a RADIUS server installed on their network. This mode is not available for all radio types.

You configure the AP to use a particular Security mode by setting the Authentication Mode parameter. The following table summarizes the Authentication Mode options available in the HTTP Interface's **Configure** > **Security** > **Authentication** screen and describes how each of these options correspond to the six Security Modes listed above:

Authentication Mode Setting	Authentication Method Employed	Encryption Method Employed
None	None	None or manually configured Static WEP settings (from **Configure** > **Security** > **Encryption** screen)
802.1x	802.1x	Dynamic WEP Keying
Mixed	802.1x or None (depends on a client's configuration)	Dynamic WEP Keying or Static WEP (depends on client's configuration)
WPA	802.1x	Dynamic TKIP Keying
WPA-PSK	Manually configured Pre-shared Key	Dynamic TKIP Keying

NOTE

Before enabling the 802.1x, Mixed, or WPA mode, the 802.1x server should be configured. Set the encryption key in Mixed mode after the authentication is set to Mixed mode.

Enable WEP Encryption

Follow these steps to set up WEP encryption on an AP:

1. Click **Configure** > **Security** > **Authentication**.
2. Set **Authentication Mode** to **None** (if necessary).
3. Click the **Encryption** tab.
4. Place a check mark in the box labeled **Enable Encryption (WEP)**.
5. Enter one to four Encryption Keys in the fields provided. Keep in mind the following:
   - If entering more than one Key, use the same number of characters for each Key. All Keys need to be the same Key Size (64, 128, or 152-bit).
   - You can enter the Encryption Keys in either hexadecimal or ASCII format.
   - You need to configure your wireless clients to use the same Keys in order for the clients and the AP to communicate.
6. Select the Key that the AP will use to encryption outgoing data from the **Encrypt Data Transmissions Using** drop-down menu. By default, this parameter is set to Key 1.
7. Click **OK**.

Enable 802.1x Security

Follow these steps to enable 802.1x only:

1. Click **Configure** > **Security** > **Authentication**.
2. Set **Authentication Mode** to **802.1x**.
3. Select an **Encryption Key Length**.
   - An 802.11b AP supports 64-bit and 128-bit encryption.
   - An 802.11a or 802.11b/g AP supports 64-bit and 128-bit encryption.
4. Enter a **Re-keying Interval**.
   - The Re-keying Interval determines how often a client's encryption key is changed and can be set to any value between 60 - 65535 seconds. Rekeying frustrates hacking attempts without taxing system resources. Setting a fairly frequent rekey value (900 seconds=15 minutes) effectively protects against intrusion without disrupting network activities.
5. Click **OK** to save the changes.
6. If you have not already done so, configure the RADIUS authentication settings (see RADIUS Authentication with 802.1x for details).
7. Reboot the Access Point.

Enable Mixed Mode (802.1x and WEP Encryption)

Follow these steps to use both 802.1x and WEP Encryption simultaneously (clients that do not support 802.1x use WEP Encryption for security purposes):

1. Click **Configure** > **Security** > **Authentication**.
2. Set **Authentication Mode** to **Mixed**.
3. Enter a **Re-keying Interval**.
   - The Re-keying Interval determines how often a client's encryption key is changed and can be set to any value between 60 - 65535 seconds. Rekeying frustrates hacking attempts without taxing system resources. Setting a fairly frequent rekey value (900 seconds=15 minutes) effectively protects against intrusion without disrupting network activities.
4. Click **OK** to save the changes.
5. Click the **Encryption** tab.
6. Place a check mark in the box labeled **Enable Encryption (WEP)**.
7. Configure **Encryption Key 1** only (i.e., do not configure Keys 2 through 4). Keep in mind the following:
   - For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see ASCII Character Chart).
   - For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.
   - You can enter the Encryption Keys in either hexadecimal or ASCII format.
   - You need to manually configure your wireless clients that do not support 802.1x to use the same Encryption Key.
8. Confirm that **Key 1** is selected in the **Encrypt Data Transmissions Using** drop-down menu.
9. Click **OK**.
10. If you have not already done so, configure the RADIUS authentication settings (see RADIUS Authentication with 802.1x for details).
11. Reboot the Access Point.

802.1x Security and Wireless Distribution Systems (WDS)

Wireless Distribution Systems (WDS) are configured using specific ports on an 802.11a, 802.11b, or 802.11b/g AP. To use 802.1x with WDS, you need to set the 802.1x Security Mode to Mixed (WEP and 802.1x) and confirm that the APs communicating in the WDS share the same encryption key (Key 1). See Wireless Distribution System (WDS) for more information.

Enable WPA Mode

NOTE

For Dual-radio APs: WPA is available for APs an HP ProCurve Wireless 802.11g AP Card 170wl only.

1. Click **Configure** > **Security** > **Authentication**.
2. Set **Authentication Mode** to **WPA**.
3. Enter a **Re-keying Interval**.
   - The Re-keying Interval determines how often a client's encryption key is changed and can be set to any value between 60 and 65535 seconds. Rekeying frustrates hacking attempts without taxing system resources. Setting a fairly frequent rekey value (900 seconds=15 minutes) effectively protects against intrusion without disrupting network activities.
4. Click **OK**.
5. If you have not already done so, configure the RADIUS authentication settings (see RADIUS Authentication with 802.1x for details).
6. Reboot the Access Point.

Enable WPA-PSK Mode

NOTE

For Dual-radio APs: WPA is available for APs an HP ProCurve Wireless 802.11g AP Card 170wl only.

1. Click **Configure** > **Security** > **Authentication**.
2. Set **Authentication Mode** to **WPA-PSK**.
3. Enter a **Re-keying Interval**.
   - The Re-keying Interval determines how often a client's encryption key is changed and can be set to any value between 60 and 65535 seconds. Rekeying frustrates hacking attempts without taxing system resources. Setting a fairly frequent rekey value (900 seconds=15 minutes) effectively protects against intrusion without disrupting network activities.
4. Configure the Pre-Shared Key.
   - You must also configure your clients to use this same key.
   - Do one of the following:
     — Enter 64 hexadecimal digits in the **Pre-Shared Key** field.
     — Enter a phrase in the **PSK Pass Phrase** field. The AP will automatically generate a Pre-Shared Key based on the phrase you enter. Enter between 8 and 63 characters; HP recommends using a pass phrase of at least 13 characters, including both numbers and upper and lower case letters, to ensure that the generated key cannot be easily deciphered by network infiltrators.
5. Click **OK**.
6. Reboot the Access Point.

MAC Access

The MAC Access tab allows you to build a list of stations, identified by their MAC addresses, authorized to access the network through the AP. The list is stored inside each AP within your network. Note that you must reboot the AP for any changes to the MAC Access Control Table to take effect.

- **Enable MAC Access Control:** Check this box to enable the Control Table.
- **Operation Type:** Choose between **Passthru** and **Block**. This determines how the stations identified in the MAC Access Control Table are filtered.
  - If set to **Passthru**, only the addresses listed in the Control Table will pass through the bridge.
  - If set to **Block**, the bridge will block traffic to or from the addresses listed in the Control Table.
- **MAC Access Control Table:** Click **Add** to create a new entry. Click **Edit** to change an existing entry. Each entry contains the following field:
  – **MAC Address:** Enter the wireless client's MAC address.
  – **Comment:** Enter an optional comment such as the client's name.
  - **Status:** The entry is enabled automatically when saved (so the Status field is only visible when editing an entry). You can also disable or delete entries by changing this field's value.

NOTE

For larger networks that include multiple Access Points, you may prefer to maintain this list on a centralized location using the MAC Access Control by way of RADIUS Authentication.

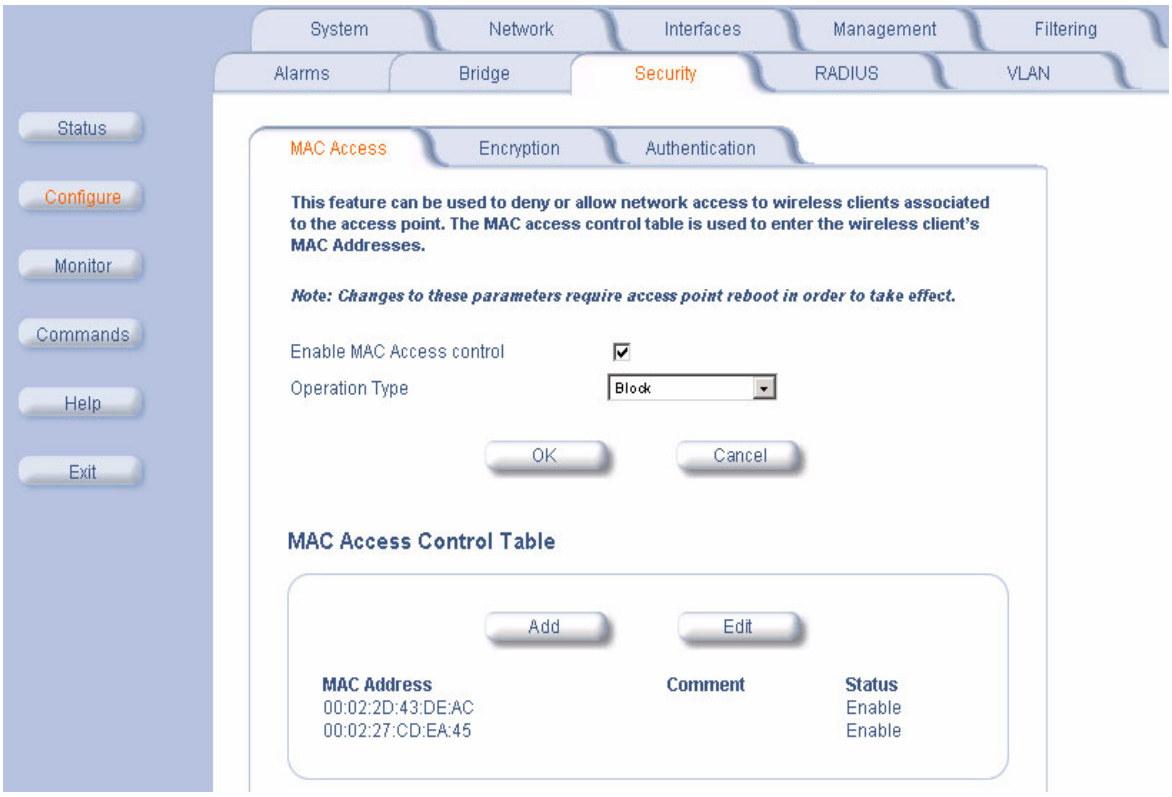


Figure 4-16 MAC Access Configuration Screen

Rogue Access Point Detection (RAD)

The Rogue AP Detection (RAD) feature provides an additional security level for wireless LAN deployments. RAD detects unauthorized Access Points in the coverage area. When enabled, the Access Point scans the coverage area and identifies all active Access Points. Support is available for all versions and operation modes of Access Points. For example, an 802.11a Access Point identifies all similar Access Points. However, it will not detect Access Points that are not of this type like 802.11b and 802.11g.

The Rogue AP Scan employs background scanning using low-level 802.11 scanning functions for effective wireless detection of Access Points in its coverage area with minimal impact on the normal operation of the Access Point.

This RAD feature can be enabled on an Access Point with its HTTP, CLI, or SNMP Interfaces. The scan repetition duration is configurable. If the Access Point uses directional antennas to provide directional coverage, then the interface bitmask can be configured to maximize the scanning coverage area. The Access Point will periodically scan the wireless network and report all the available Access Points within its coverage area using SNMP traps. For additional reliability the results are stored in the Access Point in a table, which can be queried by way of SNMP. The BSSID and Channel number of the detected Access Points are provided in the scan results.

The RAD scan is done on a channel list initialized based on the regulatory domain of the device. The RAD Scan then performs background scanning on all the channels in this channel list using 802.11 MAC scanning functions. It will either actively scan the network by sending probe requests or passively scan by only listening for beacons. The access point information is then gathered from the probe responses and beacons.

To minimize traffic disruption and maximize the scanning efficiency, the RAD feature employs an enhanced background-scanning algorithm and uses the CTS to Self mechanism to keep the clients silent. The scanning algorithm allows traffic to be serviced between each channel scan. Before start of every scan (except scan on the working channel) the CTS to self-mechanism is used to set the NAV values of clients to keep them silent during the scanning period. In addition, the scan repetition duration can also be configured to reduce the frequency of RAD scan cycles to maximize Access Point performance.

RAD Configuration Requirements

The RAD feature can be configured/monitored by way of the HTTP, CLI, or SNMP management interfaces.

The following management options are provided:

- The RAD feature can be enabled or disabled.
- The repetition interval of RAD can be configured.
- The interface on which RAD can operate can be configured.
- SNMP Traps are sent after completion of a RAD scan cycle and also whenever a new Access Point is detected.
- Additionally, the RAD scan results are maintained in a table that can be queried by way of SNMP.

The system administrator has to enable RAD on the Access Points in the wireless network and also configure the Trap Host on all these Access Points to the IP address of the management station. The Access Points on detecting a new Access Point sends a RAD Scan Result Trap to the management station.

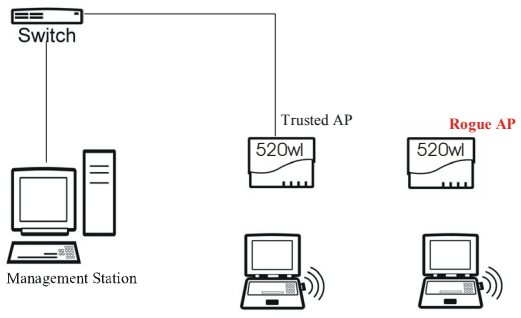


Figure 4-17 Example Rogue AP Detection Deployment

An example network deployment is shown. The Trusted AP has Rogue Access Detection enabled and the trap host is configured to be the management station. The Trusted AP on detecting the Rogue AP will send a trap to the management station with the Channel and BSSID of the Rogue Access Point.

Configuring RAD

Perform this procedure to enable RAD and define the Scan Interval and Scan Interface.

The RAD screen also displays the time of the last scan and the number of new access points detected in the last scan.

1. Enable the Security Alarm Group. Select the Security Alarm Group link from the RAD screen. Configure a Trap Host to receive the list of access points detected during the scan.
2. Click **Configure** > **Security** > **RAD**.
3. Enable RAD by checking **Enable Rogue AP Detection**.
4. Enter the **Scan Interval**.
   - The Scan Interval specifies the time period in minutes between scans and can be set to any value between 15 and 1440 minutes.
5. Select the **Scan Interface** as Slot A, Slot B, or both.
6. Click **OK**.

The results of the RAD scan can be viewed in the **Status** page in the HTTP interface.

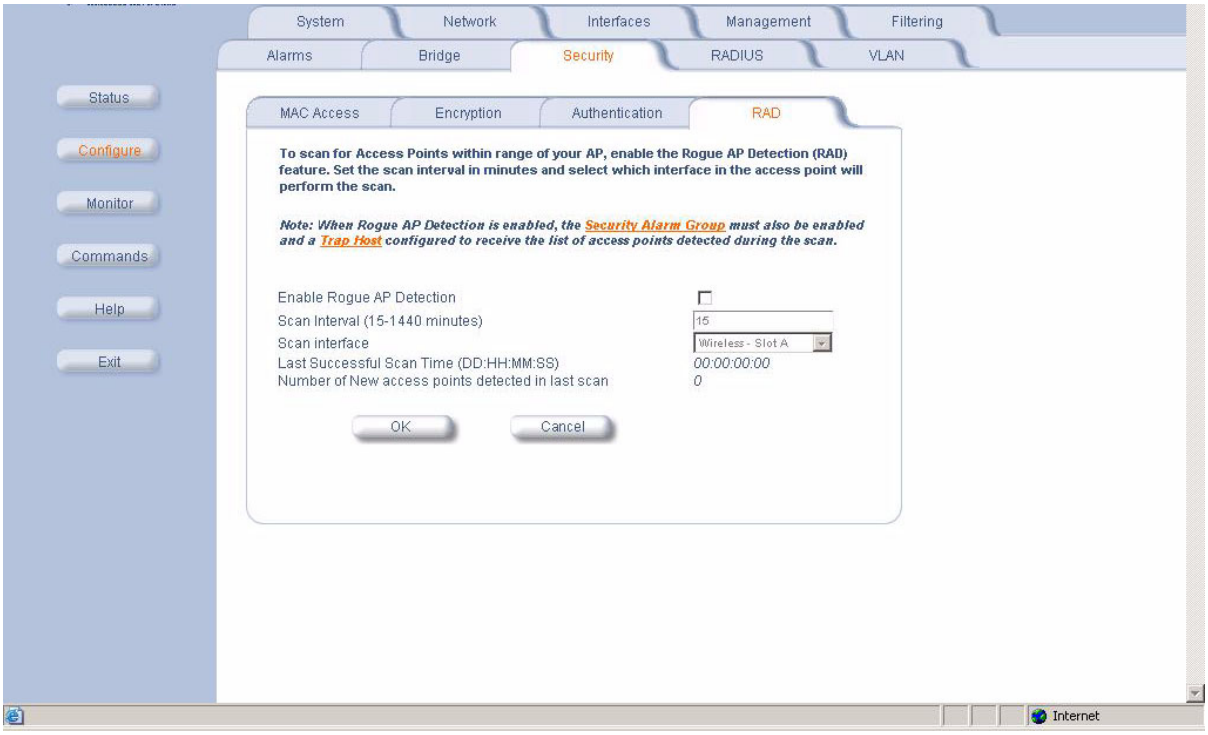


Figure 4-18 Rogue Access Point Detection Screen

RADIUS

The AP communicates with a network's RADIUS server to provide the following features:

- MAC Access Control by way of RADIUS Authentication
- RADIUS Authentication with 802.1x
- RADIUS Accounting

The network administrator can configure multiple RADIUS Authentication Servers for different Authentication types. The current available authentication types are EAP/802.1x authentication and MAC-based authentication.You can configure two separate sets of Primary and Secondary RADIUS Servers for each of the two supported Authentication types, 802.1x EAP Based authentication and MAC based authentication.

You can configure the AP to communicate with up to six different RADIUS servers:

- Primary Authentication Server (MAC-based authentication)
- Back-up Authentication Server (MAC-based authentication)
- Primary Authentication Server (EAP/802.1x authentication)
- Back-up Authentication Server (EAP/802.1x authentication)
- Primary Accounting Server
- Back-up Accounting Server

NOTE

You must have configured the settings for at least one Authentication server before configuring the settings for an Accounting server.

The back-up servers are optional, but when configured, the AP will communicate with the back-up server if the primary server is off-line. After the AP has switched to the backup server, it will periodically check the status of the primary RADIUS server every five (5) minutes. Once the primary RADIUS server is again online, the AP automatically reverts from the backup RADIUS server back to the primary RADIUS server. All subsequent requests are then sent to the primary RADIUS server.

You can view monitoring statistics for each of the configured RADIUS servers.

MAC Access Control by way of RADIUS Authentication

If you want to control wireless access to the network and if your network includes a RADIUS Server, you can store the list of MAC addresses on the RADIUS server rather than configure each AP individually. From the RADIUS Authentication tab, you can define the IP Address of the server that contains a central list of MAC Address values that identify the authorized stations that may access the wireless network. You must specify information for at least the primary RADIUS server. The back-up RADIUS server is optional.

NOTE

Contact your RADIUS server manufacturer if you have problems configuring the server or have problems using RADIUS authentication.

Follow these steps to enable RADIUS MAC Access Control:

1. Within the ***RADIUS Auth*** screen, place a check mark in the box labeled **Enable RADIUS MAC Access Control**.
2. Place a check mark in the box labeled **Enable Primary RADIUS Authentication Server**.
3. If you want to configure a back-up RADIUS server, place a check mark in the box labeled **Enable Back-up RADIUS Authentication Server**.
4. Enter the time, in seconds, each client session may be active before being automatically re-authenticated in the **Authorization Lifetime** field. This parameter supports a value between 900 and 43200 sec; the default is 900 sec.
5. Select a **MAC Address Format Type**. This should correspond to the format in which the clients' 12-digit MAC addresses are listed within the RADIUS server. Available options include:
   - **Dash delimited:** dash between each pair of digits: xx-yy-zz-aa-bb-cc
   - **Colon delimited:** colon between each pair of digits: xx:yy:zz:aa:bb:cc)
   - **Single dash delimited:** dash between the sixth and seventh digits: xxyyzz-aabbcc
   - **No delimiters:** No characters or spaces between pairs of hexadecimal digits: xxyyzzaabbcc

6. Select a **Server Addressing Format** type (IP Address or Name).
   - If you want to identify RADIUS servers by name, you must configure the AP as a DNS Client. See DNS Client for details.
7. Enter the server's IP address or name in the field provided.
8. Enter the port number which the AP and the server will use to communicate. By default, RADIUS servers communicate on port 1812.
9. Enter the Shared Secret in the **Shared Secret** and **Confirm Shared Secret** field. This is a password shared by the RADIUS server and the AP. The same password must also be configured on the RADIUS server.
10. Enter the maximum time, in seconds, that the AP should wait for the RADIUS server to respond to a request in the **Response Time** field. Range is 1-10 seconds; default is 3 seconds.
11. Enter the maximum number of times an authentication request may be retransmitted in the **Maximum Retransmissions** field. Range is 1-4; default is 3.
12. If you are configuring a back-up server, repeat Steps 6 through 11 for the back-up server.
13. Click **OK** to save your changes.
14. Reboot the AP for these changes to take effect.

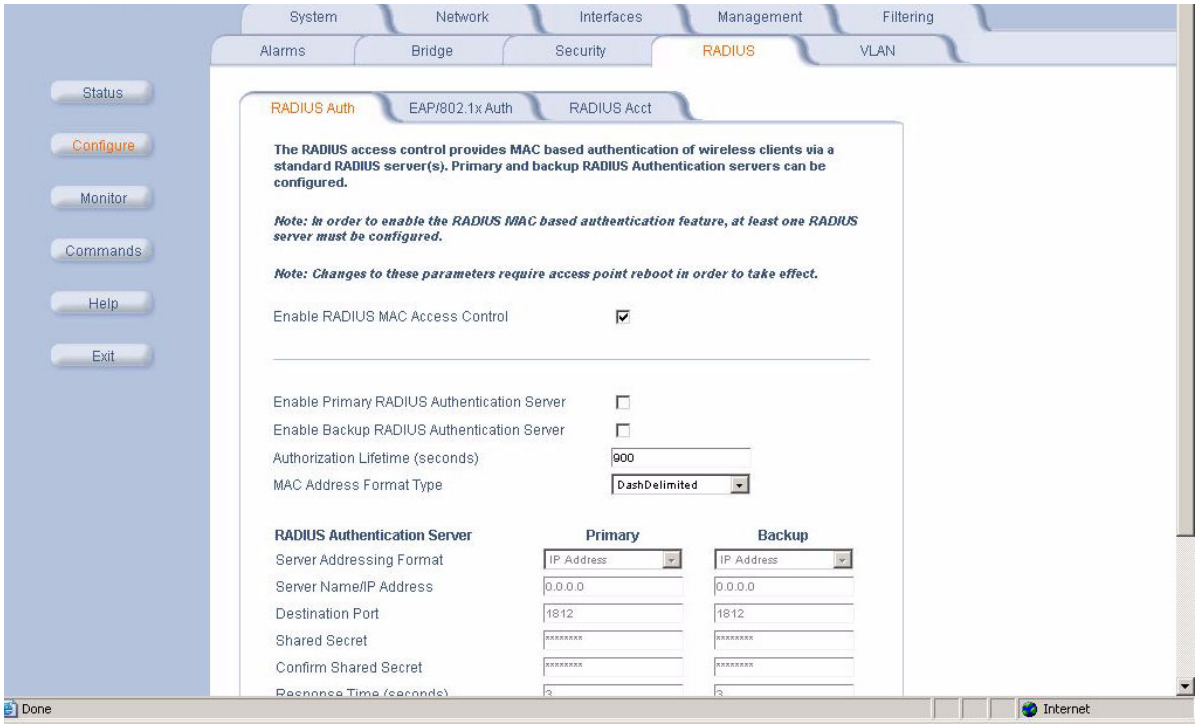


Figure 4-19 RADIUS MAC-Based Access Control Screen

RADIUS Authentication with 802.1x

You must configure a primary EAP/802.1x Authentication server to use 802.1x security. A back-up server is optional.

NOTE

Problems with RADIUS Server configuration or RADIUS Authentication should be referred to the RADIUS Server developer.

Follow these steps to enable a RADIUS Authentication server for 802.1x security:

1. Click the **RADIUS** tab.
2. Click the **EAP/802.1x Auth** sub-tab.
3. Place a check mark in the box labeled **Enable Primary EAP/802.1x Authentication Server**.

4. If you want to configure a back-up RADIUS server, place a check mark in the box labeled **Enable Backup EAP/802.1x Authentication Server**.
5. Select a **Server Addressing Format** type (IP Address or Name).
   - If you want to identify RADIUS servers by name, you must configure the AP as a DNS Client. See DNS Client for details.
6. Enter the server's IP address or name in the field provided.
7. Enter the port number which the AP and the server will use to communicate. By default, RADIUS servers communicate on port 1812.
8. Enter the Shared Secret in the **Shared Secret** and **Confirm Shared Secret** field. This is a password shared by the RADIUS server and the AP. The same password must also be configured on the RADIUS server.
9. Enter the maximum time, in seconds, that the AP should wait for the RADIUS server to respond to a request in the **Response Time** field. Range is 1-10 seconds; default is 3 seconds.
10. Enter the maximum number of times an authentication request may be retransmitted in the **Maximum Retransmissions** field. Range is 1-4; default is 3.
11. If you are configuring a back-up server, repeat Steps 7 through 12 for the back-up server.
12. Click **OK** to save your changes.
13. Reboot the AP device for these changes to take effect.

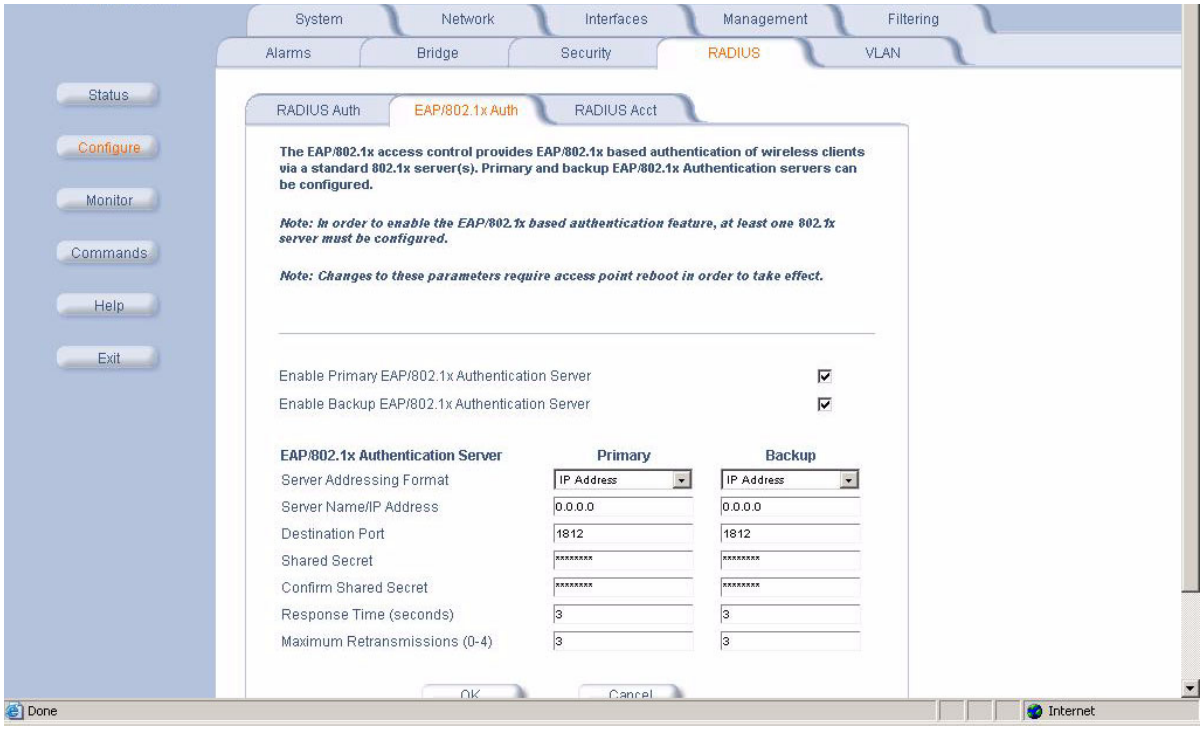


Figure 4-20 RADIUS EAP/802.1x Authentication Screen

RADIUS Accounting

Using an external RADIUS server, the AP can track and record the length of client sessions on the access point by sending RADIUS accounting messages per RFC2866. When a wireless client is successfully authenticated, RADIUS accounting is initiated by sending an “Accounting Start” request to the RADIUS server. When the wireless client session ends, an “Accounting Stop” request is sent to the RADIUS server.

Session Length

Accounting sessions continue when a client reauthenticates to the same AP. Sessions are terminated when:

- A client disassociates.
- A client does not transmit any data to the AP for a fixed amount of time.
- A client is detected on a different interface.

If the client roams from one AP to another, one session is terminated and a new session is begun.

NOTE

This feature requires RADIUS authentication using MAC Access Control or 802.1x. Wireless clients configured in the Access Point’s static MAC Access Control list are not tracked.

Configuring RADIUS Accounting

Follow these steps to enable RADIUS accounting on the AP:

1. Within the ***RADIUS Accounting Configuration*** screen, place a check mark in the **Enable RADIUS Accounting** box to turn on this feature.
2. Place a check mark in the box labeled **Enable Primary RADIUS Accounting Server**.
3. If you want to configure a back-up RADIUS server, place a check mark in the box labeled **Enable Back-up RADIUS Accounting Server**.
4. Enter the session timeout interval in minutes within the **Accounting Inactivity Timer** field. An accounting session automatically ends for a client that is idle for the period of time specified. Range is 1-60 minutes; default is 5 minutes.
5. Select a **Server Addressing Format** type (IP Address or Name).
   - If you want to identify RADIUS servers by name, you must configure the Access Point as a DNS Client. See DNS Client for details.
6. Enter the server’s IP address or name in the field provided.
7. Enter the port number which the AP and the server will use to communicate. By default, RADIUS accounting uses port 1813.
8. Enter the Shared Secret in the **Shared Secret** and **Confirm Shared Secret** field. This is a password shared by the RADIUS server and the AP. The same password must also be configured on the RADIUS server.
9. Enter the maximum time, in seconds, that the AP should wait for the RADIUS server to respond to a request in the **Response Time** field. Range is 1-10 seconds; default is 3 seconds.
10. Enter the maximum number of times an authentication request may be retransmitted in the **Maximum Retransmissions** field. Range is 1-4; default is 3.
11. If you are configuring a back-up server, repeat Steps 5 through 10 for the back-up server.
12. Click **OK** to save your changes.
13. Reboot the AP device for these changes to take effect.

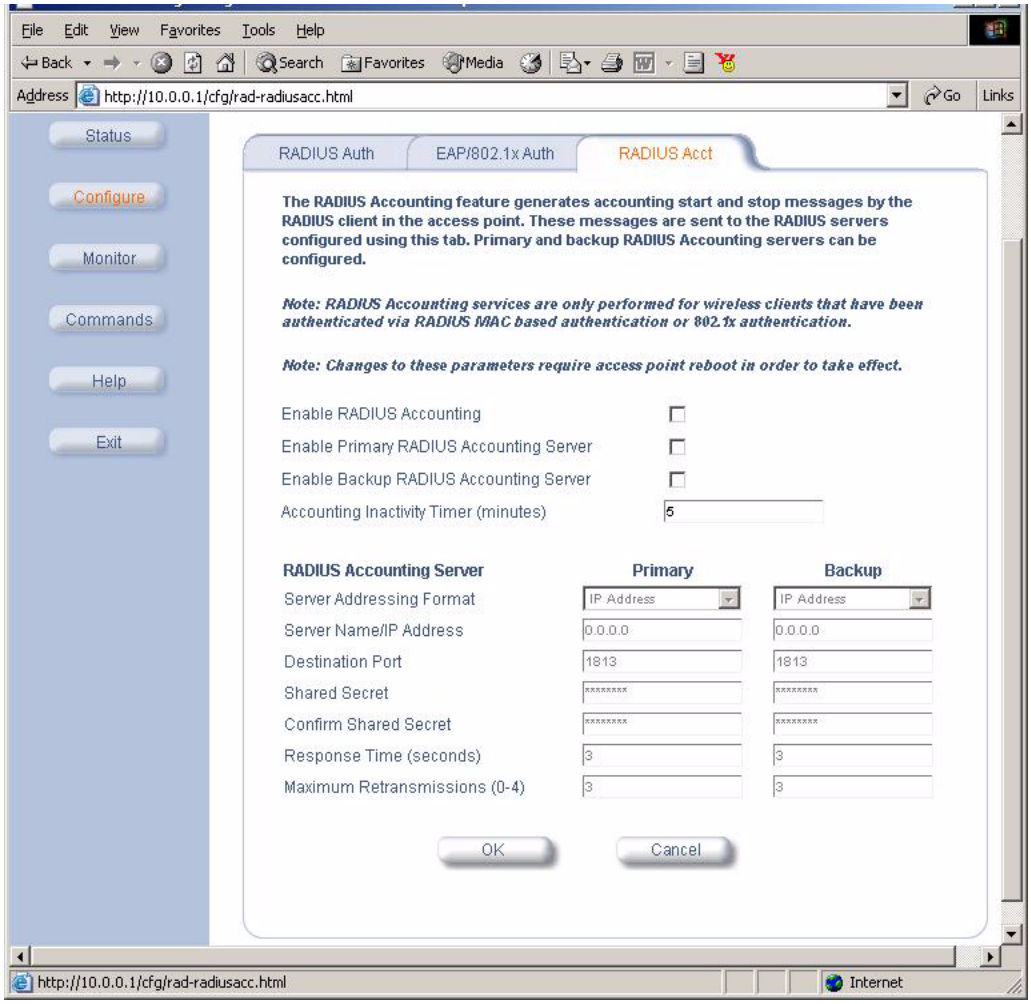


Figure 4-21 RADIUS Accounting Server Configuration

VLAN/SSID

The AP allows you to segment wireless networks into multiple sub-networks based on Network Name (SSID) and VLAN membership.

A Network Name (SSID) identifies a wireless network. Clients associate with Access Points that share its SSID. During installation, the Setup Wizard prompts you to configure one Network Name for each wireless interface. After initial setup, the AP can be configured to support up to 16 SSIDs per wireless interface to segment wireless networks based on VLAN membership.

NOTE

16 VLAN/SSID pairs are available for APs with an HP ProCurve Wireless 802.11g AP Card 170wl only.

VLAN Overview

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to clients) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify traffic flow between clients and their frequently-used or restricted resources.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks by way of SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

AP devices are fully VLAN-ready; however, by default VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured, and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

Once enabled, VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
  - Improve network performance and reduce latency
- Increase security
  - Secure network restricts members to resources on their own VLAN
  - Clients roam without compromising security

VLAN tagged data is collected and distributed through an AP's wireless interface(s) based on Network Name (SSID). An Ethernet port on the access point connects a wireless cell or network to a wired backbone. The access points communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports. On the wired network, a RADIUS server authenticates traffic and a DHCP server manages IP addresses for the VLAN(s). Resources like servers and printers may be present, and a hub may include multiple APs, extending the network over a larger area.

In this figure, the numbered items correspond to the following components:

1. VLAN-enabled access point
2. VLAN-aware switch (IEEE 802.1Q uplink)
3. AP management by way of wired host (SNMP, Web interface or CLI)
4. DHCP Server
5. RADIUS Server
6. VLAN 1
7. VLAN 2

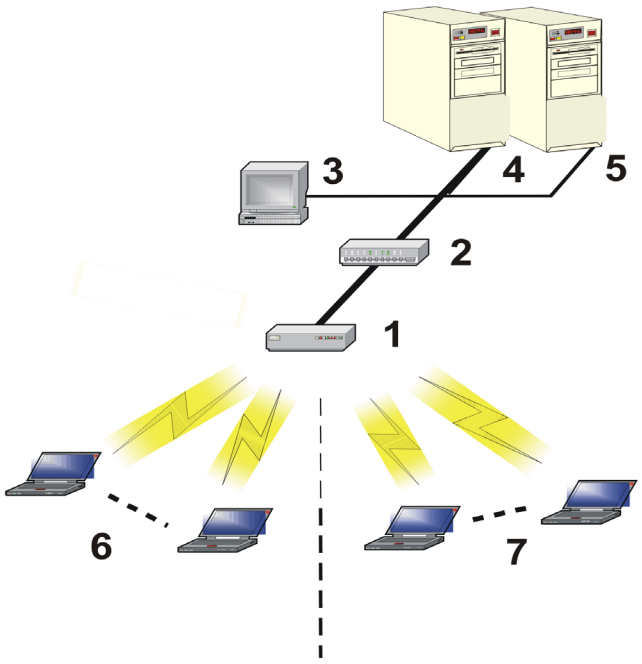


Figure 4-22 Components of a typical VLAN

VLAN Workgroups and Traffic Management

Access Points that are not VLAN-capable typically transmit broadcast and multicast traffic to all wireless Network Interface Cards (NICs). This process wastes wireless bandwidth and degrades throughput performance. In comparison, VLAN-capable AP is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 16 VLAN/SSID pairs per radio (based on model type).

NOTE

16 VLAN/SSID pairs are available for APs with an HP ProCurve Wireless 802.11g AP Card 170wl only.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

Traffic Management

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a workgroup; for example, one VLAN could be used for an EMPLOYEE workgroup and the other, for a GUEST workgroup.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as EMPLOYEE or GUEST, depending on which wireless NIC received it. The AP would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the EMPLOYEE workgroup to the appropriate corporate resources such as printers and servers. Packets from the GUEST workgroup could be restricted to a gateway that allowed access to only the Internet. A member of the GUEST workgroup could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

Typical User VLAN Configurations

VLANs segment network traffic into workgroups, which enable you to limit broadcast and multicast traffic. Workgroups enable clients from different VLANs to access different resources using the same network infrastructure. Clients using the same physical network are limited to those resources available to their workgroup.

The AP can segment users into a maximum of 16 different workgroups (32 if using two cards in a Dual-radio AP) based on an SSID/VLAN pair (also referred as a VLAN Workgroup or a Sub-network).

NOTE

16 VLAN/SSID pairs are available for APs with an HP ProCurve Wireless 802.11g AP Card 170wl only.

The four primary scenarios for using VLAN workgroups are as follows:

1. VLAN disabled: Your network does not use VLANs, but you can configure the AP to use multiple SSIDs.
2. VLAN enabled, all VLAN Workgroups use the same VLAN ID Tag
3. VLAN enabled, each VLAN workgroup uses a different VLAN ID Tag
4. VLAN enabled, a mixture of Tagged and Untagged workgroups

Configure Multiple VLAN/SSID Pairs

NOTE

You must reboot the AP before any changes to these parameters take effect.

1. Click **Configure** > **VLAN**.
2. Place a check mark in the **Enable VLAN Protocol** box to enable VLAN support.
3. Click the tab for Wireless A or Wireless B (if applicable).
4. Add one or more new SSID/VLAN entries. Follow these steps:

NOTE

16 VLAN/SSID pairs are available for APs with an HP ProCurve Wireless 802.11g AP Card 170wl only.

   1. Click **Add** to create a new SSID/VLAN entry.
   2. Enter a **Network Name (SSID)**, between 2 and 31 characters, in the field provided.
   3. Enter a **VLAN ID** in the field provided.
      - As defined by the 802.1Q standard, a VLAN ID is a number between 1 and 4094. A value of -1 means that an entry is "untagged". If 802.1q VLAN tagged packets travel through a Wireless Distribution System (WDS) link, tags are maintained for all traffic coming either from the wired or the wireless side of the network. .
      - You can use the same VLAN ID for all SSIDs if you want all wireless clients to be part of the same VLAN.
      - You can specify a different VLAN ID for each SSID.
      - The VLAN ID must match an ID used by your network; contact your network administrator if you need assistance defining the VLAN IDs.
      - You can set the VLAN ID to "-1" or "untagged" if you do not want clients that are using a specific SSID to be members of a VLAN workgroup.
   4. Click **OK**.
   5. Click the back arrow button to return to the previous screen.
5. Click **Edit** if you want to modify an existing entry. You can also disable or delete an entry from the ***Edit*** screen.
6. Click the tab for the second wireless interface (if applicable) and create/modify SSID/VLAN entries as necessary.
7. Reboot the AP.

Typical VLAN Management Configurations

Control Access to the AP

Management access to the AP can easily be secured by making management stations or hosts and the AP itself members of a common VLAN. Simply configure a non-zero management VLAN ID and enable VLAN to restrict management of the AP to members of the same VLAN.

CAUTION

If a non-zero management VLAN ID is configured then management access to the AP is restricted to wired or wireless hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the AP.

1. Click **Configure** > **VLAN**.
2. Set the **VLAN Management ID** to a value between 0 and 4094 (a value of 0 disables VLAN management).
3. Place a check mark in the **Enable VLAN Protocol** box.

Provide Access to a Wireless Host in the Same Workgroup

The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN User ID, then those wireless clients who are members of that VLAN will have AP management access.

CAUTION

Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.

1. Click **Configure** > **VLAN**.
2. Set the **VLAN Management ID** to use the same VLAN ID as one of the configured SSID/VLAN pairs. See Typical User VLAN Configurations for details.
3. Place a check mark in the **Enable VLAN Protocol** box.

Disable VLAN Management

1. Click **Configure** > **VLAN**.
2. Remove the check mark from the **Enable VLAN Protocol** box (to disable all VLAN functionality) or set the **VLAN Management ID** to 0 (to disable VLAN Management only).

Monitor Information

5

In This Chapter

- Version: Provides version information for the Access Point's system components.
- ICMP: Displays statistics for Internet Control Message Protocol packets sent and received by the AP.
- IP/ARP Table: Displays the AP's IP Address Resolution table.
- Learn Table: Displays the list of nodes that the AP has learned are on the network.
- IAPP: Provides statistics for the Inter-Access Point Protocol messages sent and received by the AP.
- RADIUS: Provides statistics for the configured primary and backup RADIUS server(s).
- Interfaces: Displays the Access Point's interface statistics (Wireless and Ethernet).
- Link Test: Evaluates the link with a wireless client.
- Station Statistics: Displays statistics for stations and Wireless Distribution System links.

Accessing Monitor Features

1. Click the **Monitor** button located on the left-hand side of the screen.

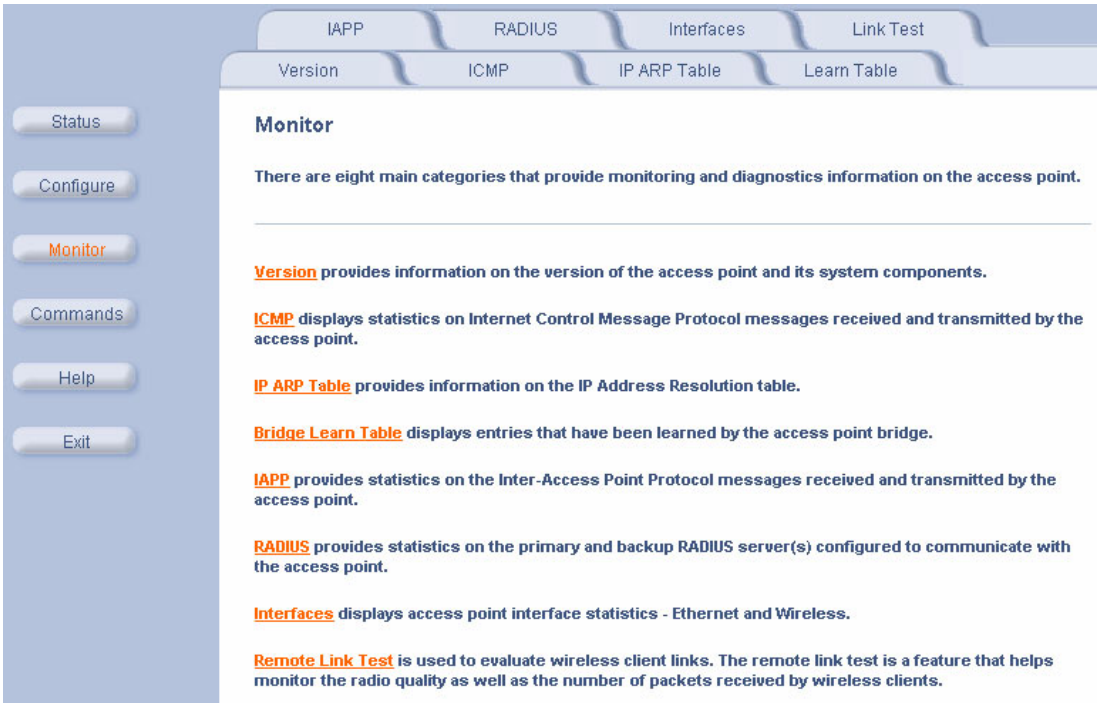


Figure 5-1 Monitor Main Screen

2. Click the tab that corresponds to the statistics you want to review. For example, click **Learn Table** to see the list of nodes that the AP has discovered on the network.
3. If applicable, click the **Refresh** button to update the statistics.

Version

From the HTTP interface, click the **Monitor** button and select the **Version** tab. The list displayed provides you with information that may be pertinent when calling Technical Support. With this information, your Technical Support representative can verify compatibility issues and make sure the latest software are loaded. This screen displays the following information for each Access Point component:

- **Serial Number:** The component's serial number, if applicable.
- **Component Name**
- **ID:** The AP identifies a system component based on its ID. Each component has a unique identifier.
- **Variant:** Several variants may exist of the same component (for example, a hardware component may have two variants, one with more memory than the other).
- **Version:** Specifies the component's version or build number. The Software Image version is the most useful information on this screen for the typical end user.

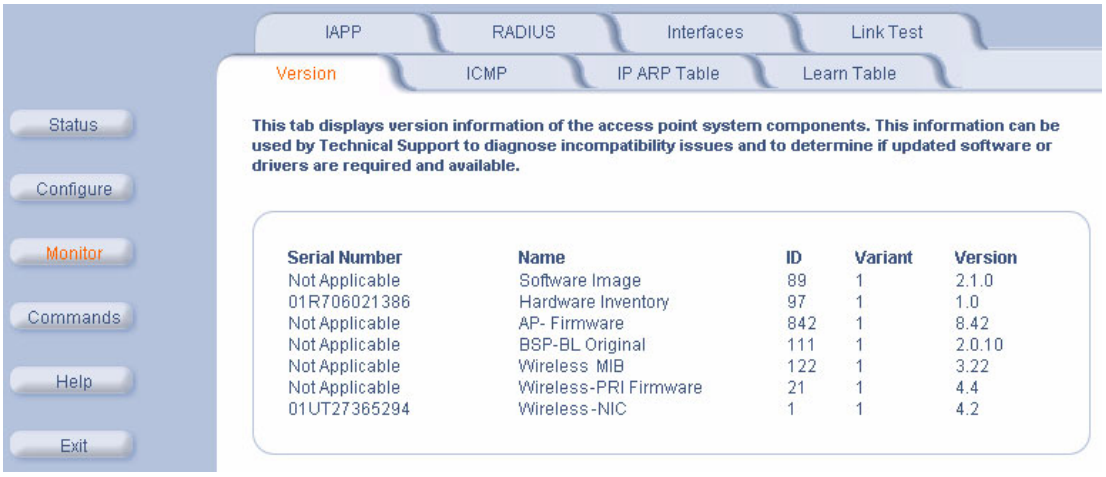


Figure 5-2 Version Information Screen

ICMP

This tab provides statistical information for both received and transmitted messages directed to the AP. Not all ICMP traffic on the network is counted in the ICMP (Internet Control Message Protocol) statistics.

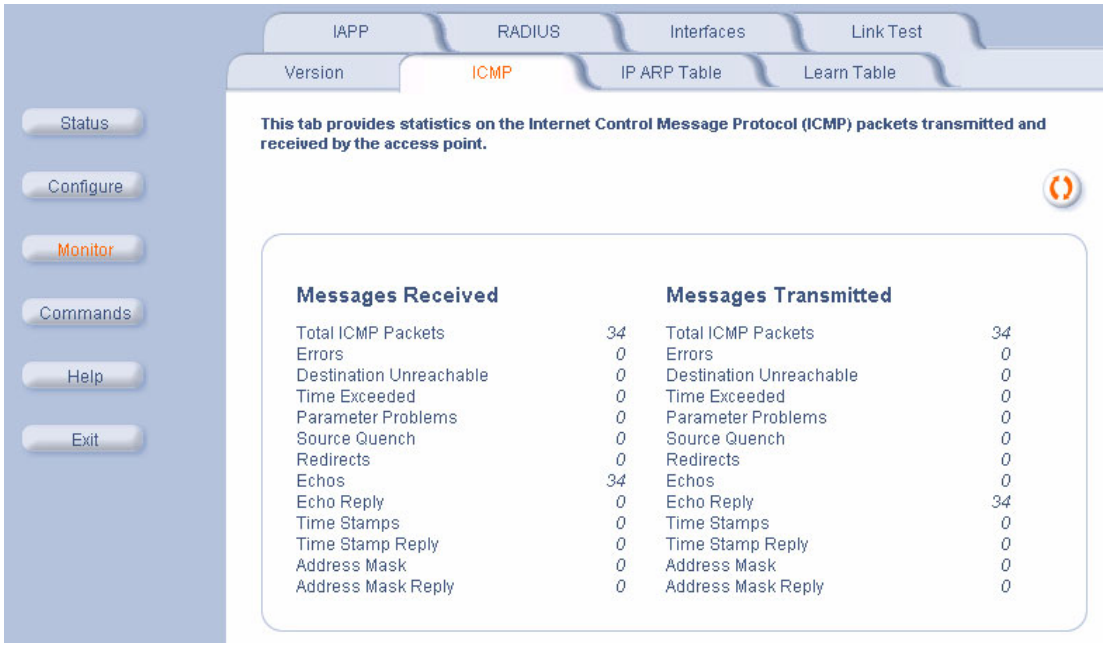


Figure 5-3 ICMP Monitoring Screen

IP/ARP Table

This tab provides information based on the Address Resolution Protocol (ARP), which relates MAC Address and IP Addresses.

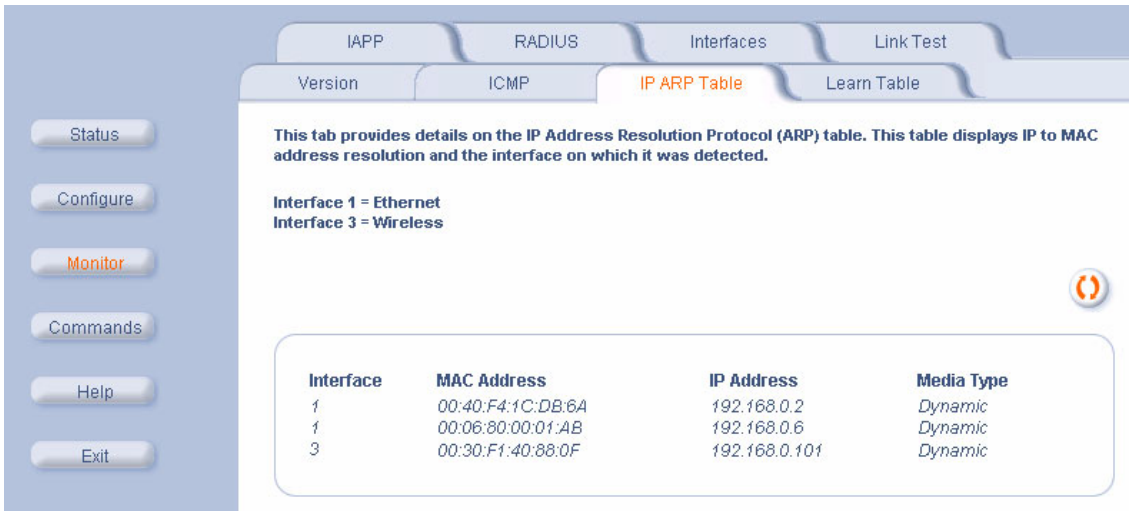


Figure 5-4 IP/ARP Table

Learn Table

This tab displays information relating to network bridging. It reports the MAC address for each node that the device has learned is on the network and the interface on which the node was detected. There can be up 10,000 entries in the Learn Table.

Figure 5-5 Learn Table

IAPP

This tab displays statistics relating to client handovers and communications between Access Points.

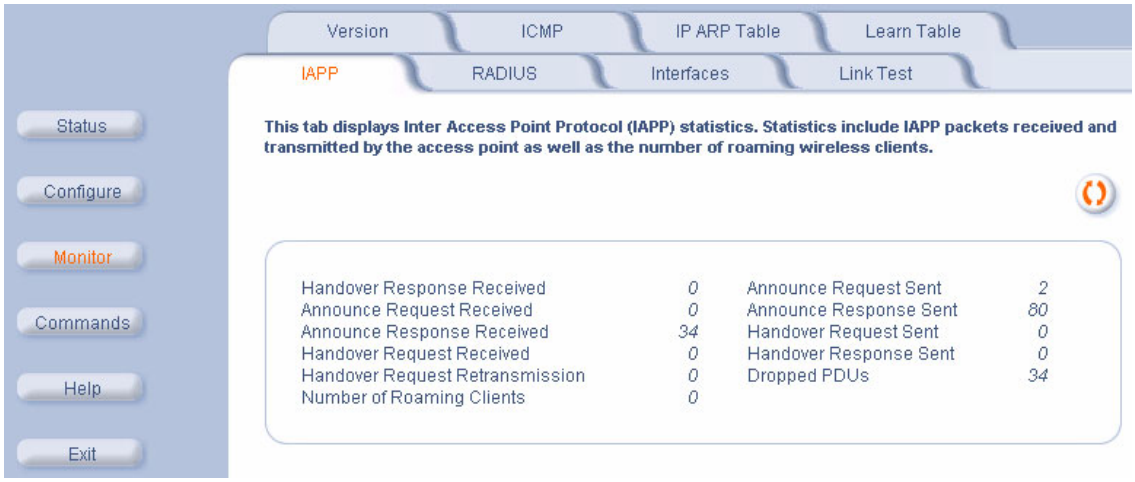


Figure 5-6 IAPP Screen

RADIUS

This tab provides RADIUS authentication, EAP/802.1x authentication, and accounting information for both the Primary and Backup RADIUS servers.

NOTE

RADIUS authentication and accounting must be enabled for this information to be valid.

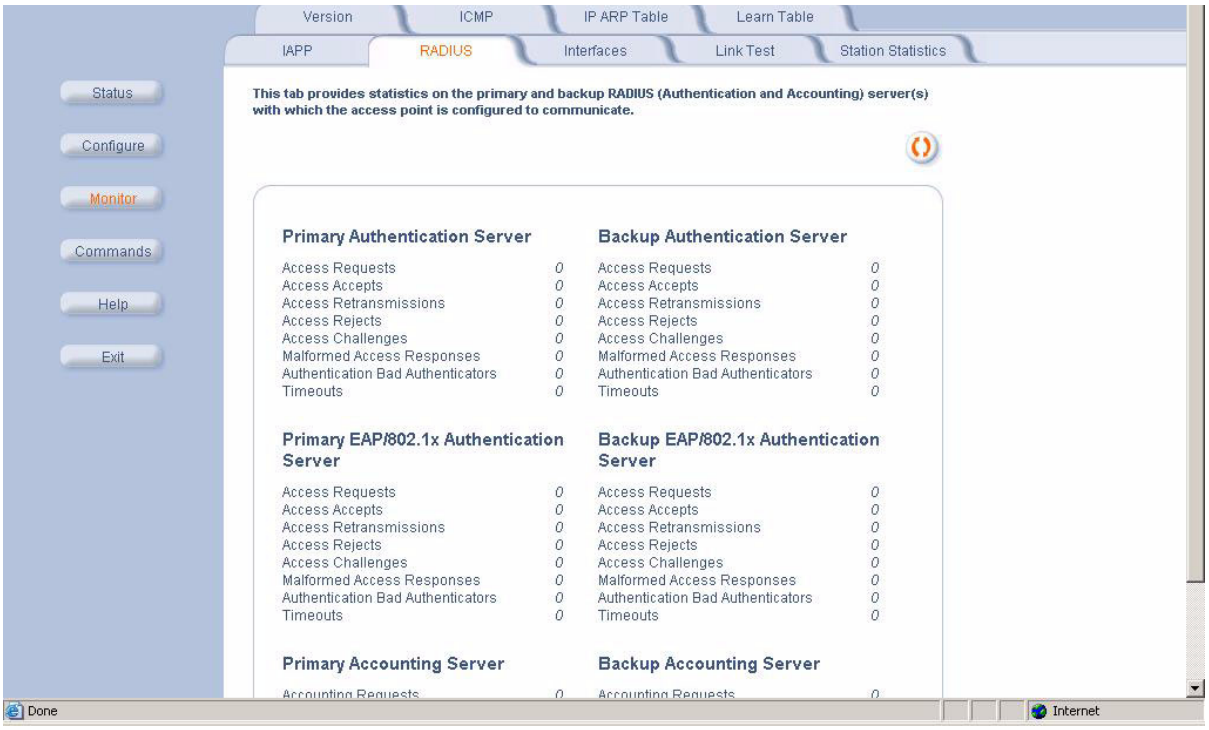


Figure 5-7 RADIUS Monitoring Screen

Interfaces

This tab displays statistics for the Ethernet and wireless interfaces. The Operational Status can be up, down, or testing.

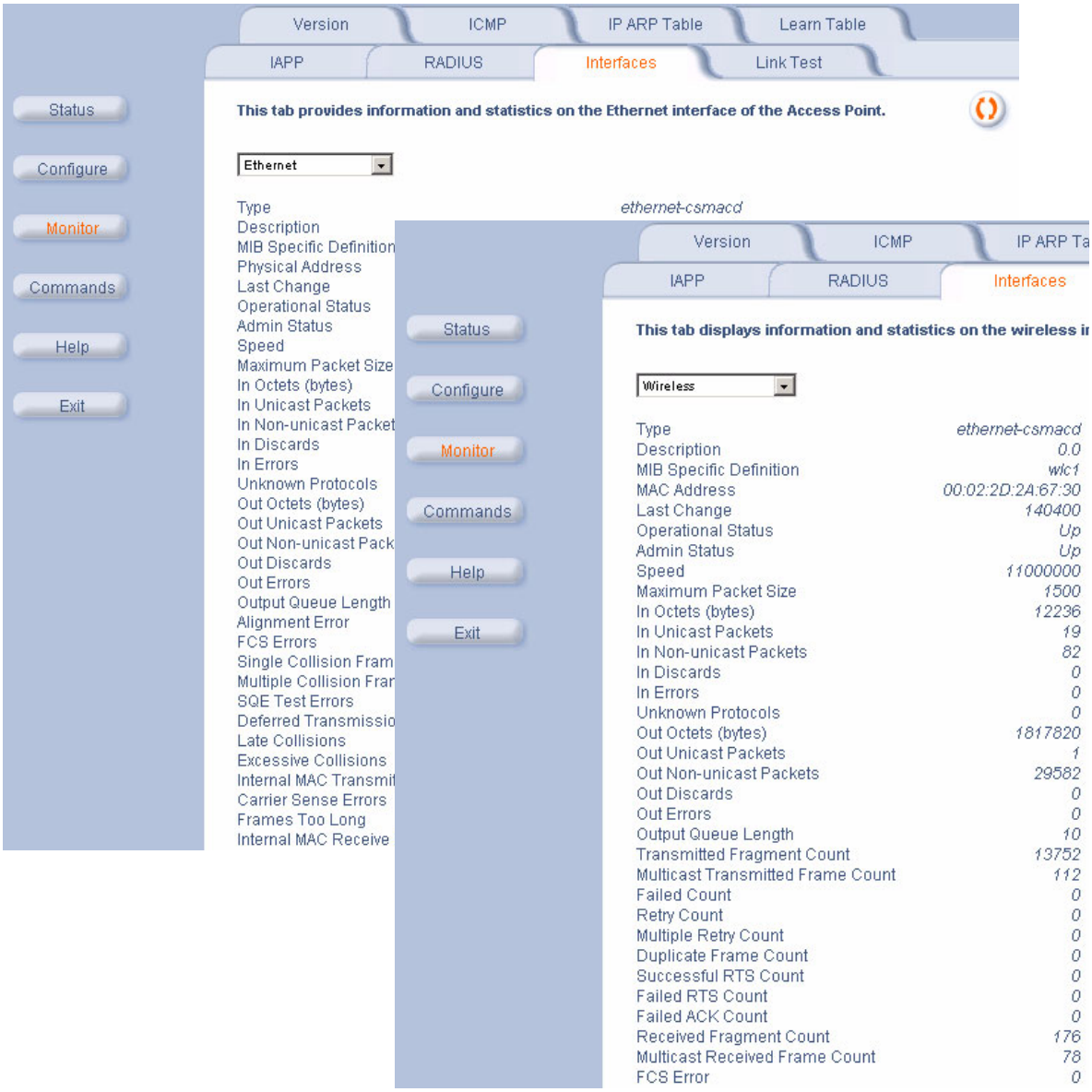


Figure 5-8 Wireless Interface Monitoring

Link Test

This tab displays information on the quality of the wireless link to clients and other APs in the Wireless Distribution System. During a Link Test, the Access Point and the selected device exchange a series of packets to test the strength of the connection. The devices start by exchanging packets at the 11 Mbits/sec rate but fall back to the slower rates if necessary.

NOTE

This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150wl. In addition, this feature will only give information for ORiNOCO/Agere/Lucent based clients.

Follow these steps to perform a Link Test:

1. Open the ***Remote Link Test*** screen.
2. Click **Explore**.
   Result: A list of detected stations will appear. If the list does not appear automatically, click **Refresh** .

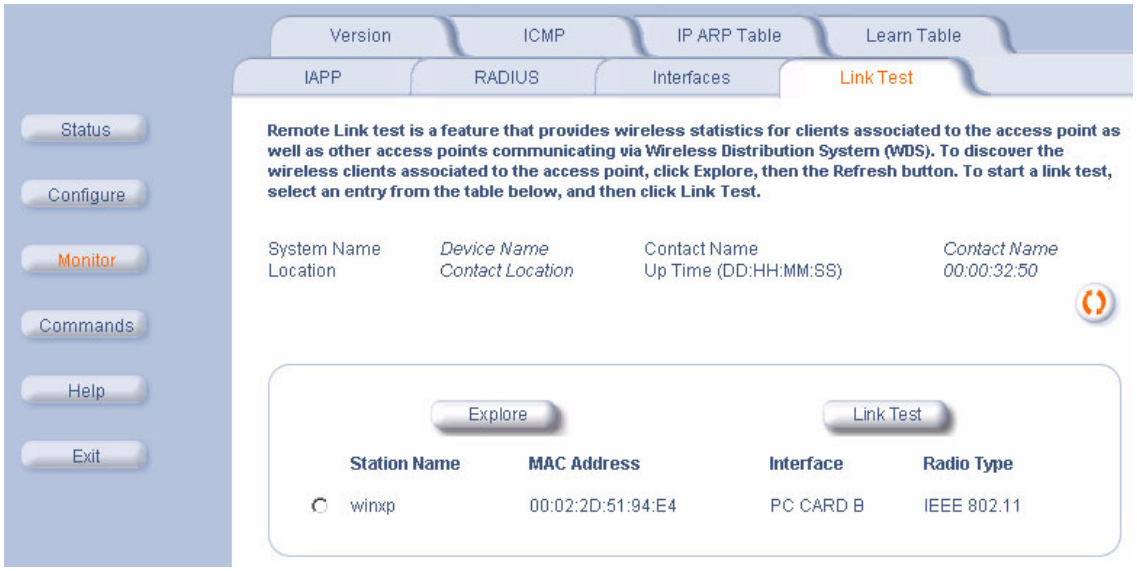


Figure 5-9 Remote Link Test Screen

3. Select a Station from the list by clicking the circle to the left of the Station's entry.
4. Click **Link Test** to start the test.
   Result: A new Link Test window opens and displays the following information for the Access Point (referred to as the **Initiator Station**) and the wireless client (referred to as the **Remote Station**):
   - **Station Name:** The Access Point's System Name or the client's Windows Networking name.
   - **MAC Address:** The station's MAC address.
   - **SNR (dB):** The Signal to Noise ratio for the received signal. The displayed value is the running average since the start of the test and is reported in decibels (dB). Higher numbers correspond to a stronger link. The bar graph also displays the relative strength of the link (a green bar indicates a strong link, a yellow bar indicates a fair link, and a red bar indicates a weak link).
   - **Signal (dBm):** The strength of the received signal in dBm (decibels referenced to 1 milliwatt). The displayed value is the running average since the start of the test and is reported as a negative number. Higher numbers correspond to a stronger link. For example, -40 dBm corresponds to a stronger signal than -50 dBm. The bar graph also displays the relative strength of the signal (a longer bar represents a stronger signal).

- **Noise (dBm):** The strength of the noise detected at the receiver reported in dBm (decibels referenced to 1 milliwatt). The displayed value is the running average since the start of the test and is reported as a negative number. Noise can interfere with the received signal so a smaller noise value corresponds to a stronger link. For example, a noise level of -95 dBm is more desirable than a noise level of -89 dBm. The bar graph displays the relative strength of the noise level (a shorter bar represents a weaker noise level and is more desirable than a longer bar).
- **11 Mbps (pkts):** The number of packets received at the 11 Mbits/sec transmit rate since the start of the Link Test. In general, most packets will be received at the 11 Mbits/sec rate if the devices have a strong link.
- **5.5 Mbps (pkts):** The number of packets received at the 5.5 Mbits/sec transmit rate since the start of the Link Test.
- **2 Mbps (pkts):** The number of packets received at the 2 Mbits/sec transmit rate since the start of the Link Test.
- **1 Mbps (pkts):** The number of packets received at the 1 Mbits/sec transmit rate since the start of the Link Test.

NOTE

Click the **Refresh** button periodically to update the test results. The test screen does not refresh automatically.

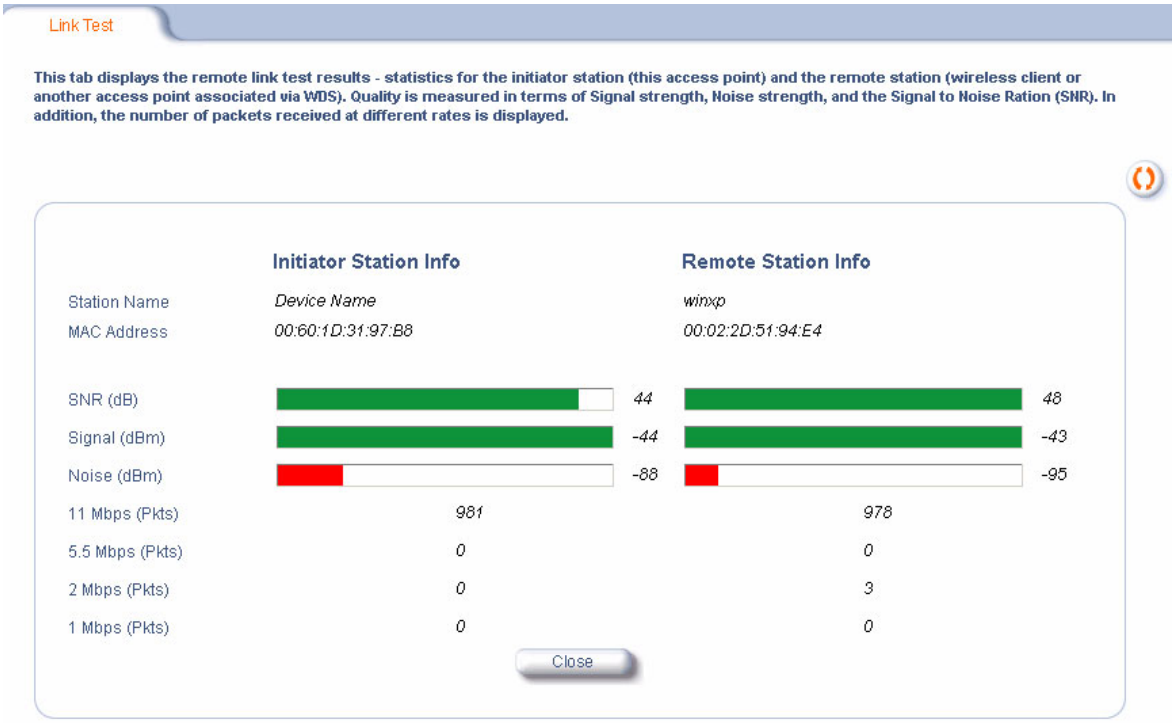


Figure 5-10 SNR Report Screen

5. Click **Close** to end the Link Test.

Station Statistics

This tab displays information on wireless clients attached to the AP and on Wireless Distribution System links.

Enabling and Viewing Station Statistics

To enable the monitoring of Stations Statistics, perform the following procedure:

1. Click on the **Monitor** tab on the left on the web page.
2. Click on the **Station Statistics** tab on the Monitor screen.
3. Enable the Monitoring Station Statistics feature (Station Statistics are disabled by default) by checking **Enable Monitoring Station Statistics** and click **OK**.

You do not need to reboot the AP for the changes to take effect. If clients are connected to the device or WDS links are configured for the device, the statistics will now be shown on the screen.

Refreshing Station Statistics

Click on the **Refresh** button in the browser window to view the latest statistics. If any new clients associate to the AP, you can see the statistics of the new clients after you click the refresh button.

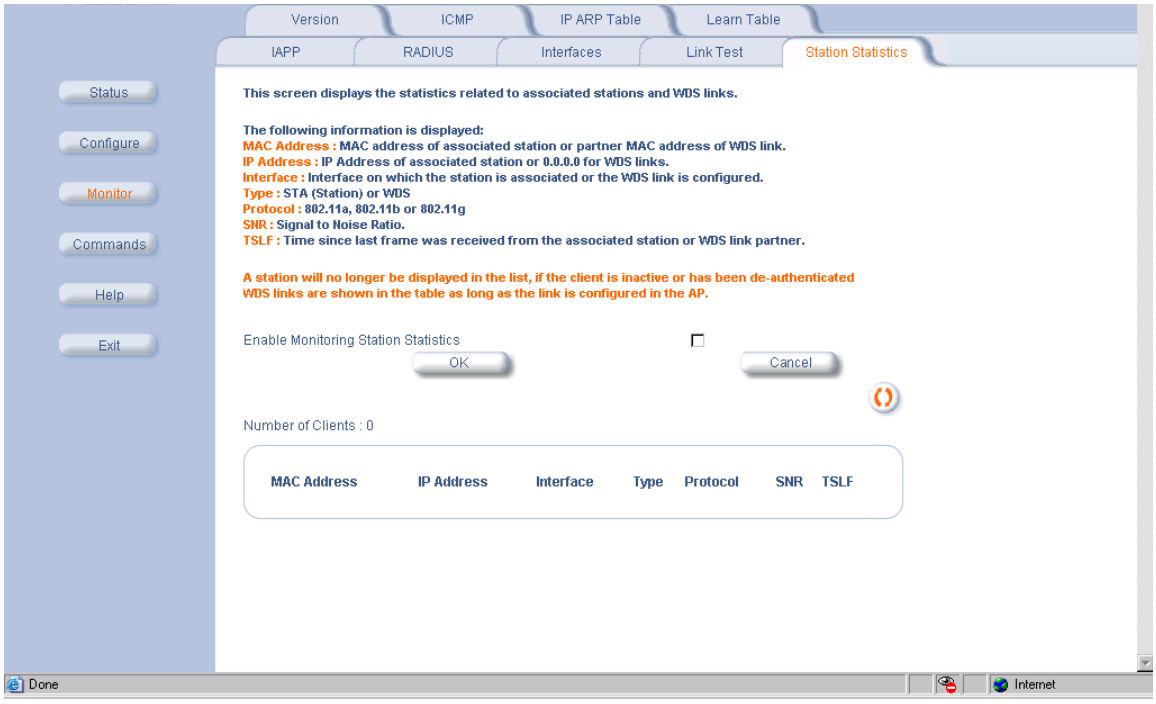


Figure 5-11 Station Statistics Screen

Description of Station Statistics

The following stations statistics are displayed:

- **MAC Address**: The MAC address of the wireless client for which the statistics are gathered. For WDS links, this is the partner MAC address of the link.
- **IP Address**: The IP address of the associated wireless station for which the Statistics are gathered. (0.0.0.0 for WDS links)
- **Interface to which the Station is connected**: The interface number on which the client is connected with the AP. For WDS links this is the interface on which the link is configured.
- **Station Type**: The type of wireless client (STA or WDS).

Monitor Information

- **MAC Protocol**: The MAC protocol for this wireless client (or WDS link partner). The possible values are 802.11a, 802.11b, 802.11g
- **Signal / Noise**: The Signal /Noise Level measured at the AP when frames are received from the associated wireless station (or WDS link partner)
- **Time since Last Packet Received**: The time elapsed since the last frame from the associated wireless station (or WDS link partner) was received.
- **Number of Clients**: The number of stations and WDS links monitored.

The following stations statistics are not displayed in the Graphical User Interface, but can be viewed from a MIB browser:

- **Octets Received**: The number of octets received from the associated wireless station (or WDS link partner) by the AP.
- **Unicast Frames Received**: The number of Unicast frames received from the associated wireless station (or WDS link partner) by the AP.
- **Non-Unicast Frames Received**: The number of Non-Unicast frames received (i.e. broadcast or multicast) from the associated wireless station (or WDS link partner) by the AP.
- **Octets Transmitted**: The number of octets sent to the associated wireless station (or WDS link partner) from the AP.
- **Unicast Frames Transmitted**: The number of Unicast frames transmitted to the associated wireless station (or WDS link partner) from the AP.

Commands

6

In This Chapter

- Logging into the HTTP Interface
- Introduction to File Transfer via TFTP or HTTP: Describes the available file transfer methods.
- Update AP via TFTP: Download files from a TFTP server to the AP.
- Update AP via HTTP: Download files to the AP from HTTP.
- Retrieve File via TFTP: Upload configuration files from the AP to a TFTP server.
- Retrieve File via HTTP: Upload configuration files from the AP via HTTP.
- Reboot: Reboot the AP in the specified number of seconds.
- Reset: Reset all of the Access Point's configuration settings to factory defaults.
- Help Link: Configure the location where the AP Help files can be found.

Logging into the HTTP Interface

Once the AP has a valid IP Address and an Ethernet connection, you may use your web browser to issue commands.

The Command Line Interface (CLI) also provides a method for issuing commands using Telnet or a serial connection. This section covers only use of the HTTP Interface. For more information about issuing commands with the CLI, refer to Command Line Interface (CLI).

Follow these steps to view the available commands supported by the AP's HTTP interface:

1. Open a Web browser on a network computer.

NOTE

The HTTP interface supports the following Web browser:

- Microsoft Internet Explorer 6 with Service Pack 1 or later
- Netscape 6.1 or later

2. If necessary, disable the Internet proxy settings. For Internet Explorer users, follow these steps:
   - Select **Tools > Internet Options...**.
   - Click the **Connections** tab.
   - Click **LAN Settings...**.
   - If necessary, remove the check mark from the **Use a proxy server** box.
   - Click **OK** twice to save your changes and return to Internet Explorer.
3. Enter the Access Point's IP address in the browser's **Address** field and press **Enter**.
   - Result: The ***Enter Network Password*** screen appears.
4. Enter the HTTP password in the **Password** field and click **OK**. Leave the **User Name** field blank. (By default, the HTTP password is "public").
   - Result: The ***System Status*** screen appears.

Commands

Figure 6-1 Enter Network Password Screen

5. Click the **Commands** button located on the left-hand side of the screen.

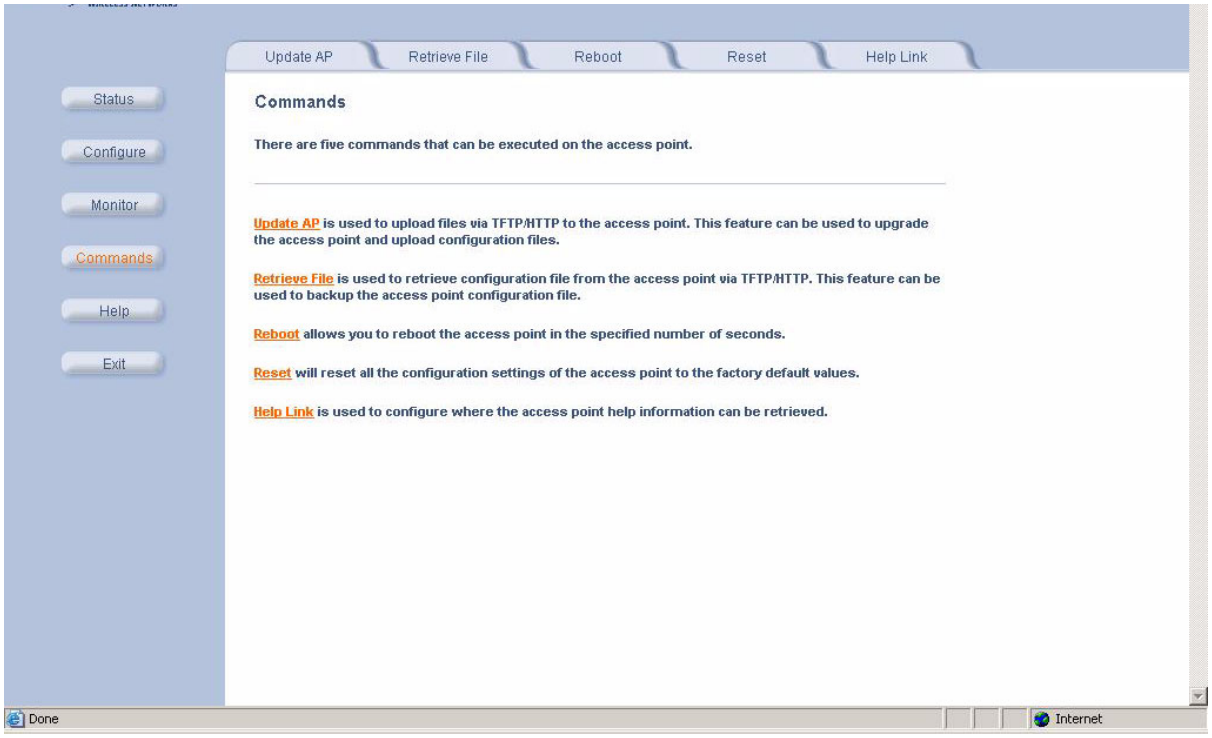


Figure 6-2 Commands Main Screen

6. Click the tab that corresponds to the command you want to issue. For example, click **Reboot** to restart the unit.

Introduction to File Transfer via TFTP or HTTP

There are two methods of transferring files to or from the AP, TFTP or HTTP (or HTTPS if enabled).

The following procedures describe downloading Configuration, AP Image, Bootloader, Private Key, and Certificate files to the AP:

- Update AP via TFTP
- Update AP via HTTP

The following procedures describe uploading Configuration files from the AP:

- Retrieve File via TFTP
- Retrieve File via HTTP

TFTP File Transfer Guidelines

A TFTP server must be running and configured to point to the directory containing the file.

If you do not have a TFTP server installed on your system, install the TFTP server from the CD.

HTTP File Transfer Guidelines

HTTP file transfer can be performed either with or without SSL enabled.

HTTP file transfers with SSL require enabling Secure Management and Secure Socket Layer. HTTP transfers that use SSL may take additional time.

NOTE

SSL requires Internet Explorer version 6, 128 bit encryption, Service Pack 1, and patch Q323308.

Image Error Checking during File Transfer

The Access Point performs checks to verify that an image downloaded through HTTP or TFTP is valid. The following checks are performed on the downloaded image:

- Zero Image size
- Large image size
- Non VxWorks image
- AP image
- Digital signature verification

If any of the above checks fail on the downloaded image, the Access Point deletes the downloaded image and retains the old image. Otherwise, if all checks pass successfully, the AP deletes the old image and retains the downloaded image.

These checks are to ensure that the AP does not enter an invalid image state. The storage of the two images is only temporary to ensure the proper verification; the two images will not be stored in the AP permanently.

Image error checking functions automatically in the background. No user configuration is required.

Update AP via TFTP

Use the **Update AP via TFTP** tab to download Configuration, AP Image, Bootloader files, and Certificate and Private Key files to the AP. A TFTP server must be running and configured to point to the directory containing the file.

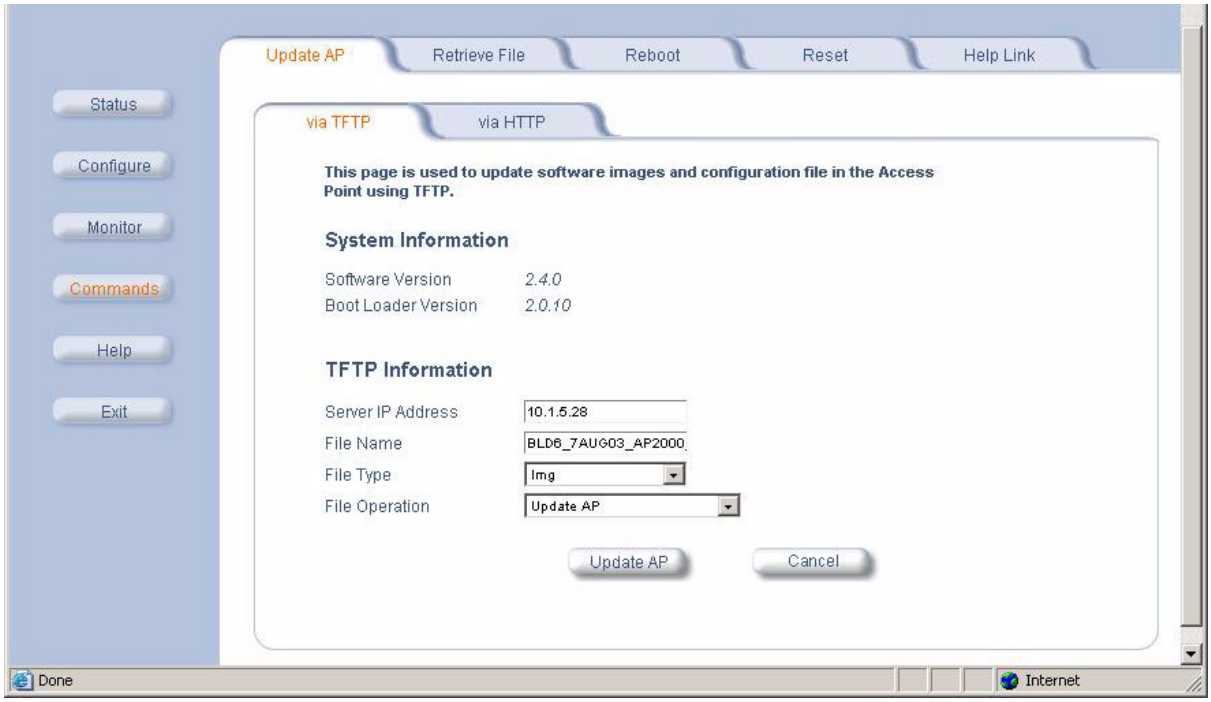


Figure 6-3 Update AP via TFTP Command Screen

If you do not have a TFTP server installed on your system, install the TFTP server from the CD.

The **Update AP via TFTP** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address:** Enter the TFTP server IP Address.
  - Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server. Note: This is the IP address that will be used to point the Access Point to the AP Image file.
- **File Name:** Enter the name of the file to be downloaded (including the file extension).
  - Copy the updated AP Image file to the TFTP server's root folder. The default AP Image is located at c*:/Program Files/HP/AP_520wl/*.
- **File Type:** Select the proper file type. Choices include:
  - **Config** for configuration information, such as System Name, Contact Name, and so on.
  - **Image** for the AP Image (executable program).
  - **BspBl** for the Bootloader software.
  - **Certificate**: the digital certificate for authentication in SSL communications.
  - **Private Key**: the private key for encryption in SSL communications.
- **File Operation:** Select either **Update AP** or **Update AP & Reboot**. You should reboot the AP after downloading files.

Update AP via HTTP

Use the **Update AP via HTTP** tab to download Configuration, AP Image, Bootloader files, and Certificate and Private Key files to the AP.

Once on the Update AP screen, click on the via **HTTP** tab.

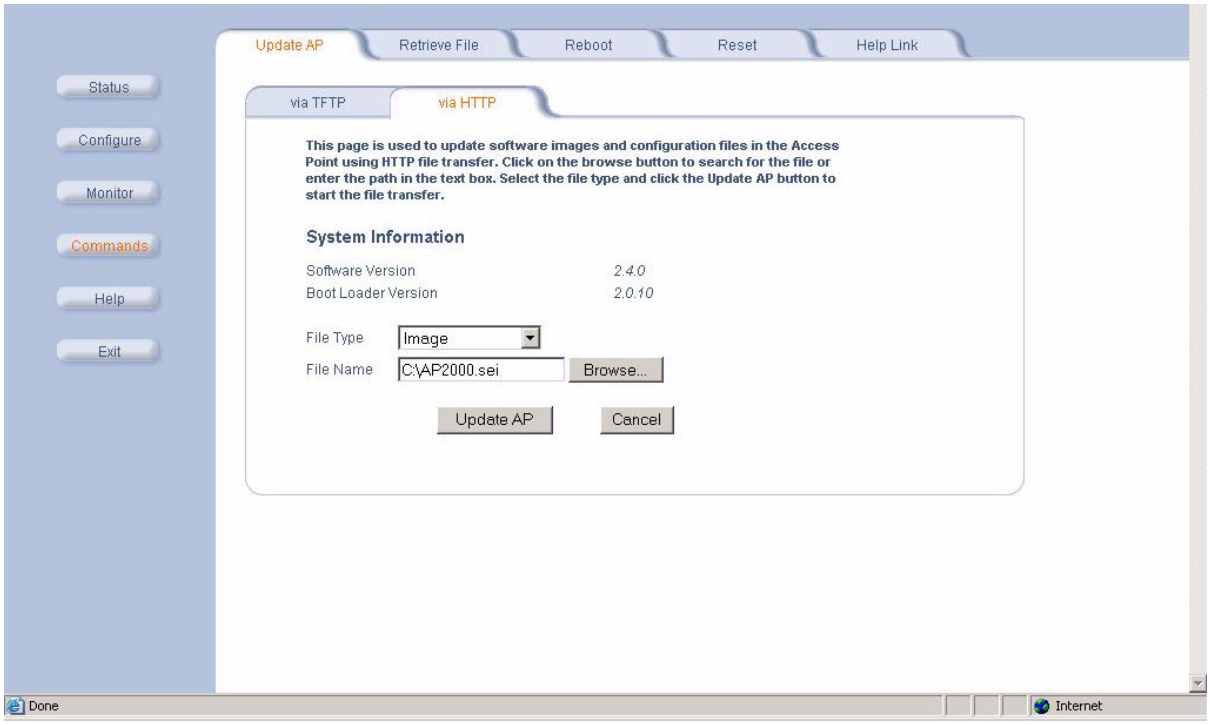


Figure 6-4 Update AP via HTTP Command Screen

The **Update AP via HTTP** tab shows version information and allows you to enter HTTP information as described below.

- Select the File Type that needs to be updated from the drop-down box. Choices include:
  - **Config** for configuration information, such as System Name, Contact Name, and so on.
  - **Image** for the AP Image (executable program).
  - **Bsp/Bl** for the Bootloader software.
  - **Certificate**: the digital certificate for authentication in SSL communications.
  - **Private Key**: the private key for encryption in SSL communications.

Use the **Browse** button or manually type in the name of the file to be downloaded (including the file extension) in the File Name field. If typing the file name, you must include the full path and the file extension in the file name text box.

To initiate the HTTP Update operation, click the **Update AP** button.

A warning message gets displayed that advises the user that a reboot of the device will be required for changes to take effect.

Figure 6-5 Warning Message

Click **OK** to continue with the operation or Cancel to abort the operation.

NOTE

An HTTP file transfer using SSL may take extra time.

If the operation completes successfully the following screen appears.

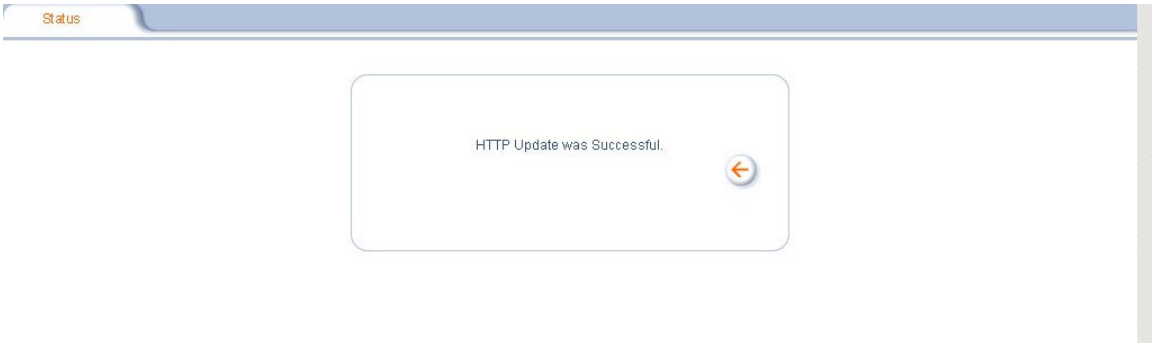


Figure 6-6 Update AP Successful

If the operation did not complete successfully the following screen appears, and the reason for the failure is displayed.

Figure 6-7 Update AP Unsuccessful

Retrieve File via TFTP

Use the **Retrieve File via TFTP** tab to upload Configuration files from the AP to the TFTP server. The TFTP server must be running and configured to point to the directory to which you want to copy the uploaded file. We suggest you assign the file a meaningful name, which may include version or location information.

If you don't have a TFTP server installed on your system, install the TFTP server from the CD.

The **Retrieve AP via TFTP** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address:** Enter the TFTP server IP Address.
  - Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server.
- **File Name:** Enter the name of the file to be uploaded.

NOTE

Use the following procedure to retrieve a Configuration file from an AP to a file:

1. Configure all the required parameters in their respective tabs.
2. Reboot the device.
3. Retrieve and store the Configuration file. Click the **Retrieve Config File** button to initiate the upload of the Configuration file from the AP to the TFTP server.
4. Update the Configuration file as necessary.

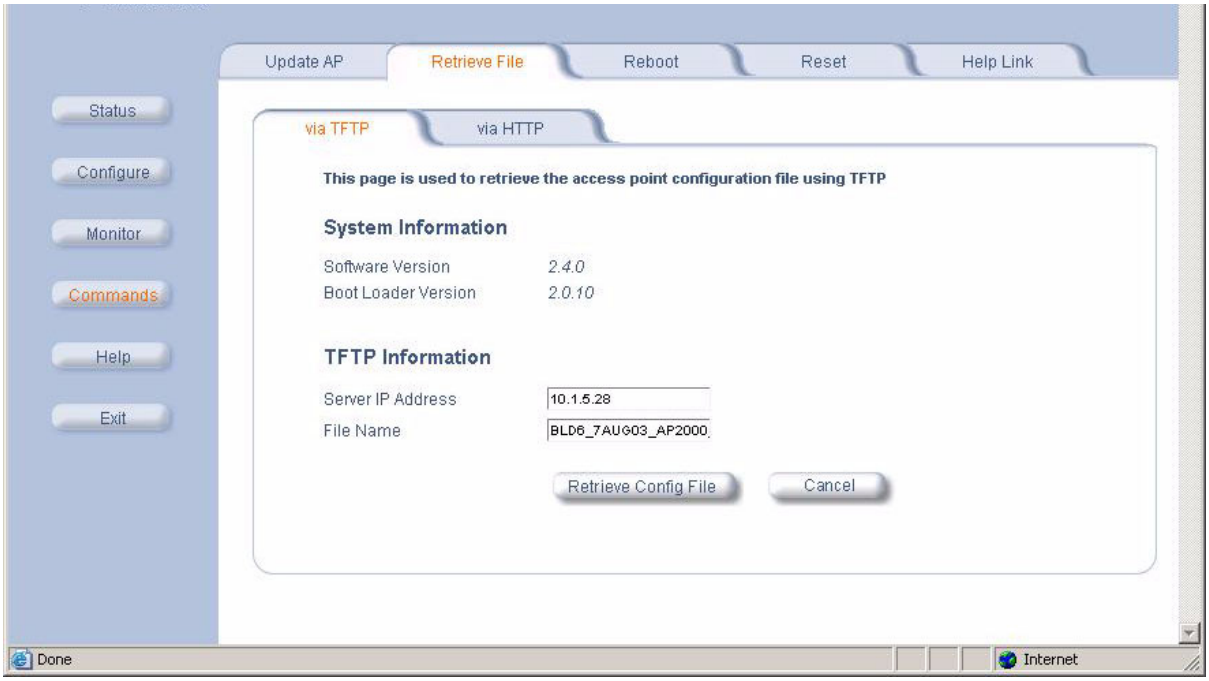


Figure 6-8 Retrieve File via TFTP Command Screen

Retrieve File via HTTP

Use the **Retrieve File via HTTP** tab to retrieve the configuration file from the AP. Click on the **Retrieve Config File** button to initiate this operation.

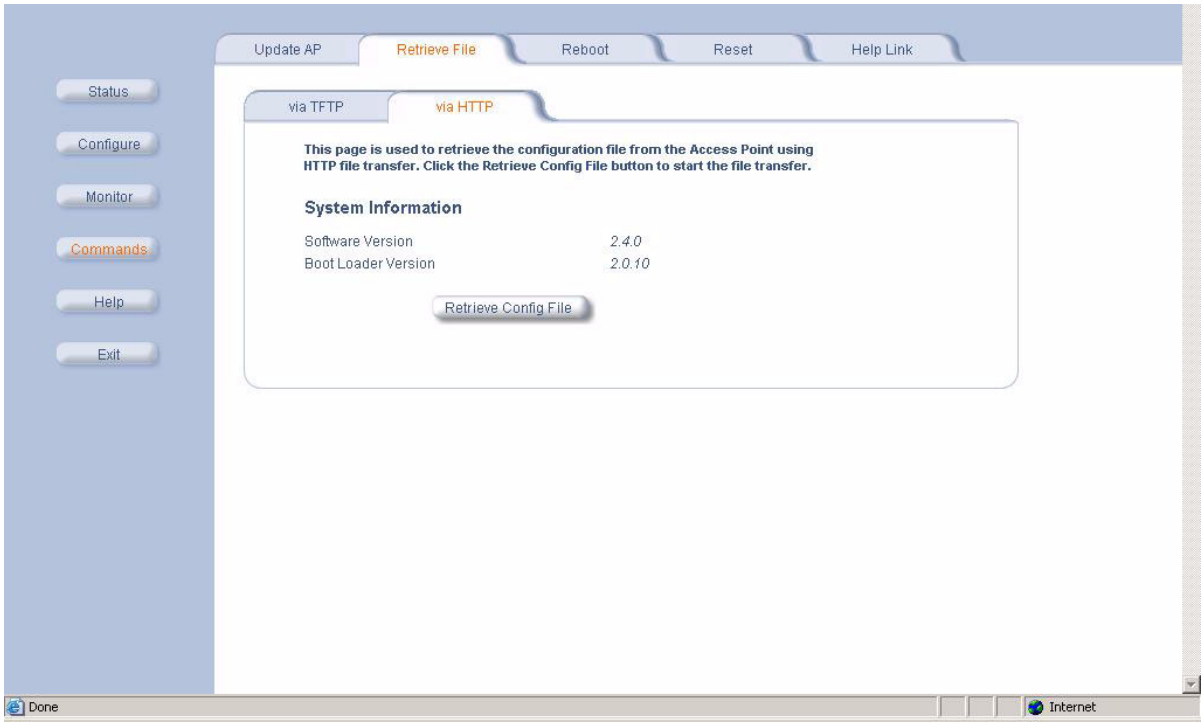


Figure 6-9 Retrieve File via HTTP Command Screen

A confirmation message gets displayed that asks if the user wants to proceed with retrieving the configuration file. Click **OK** to continue with the operation or Cancel to abort the operation.

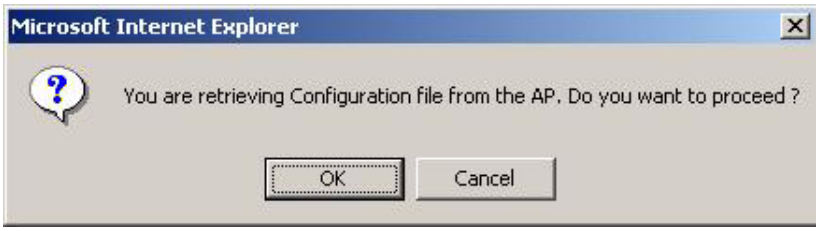


Figure 6-10 Retrieve File Confirmation Dialog

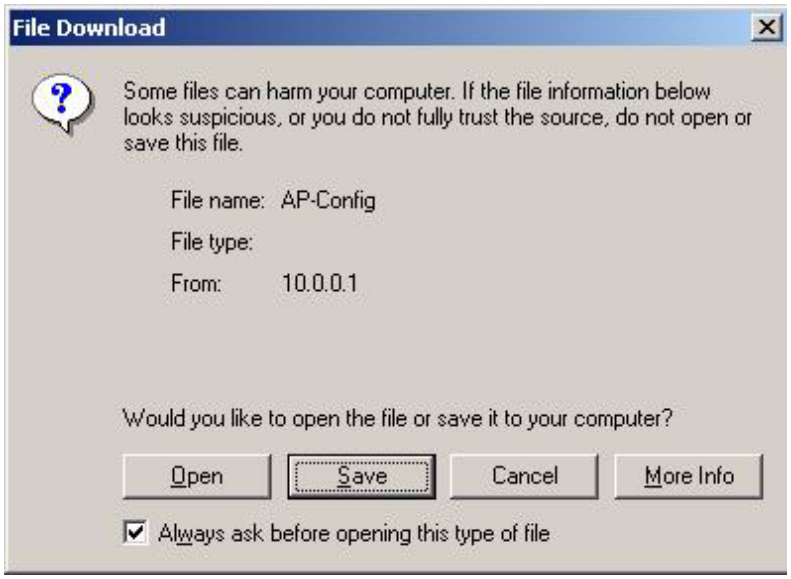


Figure 6-11 File Download Dialog Box

On clicking the **Save** button the following Save As window displays, where the user is prompted to choose the filename and location where the Configuration file is to be downloaded. Select an appropriate filename and location and click **OK**.

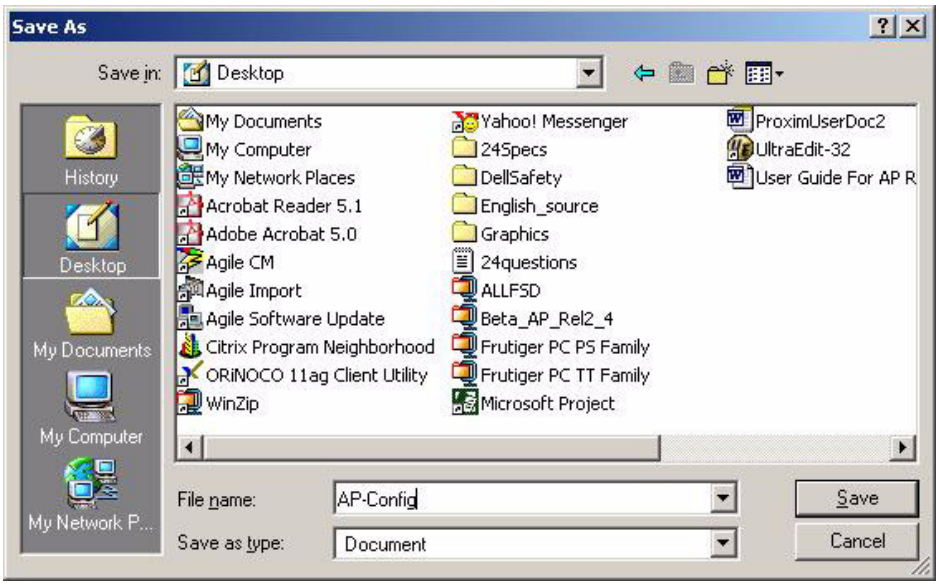


Figure 6-12 Retrieve File Save As Dialog

Reboot

Use the **Reboot** tab to save configuration changes (if any) and reset the AP. Entering a value of 0 (zero) seconds causes an immediate reboot. Note that **Reset**, described below, does not save configuration changes.

CAUTION

Rebooting the AP will cause all users who are currently connected to lose their connection to the network until the AP has completed the restart process and resumed operation.

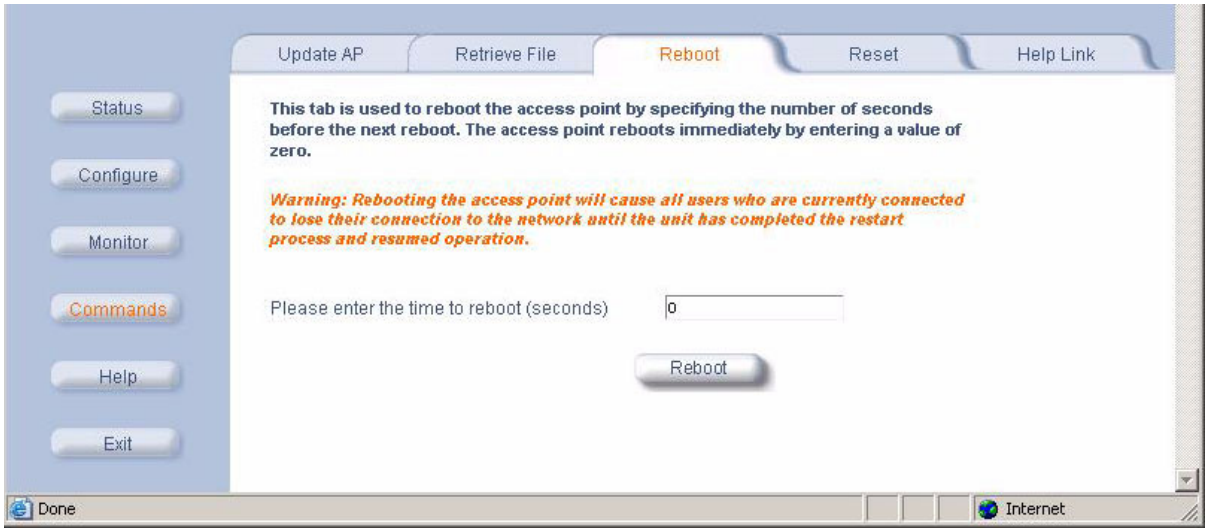


Figure 6-13 Reboot Command Screen

Reset

Use the **Reset** tab to restore the AP to factory default conditions. The AP may also be reset from the **RESET** button located on the side of the unit. Since this will reset the Access Point's current IP address, a new IP address must be assigned. Refer to Recovery Procedures for more information.

CAUTION

Resetting the AP to its factory default configuration will permanently overwrite all changes that have made to the unit. The AP will reboot automatically after this command has been issued.

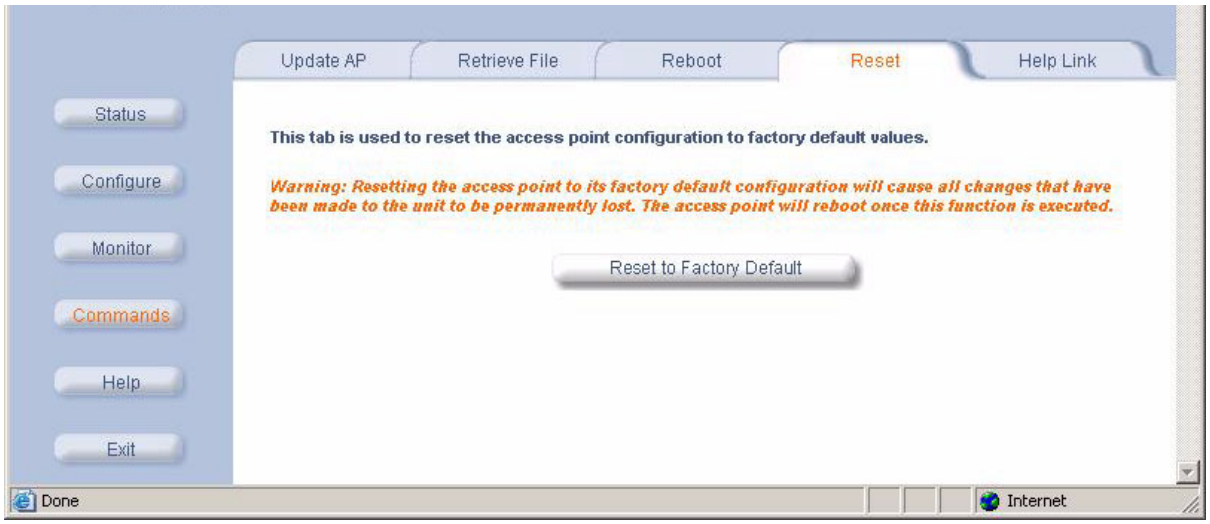


Figure 6-14 Reset to Factory Defaults Command Screen

Help Link

To open **Help**, click the **Help** button on any display screen.

During initialization, the AP on-line help files are downloaded to the default location: **c:/Program Files/HP/AP_520wl/Help/English/index.htm**.

NOTE

Use the forward slash character ("/") rather than the backslash character ("\") when configuring the **Help Link** location.

NOTE

Add the AP's management IP address into the Internet Explorer list of Trusted Sites.

The AP Help information is available in English. The Help files are copied to your computer in one language only.

If you want to place these files on a shared drive, copy the Help Folder to the new location, and then specify the new path in the **Help Link** box.

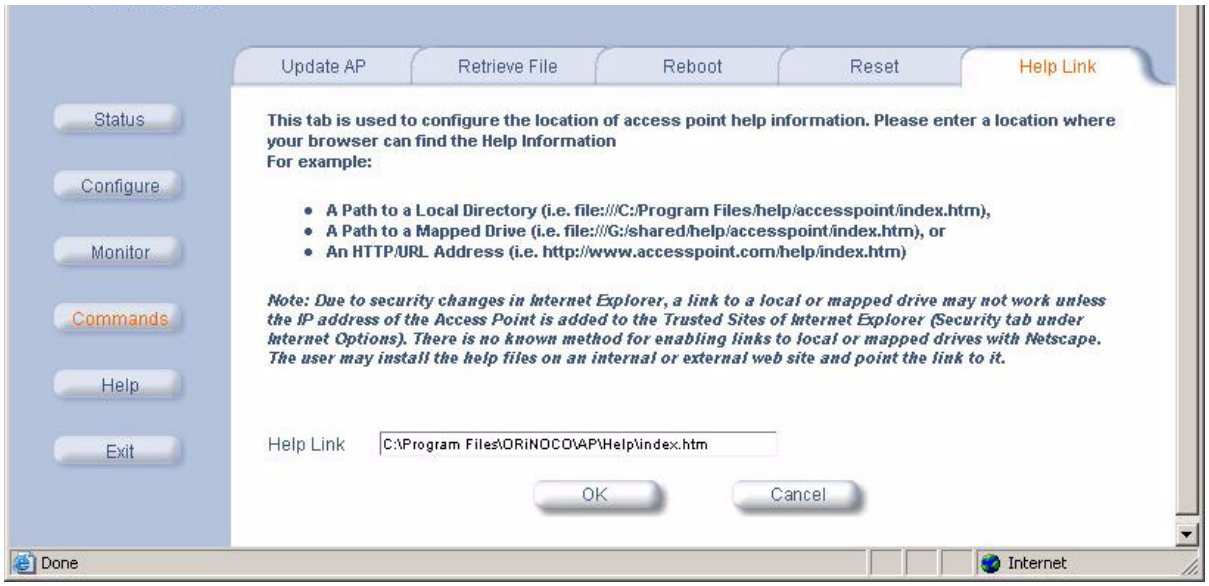


Figure 6-15 Help Link Configuration Screen

Troubleshooting 7

In This Chapter

- Troubleshooting Concepts
- Symptoms and Solutions
- Recovery Procedures
- Related Applications

NOTE

This section helps you locate problems related to the AP device setup. For details about RADIUS, TFTP, serial communication programs (such as HyperTerminal), Telnet applications, or web browsers, please refer to the documentation that came with the application for assistance.

Troubleshooting Concepts

The following list identifies important troubleshooting concepts and topics. The most common initialization and installation problems relate to IP addressing. For example, you must have valid IP addresses for both the AP and the management computer to access the unit's HTTP interface.

- **IP Address management is fundamental.**
- **Factory default units are set for "Dynamic" (DHCP) IP Address assignment.** The default IP address for the AP is 10.0.0.1 if your network does not have a DHCP server. If you connect the AP to a network with an active DHCP server, then use ScanTool to locate the IP address of your unit. If a DHCP server is not active on your subnet, then use ScanTool to assign a static IP address to the unit.
- **The Trivial File Transfer Protocol (TFTP) provides a means to download and upload files.** These files include the AP Image (executable program) and configuration files.
- **If the AP password is lost or forgotten, you will need to reset to default values.** The Reset to Factory Default Procedure resets configuration, but does not change the current AP Image.
- **If all else fails…** Use the Forced Reload Procedure to erase the current AP Image and then download a new image. Once the new image is loaded, use the Reset to Factory Default Procedure to set the unit to factory default values and reconfigure the unit.
- **The AP Supports a Command Line Interface (CLI).** If you are having trouble locating your AP on the network, connect to the unit directly using the serial interface and refer to Command Line Interface (CLI) for CLI command syntax and parameter names.

Symptoms and Solutions

Connectivity Issues

Connectivity issues include any problem that prevents you from powering up or connecting to the AP.

AP Unit Will Not Boot - No LED Activity

1. Make sure your power source is operating.
2. Make sure all cables are connected to the AP correctly.
3. If you are using Active Ethernet, make sure you are using a Category 5, foiled, twisted pair cable to power the AP.

Serial Link Does Not Work

1. Make sure you are using a standard, straight-through, 9-pin serial cable.
2. Double-check the physical network connections.
3. Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values:
   – Com Port: (COM1, COM2, etc. depending on your computer);
   – Baud rate: 9600; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None;
   – Line Feeds with Carriage Returns
   (In HyperTerminal select:
   File -> Properties -> Settings -> ASCII Setup -> Send Line Ends with Line Feeds)

Ethernet Link Does Not Work

1. Double-check the physical network connections. Use a known-good unit to make sure the network connection is present. Once you have the AP IP address, you can use the “Ping” command over Ethernet to test the IP Address. If the AP responds to the Ping, then the Ethernet Interface is working properly.
2. By default, the Access Point will attempt to automatically detect the Ethernet settings. However, if you are having problems with the Ethernet link, manually configure the Access Point’s Ethernet settings. For example, if your switch operates at 100 Mbits/sec/Full Duplex, manually configure the Access Point to use these settings (see Ethernet). If you cannot access the unit over Ethernet, then use the CLI interface over the serial port to configure the Ethernet port (see Command Line Interface (CLI) and Set Ethernet Speed and Transmission Mode).
3. Perform network infrastructure troubleshooting (check switches, routers, etc.).

Basic Software Setup and Configuration Problems

Lost AP, Telnet, or SNMP Password

1. Perform the Reset to Factory Default Procedure in this guide. This procedure resets system and network parameters, but does not affect the AP Image.
   The default AP HTTP password is “public”, and the default Telnet password is also “public”.

Client Computer Cannot Connect

1. Client computers should have the same Network Name and security settings as the AP.
2. Network Names should be allocated and maintained by the Network Administrator.
3. Refer to the documentation that came with your client card for additional troubleshooting suggestions.

AP Has Incorrect IP Address

1. Default IP Address Assignment mode is dynamic (DHCP). If you do not have a DHCP server on your network, the default IP Address is 10.0.0.1. If you have more than one unintialized AP connected to the network, they will all have the same default IP address and you will not be able to communicate with them (due to an IP address conflict). In this case, assign each AP a static IP address by way of the serial cable or turn off all units but one and change the IP address using ScanTool one at a time.

2. The AP only contacts a DHCP server during boot-up. If your network's DHCP server is not available while the AP is booting, the device will retain the last IP Address it had. Reboot the AP once your DHCP server is on-line again or use the ScanTool to find the Access Point's current IP address.
3. To find the unit's current IP address if using DHCP, open the IP Client Table in the DHCP Server and match the Access Point's IP address to its MAC address (found on the product label). Alternatively, use ScanTool to identify an Access Point's current IP address.
4. Once you have the current IP address, use the HTTP or CLI Interface to change the unit's IP settings, if necessary.
5. If you use static IP Address assignments, and cannot access the unit over Ethernet, use the Initializing the IP Address using CLI procedure. Once the IP Address is set, you can use the Ethernet Interface to complete configuration.
6. Perform the Reset to Factory Default Procedure in this guide. This will reset the unit to "DHCP" mode. If there is a DHCP Server on the network, the DHCP Server will assign an IP Address to the AP.

HTTP (browser) or Telnet Interface Does Not Work

1. Make sure you are using a compatible browser:
   - Microsoft Internet Explorer 6 with Service Pack 1 or later
   - Netscape 6.1 or later
2. Make sure you have the proper IP address. Enter your Access Point's IP Address in the browser address bar, similar to this example:
   http://192.168.1.100
   When the ***Enter Network Password*** window appears, leave the **User Name** field empty and enter the HTTP password in the **Password** field. The default HTTP password is "public".
3. Use the CLI over the serial port to check the IP Access Table, which can be restricting access to Telnet and HTTP.

HTML Help Files Do Not Appear

1. Verify that the HTML Help files are installed in the default directory:
   C:/Program Files/HP/AP_520wl/Help/English/Index.htm
2. If the Help files are not located in this folder, contact your network administrator to find out where the Help files are located on your server.
3. Perform the following steps to verify the location or to enter the pathname for the Help files:
   a. Click the **Commands** button in the HTTP interface.
   b. Select the **Help** tab located at the top of the screen.
   c. Enter the pathname where the Help files are located in the **Help Link** box.
   d. Click **OK** when finished.

Telnet CLI Does Not Work

1. Make sure you have the proper IP Address. Enter your **AP** IP address in the Telnet connection dialog, from a DOS prompt, type:
   C:\> telnet <AP IP Address>
2. Confirm that your computer has an IP address in the same IP subnet as your Access Point.
3. Use the CLI over the serial port to check the IP Access Table, which can be restricting access to Telnet and HTTP.

TFTP Server Does Not Work

1. Make sure the TFTP Server has been started.
2. Verify the IP address of the TFTP Server. The server may be local or remote, so long as it has a valid IP address.
3. Configure the TFTP Server to "point" to the folder containing the file to be downloaded (or to the folder in which the file is to be uploaded).
4. Verify that you have entered the proper AP Image file name (including the file extension) and directory path.
5. If you have a problem uploading a file, verify that the TFTP server is configured to allow uploads (typically the default setting is to allow only downloads).

Troubleshooting

Client Connection Problems

Client Software Finds No Connection

Make sure you have configured your client software with the proper Network Name and Security settings. Network Names and WEP Keys are typically allocated and maintained by your network administrator.

Client PC Card Does Not Work

1. Make sure you are using the latest PC Card driver software.
2. Download and install the latest client software.

Intermittent Loss of Connection

1. Make sure you are within range of an active AP.
2. You can check the signal strength using the signal strength gauge on your client software. If you have an 802.11b AP, you can also use the Remote Link Test available in the Access Point's HTTP interface. See Link Test.

Client Does Not Receive an IP Address - Cannot Connect to Internet

1. If the AP is configured as a DHCP server, open the Web-browser Interface and select the **Configure** button and then the **Network** tab to make sure the proper DHCP settings are being used.
2. If you are not using the DHCP server feature on the AP, then make sure that your local DHCP server is accessible from the Access Point's subnet.
3. From the client computer, use the "ping" network command to test the connection with the AP. If the AP responds, but you still cannot connect to the Internet, there may be a physical network configuration problem (contact your network support staff).
4. If using Active Ethernet, make sure you are not using a crossover Ethernet cable between the AP and the hub.

VLAN Operation Issues

Verifying Proper Operation of the VLAN Feature

The correct VLAN configuration can be verified by "pinging" both wired and wireless hosts from both sides of the AP device and the network switch. Traffic can be "sniffed" on both the wired (Ethernet) and wireless (WDS) backbones (if configured). Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the AP.

NOTE

16 VLAN/SSID pairs are available APs with an HP ProCurve Wireless 802.11g AP Card 170wl only.

VLAN Workgroups

The correct VLAN assignment can be verified by pinging the AP to ensure connectivity, by pinging the switch to ensure VLAN properties, and by pinging hosts past the switch to confirm the switch is functional. Ultimately, traffic can be "sniffed" on the Ethernet or WDS interfaces (if configured) using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the user's assigned network name.

What if network traffic is being directed to a nonexistent host?

– All sessions are disconnected, traffic is lost, and a manual override is necessary
– Workaround: you can configure the switch to mimic the nonexistent host

I have just configured the Management ID and now I can't manage the AP?

– Check to ensure your password is correct. If your password is incorrect or all inbound packets do NOT have the correct tag, then a manual override is necessary.

CAUTION

The manual override process disconnects all users and resets all values to factory defaults.

Active Ethernet (AE)

The AP Does Not Work

1. Verify that you are using a standard UTP Category 5 cable.
2. Try a different port on the same AE hub (remember to move the input port accordingly) – if it works, there is probably a faulty port or bad RJ-45 port connection.
3. If possible, try to connect the AP to a different AE hub.
4. Try using a different Ethernet cable – if it works, there is probably a faulty connection over the long cable, or a bad RJ-45 connection.
5. Check power plug and hub.
6. If the Ethernet link goes down, check the cable, cable type, switch, and hub.

There Is No Data Link

1. Verify that the indicator for the port is “on.”
2. Verify that the AE hub is connected to the Ethernet network with a good connection.
3. Verify that the Ethernet cable is Category 5 or better and is less than 100 meters (approximately 325 feet) in length from the Ethernet source to the AP.
4. Try to connect a different device to the same port on the AE hub – if it works and a link is established, there is probably a faulty data link in the AP.
5. Try to re-connect the AP to a different output port (remember to move the input port accordingly) – if it works, there is probably a faulty output or input port in the AE hub or a bad RJ-45 connection.

“Overload” Indications

1. Verify that you are not using a cross-over cable between the AE output port and the AP.
2. Verify that there is no short over any of the twisted pair cables.
3. Move the device into a different output port – if it works, there is probably a faulty port or bad RJ-45 connection.

Recovery Procedures

The most common installation problems relate to IP addressing. For example, without the TFTP server IP Address, you will not be able to download a new AP Image to the AP. IP Address management is fundamental. We suggest you create a chart to document and validate the IP addresses for your system.

If the password is lost or forgotten, you will need to reset the AP to default values. The Reset to Factory Default Procedure resets configuration settings, but does not change the current AP Image.

If the AP has a corrupted software image, follow the Forced Reload Procedure to erase the current AP Image and download a new image.

Reset to Factory Default Procedure

Use this procedure to reset the network configuration values, including the Access Point's IP address and subnet mask. The current AP Image is not deleted. Follow this procedure if you forget the Access Point's password:

1. Press and hold the **RELOAD** button for 10 seconds.

NOTE

See RELOAD and RESET Buttons to identify the buttons. You need to use a pin or the end of a paperclip to press a button.

Result: The AP reboots, and the factory default network values are restored.

2. If not using DHCP, use the ScanTool or CLI over a serial connection to set the IP address, subnet mask, and other IP parameters. See Command Line Interface (CLI) for CLI information.

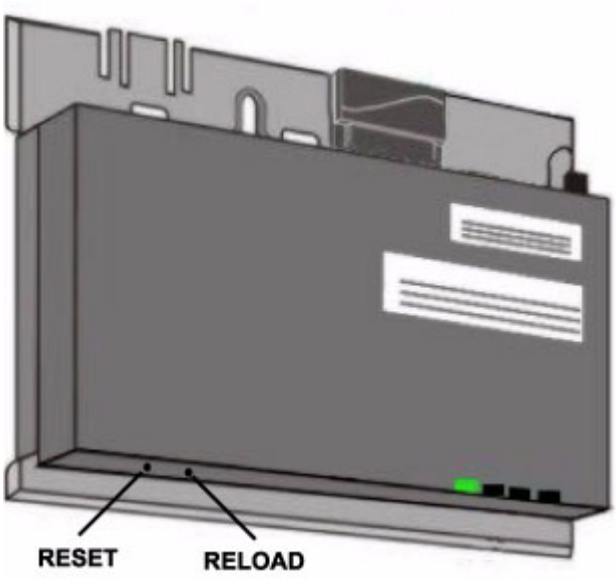


Figure 7-1 RELOAD and RESET Buttons

Forced Reload Procedure

Use this procedure to erase the current AP Image and download a new AP Image. In some cases, specifically when a missing or corrupted AP Image prevents successful booting, you may need to use ScanTool or the Bootloader CLI to download a new executable AP Image.

NOTE

This does not delete the AP's configuration (in other words, the Forced Reload Procedure does not reset to device to factory defaults). If you need to force the AP to the factory default state after loading a new AP image, use the Reset to Factory Default Procedure above.

For this procedure, you will first erase the AP Image currently installed on the unit and then use either ScanTool or the Bootloader CLI (over the serial port) to set the IP address and download a new AP Image. Follow these steps:

1. While the unit is running, press the **RESET** button.

NOTE

See RELOAD and RESET Buttons to identify the buttons. You need to use a pin or the end of a paperclip to press a button.

Result: The AP reboots and the indicators begin to flash.

CAUTION

By completing Step 2, the firmware in the AP will be erased. You will need an Ethernet connection, a TFTP server, and a serial cable (if using the Bootloader CLI) to reload firmware.

2. Press and hold the **RELOAD** button for about 20 seconds until the **POWER LED** turns amber.
   Result: The AP deletes the current AP Image.
3. Follow one of the procedures below to load a new AP Image to the Access Point:
   – Download a New Image Using ScanTool
   – Download a New Image Using the Bootloader CLI

Download a New Image Using ScanTool

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides and to a computer that is running ScanTool (this is either two separate computers connected to the same network or a single computer running both programs).

ScanTool detects if an Access Point does not have a valid software image installed. In this case, the **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's ***Change*** screen so you can download a new image to the unit. (These fields are grayed out if ScanTool does not detect a software image problem.)

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

Follow these steps to use ScanTool to download a software image to an Access Point with a missing image:

1. Download the latest software from http://www.hp.com/go/hpprocurve.
2. Copy the latest software updates to your TFTP server.
3. Launch ScanTool.
4. Highlight the entry for the AP you want to update and click **Change**.
5. Set **IP Address Type** to **Static**.

NOTE

You need to assign static IP information temporarily to the Access Point since its DHCP client functionality is not available when no image is installed on the device.

6. Enter an unused IP address that is valid on your network in the **IP Address** field. You may need to contact your network administrator to get this address.
7. Enter the network's **Subnet Mask** in the field provided.
8. Enter the network's **Gateway IP Address**, if necessary. You may need to contact your network administrator to get this address. You should only need to enter the default gateway address if the Access Point and the TFTP server are separated by a router.
9. Enter the IP address of your TFTP server in the field provided.
10. Enter the **Image File Name** (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need enter only the file name.

11. Click **OK**.
    – Result: The Access Point will reboot and the download will begin automatically. You should see downloading activity begin after a few seconds within the TFTP server's status screen.
12. Click **OK** when prompted that the device has been updated successfully to return to the ***Scan List*** screen.
13. Click **Cancel** to close the ScanTool.
14. When the download process is complete, configure the AP as described in Getting Started and Advanced Configuration.

Download a New Image Using the Bootloader CLI

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN or connected to the AP with a cross-over Ethernet cable.

You must also connect the AP to a computer with a standard serial cable and use a terminal client, such as HyperTerminal. From the terminal, enter CLI Commands to set the IP address and download an AP Image.

Preparing to Download the AP Image

Before starting, you need to know the Access Point's IP address, subnet mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

1. Download the latest software from http://www.hp.com/go/hpprocurve.
2. Copy the latest software updates to your TFTP server's default directory.
3. Use a straight-through serial cable to connect the Access Point's serial port to your computer's serial port.

NOTE

You must remove the Access Point's cable cover and front cover to access the serial port.

4. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, and so forth, depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
5. Under **File -> Properties -> Settings -> ASCII Setup**, enable the **Send line ends with line feeds** option.
   Result: HyperTerminal sends a line return at the end of each line of code.
6. Press the **RESET** button on the AP.
   Result: The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Sending Traps to SNMP manager periodically.** After this message appears, press the **ENTER** key repeatedly until the following prompt appears:

```
[Device name]>
```

7. Enter only the following statements:

   [Device name] > **set ipaddrtype static**

   [Device name] > **set ipaddr <Access Point IP Address>**

   [Device name] > **set ipsubmask <IP Mask>**

   [Device name] > **set tftpipaddr <TFTP Server IP Address>**

   [Device name] > **set tftpfilename <AP Image File Name, including file extension>**

   [Device name] > **set ipgw <Gateway IP Address>**

   [Device name] > **show ip** (to confirm your new settings)

   [Device name] > **show tftp** (to confirm your new settings)

   [Device name] > **reboot 0**

   Example:

   [Device name] > **set ipaddrtype static**

   [Device name] > **set ipaddr 10.0.0.12**

   [Device name] > **set ipsubmask 255.255.255.0**

   [Device name] > **set tftpipaddr 10.0.0.20**

   [Device name] > **set tftpfilename MyImage.bin**

   [Device name] > **set ipgw 10.0.0.30**

   [Device name] > **show ip**

   [Device name] > **show tftp**

   [Device name] > **reboot 0**

   Result: The AP will reboot and then download the image file. You should see downloading activity begin after a few seconds within the TFTP server's status screen.

8. When the download process is complete, configure the AP as described in Getting Started and Advanced Configuration.

Setting IP Address using Serial Port

Use the following procedure to set an IP address over the serial port using the CLI. The network administrator typically provides the AP IP address.

Hardware and Software Requirements

- Standard straight-through serial data (RS-232) cable with a one male DB-9 connector and one female DB-9 connector. The AP comes with a female 9-pin serial port.
- ASCII Terminal software, such as HyperTerminal.

Attaching the Serial Port Cable

1. Unlock and remove the cable cover from the AP.
2. Remove the front cover from the AP to reveal the serial port.
3. Connect one end of the serial cable to the AP and the other end to a serial port on your computer.
4. Power on the computer and AP, if necessary.

Initializing the IP Address using CLI

After installing the serial port cable, you may use the CLI to communicate with the AP. CLI supports most generic terminal emulation programs, such as HyperTerminal (which is included with the Windows operating systems). In addition, many web sites offer shareware or commercial terminal programs you can download. Once the IP address has been assigned, you can use the HTTP interface or the CLI over Telnet to complete configuration.

Follow these steps to assign the AP an IP address:

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, and so forth, depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
2. Under **File -> Properties -> Settings -> ASCII Setup**, enable the **Send line ends with line feeds** option.
   Result: HyperTerminal sends a line return at the end of each line of code.
3. Press the **RESET** button on the AP (see RELOAD and RESET Buttons to identify the location of the **RESET** button).
   Result: The terminal display shows Power On Self Tests (POST) activity, and then displays a CLI prompt, similar to the example below. This process may take up to 90 seconds.
   `[Device name]> Please enter password:`
4. Enter the CLI password (default is **public**).
   Result: The terminal displays a welcome message and then the CLI Prompt:
   `[Device name]>`
5. Enter **show ip**. Result: Network parameters appear:

```
[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

Figure 7-2 Result of "show ip" CLI Command

6. Change the IP address and other network values using **set** and **reboot** CLI commands, similar to the example below (use your own IP address and subnet mask). Note that IP Address Type is set to Dynamic by default. If you have a DHCP server on your network, you should not need to manually configure the Access Point's IP address; the Access Point will obtain an IP address from the network's DHCP server during boot-up.
   Result: After each entry the CLI reminds you to reboot; however wait to reboot until all commands have been entered.
   `[Device name]>` **set ipaddrtype static**
   `[Device name]>` **set ipaddr <IP Address>**
   `[Device name]>` **set ipsubmask <IP Subnet Mask>**
   `[Device name]>` **set ipgw <Default Gateway IP Address>**
   `[Device name]>` **show ip** (to confirm your new settings)
   `[Device name]>` **reboot 0**
7. After the AP reboots, verify the new IP address by reconnecting to the CLI and enter a **show ip** command. Alternatively, you can ping the AP from a network computer to confirm that the new IP address has taken effect.
8. When the proper IP address is set, use the HTTP interface or CLI over Telnet to configure the rest of the unit's operating parameters.

Related Applications

RADIUS Authentication Server

If you enabled RADIUS Authentication on the AP, make sure that your network's RADIUS servers are operational. Otherwise, clients will not be able to log in. There are several reasons the authentication server services might be unavailable, here are two typical things to check:

- Make sure you have the proper RADIUS authentication server information setup configured in the AP. Check the RADIUS Authentication Server's Shared Secret and Destination Port number (default is 1812; for RADIUS Accounting, the default is 1813).
- Make sure the RADIUS authentication server RAS setup matches the AP.

TFTP Server

The "Trivial File Transfer Protocol" (TFTP) server allows you to transfer files across a network. You can upload configuration files from the AP for backup or copying, and you can download configuration files or new software images. The TFTP software is located on the AP Installation CD-ROM.

If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP address. Note that you do not need a TFTP server running unless you want to transfer files to or from the AP.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP Address, the proper AP Image file name, and that the TFTP server is connected.
- **Make sure the TFTP server is configured to both send and receive, with no time-out.**

Specifications

A

- Software Features
- Hardware Specifications
- Radio Specifications

Software Features

The tables below compare the software features available depending on the card type in the Access Point:

- Number of Stations per BSS
- Management Functions
- Advanced Bridging Functions
- Medium Access Control (MAC) Functions
- Security Functions
- Network Functions
- Advanced Wireless Functions

Number of Stations per BSS

Feature	150wl card	160wl card	170wl card
Without encryption	up to 250	up to 255	up to 63
With WEP encryption	up to 250	up to 60	up to 63
With 802.1x Authentication	up to 250	up to 50	up to 63
With WPA	N/A	N/A	up to 63

Management Functions

Feature	802.11b	802.11a	802.11b/g
Web User Interface	yes	yes	yes
Telnet / CLI	yes	yes	yes
SNMP Agent	yes	yes	yes
TFTP	yes	yes	yes

Advanced Bridging Functions

Feature	802.11b	802.11a	802.11b/g
IEEE 802.1d Bridging	yes	yes	yes
WDS Relay	yes	yes	yes
Roaming	yes	yes	yes
Protocol Filtering	yes	yes	yes
Multicast/Broadcast Storm Filtering	yes	yes	yes
Proxy ARP	yes	yes	yes
TCP/UDP Port Filtering	yes	yes	yes
Blocking Intra BSS Clients	yes	yes	yes
Packet Forwarding	yes	yes	yes

Specifications

Medium Access Control (MAC) Functions

Feature	802.11b	802.11a	802.11b/g
Automatic Channel Selection (ACS)	yes	yes	yes
Dynamic Frequency Selection (DFS) [1]	N/A	yes	N/A
Closed System Feature	yes	yes	yes
TX Power Control	N/A	Available with 802.11a upgrade kit. Not available with 5Ghz upgrade kit.	yes

Note 1: A user cannot manually select a channel for products sold in Europe; these products require automatic channel selection using Dynamic Frequency Selection (DFS).

Security Functions

Feature	802.11b	802.11a	802.11b/g
IEEE 802.11 WEP [1]	yes	yes	yes
MAC Access Control	yes	yes	yes
RADIUS MAC-based Access Control	yes	yes	yes
IEEE 802.1x Authentication [2]	yes	yes	yes
Multiple Authentication Server Support [4]	yes	yes	yes
Rogue Access Point Detection	no	yes	yes
Per User Per Session (PUPS) Encryption [3]	N/A	yes	yes
Wi-Fi Protected Access (WPA)	N/A	Available with 11a Upgrade Kit Not available with 5 GHz Upgrade Kit	yes

Note 1: Key lengths supported by 802.11a: 64-bit, 128-bit, and 152-bit.
Key lengths supported by 802.11b: 64-bit and 128-bit.
Key lengths supported by 802.11b/g: 64-bit, 128-bit, and 152-bit.

Note 2: EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP client supplicant supported.

Note 3: Use in conjunction with WPA or 802.1x Authentication.

Note 4: Support is provided for a primary and backup RADIUS authentication server for both MAC-based authentication and 802.1x authentication.

Network Functions

Feature	802.11b	802.11a	802.11b/g
DHCP Client	yes	yes	yes
DHCP Server	yes	yes	yes
Inter Access Point Protocol (IAPP)	yes	yes	yes
Link Integrity	yes	yes	yes
System Logging (Syslog)	yes	yes	yes
RADIUS Accounting Support [1]	yes	yes	yes
DNS Client	yes	yes	yes
TCP/IP Protocol Support	yes	yes	yes
Virtual LAN Support	One VLAN ID per wireless interface	One VLAN ID per wireless Interface	Up to 16 VLAN IDs per wireless interface

Note 1: Includes Fallback to Primary RADIUS Server, RADIUS Session Timeout, RADIUS Multiple MAC Address Formats, RADIUS DNS Host Name Support, RADIUS Start/Stop Accounting.

Advanced Wireless Functions

Feature	802.11b	802.11a	802.11b/g
WEP Plus (Weak Key Avoidance)[1]	yes	no	no
Remote Link Test[1]	yes	no	no
Load Balancing[1]	yes	no	no
AP List[1]	yes	no	no
Medium Density Distribution[1]	yes	no	no
Distance between APs	yes	no	no
Interference Robustness	yes	no	no
SpectraLink VoIP Support	yes	no	no

1 This feature is only available when using an HP ProCurve Wireless 802.11b AP Card 150wl. In addition, this feature will only give information for ORiNOCO/Agere?Lucent based clients.

Hardware Specifications

Physical Specifications

HP 520wl Unit

Dimensions (H x W x L) = 6.5 x 18.5 x 26 cm (2.5 x 7.25 x 10.25 in.)
Weight = 1.75 Kg (3.5 lb.)

802.11a Antenna Adapter

Dimensions (H x W x L) = 11.3 x 2.10 x 26.2 cm (4.5 x 0.83 x 10.3in.)
Weight = 0.18kg (0.4lb)

Electrical Specifications

Without Active Ethernet Module

Voltage = 100 to 240 VAC (50-60 Hz)
Current = 0.2 amp
Power Consumption = 20 Watts

With Active Ethernet Module

Input Voltage = 42 to 60 VDC
Output Current = 200mA at 48V
Power Consumption = 9-10 Watts

Environmental Specifications

HP 520wl Unit

Operating = 0° to 40°C (32° to 104 °F) @ 20 to 90% relative humidity
Transport = -40° to 60°C (-40° to 140°F) @ 15 to 95% relative humidity (no condensation allowed)
Storage = -10° to 60°C (14° to 140°F) @ 10 to 90% relative humidity (no condensation allowed)

802.11a Antenna Adapter

Operating = 0° to 70°C (32° to 158 °F) @ 20 to 90% relative humidity
Transport = -40° to 75°C (-40° to 167 °F) @ 15 to 95% relative humidity
Storage = -20° to 75°C (-4° to 167 °F) @ 10 to 95% relative humidity

Specifications

Ethernet Interface

10/100 Base-TX, RJ-45 female socket

Serial Port Interface

Standard RS-232C interface with DB-9, female connector

Active Ethernet Interface

Category 5, foiled, twisted pair cables must be used to ensure compliance with FCC Part 15, subpart B, Class B requirements

Standard 802.3af pin assignments

HTTP Interface

- Microsoft Internet Explorer 6 with Service Pack 1 or later
- Netscape 6.1 or later

Radio Specifications

- 802.11a Channel Frequencies
- 802.11b Channel Frequencies
- 802.11g Channel Frequencies
- Wireless Communication Range

NOTE

Refer to the Regulatory Flyer included with the AP for the latest regulatory information.

802.11a Channel Frequencies

The available 802.11a Channels varies by regulatory domain and/or country. 802.11a radio certification is available in the following regions:

- FCC: U.S., Canada, and Australia
- ETSI: Europe and the United Kingdom
- MKK: Japan
- SG: Singapore
- ASIA: China, Hong Kong, and South Korea
- TW: Taiwan

There are five sets of frequency bands that determine the available channels depending on the regulatory domain.

Some countries restrict 802.11a operation to specific frequency bands. The Web interface and CLI display the available channels for a radio's particular regulatory domain. In the CLI, any channels that are not available are labeled "Not Supported".

NOTE

The original 5 GHz Upgrade Kit only supports the Lower and Middle U-NII bands. The 11a Upgrade Kit supports all of the frequency bands described below.

Frequency Band	Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)	SG (GHz)	ASIA (GHz)	TW (GHz)
Lower Band (36 = default)	34	—	—	5.170 [1]	—	—	—
	36	5.180	5.180	—	5.180	—	—
	38	—	—	5.190	—	—	—
	40	5.200	5.200	—	5.200	—	—
	42	—	—	5.210	—	—	—
	44	5.220	5.220	—	5.220	—	—
	46	—	—	5.230	—	—	—
	48	5.240	5.240	—	5.240	—	—
Middle Band (52 = default)	52	5.260	5.260	—	—	—	5.260
	56	5.280	5.280	—	—	—	5.280
	58	5.300	5.300	—	—	—	5.300
	60	5.320	5.320	—	—	—	5.320
H Band	100	—	5.500	—	—	—	—
	104	—	5.520	—	—	—	—
	108	—	5.540	—	—	—	—
	112	—	5.560	—	—	—	—
	116	—	5.580	—	—	—	—
	120	—	5.600	—	—	—	—
	124	—	5.620	—	—	—	—
	128	—	5.640	—	—	—	—
	132	—	5.660	—	—	—	—
	136	—	5.680	—	—	—	—
	140	—	5.700	—	—	—	—
Upper Band (149 = default)	149	5.745	—	—	5.745	5.745	5.745
	153	5.675	—	—	5.675	5.675	5.675
	157	5.785	—	—	5.785	5.785	5.785
	161	5.805	—	—	5.805	5.805	5.805
ISM Band	165	5.825	—	—	5.825	—	5.825

Note 1: Channel 34 is the default channel for Japan

802.11b Channel Frequencies

The available 802.11b channels vary by regulatory domain and/or country. 802.11b radio certification is available in the following regions:

- FCC - U.S./Canada, Mexico, and Australia
- ETSI - Most of Europe, including the United Kingdom and some Eastern block countries
- MKK - Japan
- IL - Israel

Some countries restrict 802.11b operation to specific frequency bands. The web interface will always display the available channels depending in the cards regulatory domain. In the CLI, any channels that are not available are labeled "Not Supported".

Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)	IL (GHz)
1	2.412	2.412	2.412	-
2	2.417	2.417	2.417	-
3	2.422	2.422	2.422	-
4	2.427	2.427	2.427	2.427
5	2.432	2.432	2.432	2.432
6	2.437	2.437	2.437	2.437
7	2.442	2.442	2.442	2.442
8	2.447	2.447	2.447	2.447
9	2.452	2.452	2.452	-
10	2.457	2.457[1]	2.457	-
11	2.462	2.462[1]	2.462	-
12	-	2.467[1]	2.467	-
13	-	2.472[1]	2.472	-
14	-	-	2.484	-

Note 1: France is restricted to these four channels.

802.11g Channel Frequencies

The available 802.11g channels vary by regulatory domain and/or country. 802.11g radio certification is available in the following regions:

- FCC - U.S./Canada, Mexico, and Australia
- ETSI - Europe, including the United Kingdom, China, and South Korea
- MKK - Japan
- IL - Israel

Some countries restrict 802.11g operation to specific frequency bands. The web interface will always display the available channels depending in the cards regulatory domain. In the CLI, any channels that are not available are labeled "Not Supported".

Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)	IL (GHz)
1	2.412	2.412	2.412	-
2	2.417	2.417	2.417	-
3	2.422	2.422	2.422	-
4	2.427	2.427	2.427	2.427
5	2.432	2.432	2.432	2.432
6	2.437	2.437	2.437	2.437
7	2.442	2.442	2.442	2.442
8	2.447	2.447	2.447	2.447
9	2.452	2.452	2.452	-
10	2.457	2.457[1]	2.457	-
11	2.462	2.462[1]	2.462	-
12	-	2.467[1]	2.467	-
13	-	2.472[1]	2.472	-
14	-	-	2.484[2]	-

Note 1: France is restricted to these channels.

Note 2: Channel 14 is only available when using **802.11b only** mode.

Wireless Communication Range

The range of the wireless signal is related to the composition of objects in the radio wave path and the transmit rate of the wireless communication. Communications at a lower transmit range may travel longer distances. The range values listed in the Communications Range Chart are typical distances as calculated by Proxim's development team for FCC-certified products. These values provide a rule of thumb and may vary according to the actual radio conditions at the location where the product is used.

The range of your wireless devices can be affected when the antennas are placed near metal surfaces and solid high-density materials. Range is also impacted due to "obstacles" in the signal path of the radio that may either absorb or reflect the radio signal.

In Open Office environments, antennas can "see" each other (no physical obstructions between them). In Semi-open Office environments, workspace is divided by shoulder-height, hollow wall elements; antennas are at desktop level. In a Closed Office environment, solid walls and other obstructions may affect signal strength.

The following tables show typical range values for various environments for FCC-certified products (range may differ for products certified in other regulatory domains).

Specifications

802.11b

Range	11 Mbits/s	5.5 Mbits/s	2 Mbits/s	1 Mbits/s
Open Office	142 m (466 ft.)	177 m (581 ft.)	219 m (718 ft.)	272 m (892 ft.)
Semi-Open Office	98 m (322 ft.)	122 m (400 ft.)	151 m (495 ft.)	187 m (614 ft.)
Closed Office	67 m (220 ft.)	84 m (276 ft.)	104 m (341 ft.)	129 m (423 ft.)
Tx Power (dBm)	15	15	15	15
Receiver Sensitivity (dBm)	-82	-85	-88	-91
Antenna Gain	0 dBi (integrated diversity antenna module; 2.4-2.5 GHz)			

Table A-1 802.11b Wireless communication ranges

802.11a (5 GHz Upgrade Kit)

Range	54 Mbits/s	48 Mbits/s	36 Mbits/s	24 Mbits/s	18 Mbits/s	12 Mbits/s	9 Mbits/s	6 Mbits/s
Open Office	19 m (62 ft.)	33 m (108 ft.)	55 m (180 ft.)	74 m (243 ft.)	92 m (302 ft.)	106 m (348 ft.)	122 m (400 ft.)	131 m (430 ft.)
Semi-Open Office	13 m (43 ft.)	23 m (75 ft.)	38 m (125 ft.)	51 m (167 ft.)	63 m (207 ft.)	73 m (239 ft.)	84 m (276 ft.)	90 m (295 ft.)
Closed Office	9 m (30 ft.)	16 m (52 ft.)	26 m (85 ft.)	35 m (115 ft.)	43 m (141 ft.)	50 m (164 ft.)	58 m (190 ft.)	62 m (203 ft.)
Tx Power (dBm)	7	11	14	14	14	14	14	14
Receiver Sensitivity (dBm)	-65	-69	-73	-77	-80	-82	-84	-85
Antenna Gain	3.5 dBi (integrated diversity antennas; 5.15-5.35 GHz)							

Table A-2 802.11a (5 GHz Upgrade Kit) Wireless communication ranges

802.11a (11a Upgrade Kit)

Range	54 Mbits/s	48 Mbits/s	36 Mbits/s	24 Mbits/s	18 Mbits/s	12 Mbits/s	9 Mbits/s	6 Mbits/s
Open Office	46 m (151 ft.)	62 m (203 ft.)	82 m (269 ft.)	110 m (361 ft.)	136 m (446 ft.)	169 m (554 ft.)	181 m (594 ft.)	195 m (640 ft.)
Semi-Open Office	32 m (105 ft.)	42 m (138 ft.)	57 m (187 ft.)	75 m (246 ft.)	94 m (308 ft.)	116 m (381 ft.)	125 m (410 ft.)	134 m (440 ft.)
Closed Office	22 m (72 ft.)	29 m (95 ft.)	39 m (128 ft.)	52 m (171 ft.)	64 m (210 ft.)	80 m (262 ft.)	86 m (282 ft.)	92 m (302 ft.)
Tx Power (dBm)	15	15	15	15	15	15	15	15
Receiver Sensitivity (dBm)	-69	-73	-77	-81	-84	-87	-88	-89
Antenna Gain	4 dBi (integrated diversity antennas; 5.15-5.85 GHz)							

Table A-3 802.11a (11a Upgrade Kit) Wireless communication ranges

802.11b/g

Range	54 Mbits/s	48 Mbits/s	36 Mbits/s	24 Mbits/s	18 Mbits/s	12 Mbits/s	9 Mbits/s	6 Mbits/s	11 Mbits/s	5.5 Mbits/s	2 Mbits/s	1 Mbits/s
Open Office	56 m (184 ft.)	69 m (226 ft.)	107 m (351 ft.)	164 m (538 ft.)	219 m (718 ft.)	272 m (892 ft.)	292 m (958 ft.)	314 m (1030 ft.)	204 m (669 ft.)	236 m (774 ft.)	253 m (830 ft.)	338 m (1109 ft.)
Semi-Open Office	38 m (125 ft.)	48 m (157 ft.)	73 m (239 ft.)	113 m (371 ft.)	151 m (495 ft.)	187 m (614 ft.)	201 m (659 ft.)	216 m (709 ft.)	140 m (459 ft.)	162 m (531 ft.)	174 m (571 ft.)	232 m (761 ft.)
Closed Office	26 m (85 ft.)	33 m (108 ft.)	51 m (167 ft.)	78 m (256 ft.)	104 m (341 ft.)	129 m (423 ft.)	138 m (453 ft.)	149 m (489 ft.)	97 m (318 ft.)	111 m (364 ft.)	120 m (394 ft.)	160 m (525 ft.)
Tx Power (dBm)	12	13	14	15	15	15	15	15	15	15	15	15
Receiver Sensitivity (dBm)	-68	-70	-75	-80	-84	-87	-88	-89	-83	-85	-86	-90
Antenna Gain	3 dBi (integrated diversity antenna module; 2.4-2.5 GHz)											

Table A-4 802.11b/g Wireless communication ranges

ASCII Character Chart

B

You can configure WEP Encryption Keys in either Hexadecimal or ASCII format. Hexadecimal digits are 0-9 and A-F (not case sensitive). ASCII characters are 0-9, A-F, a-f (case sensitive), and punctuation marks. Each ASCII character corresponds to two hexadecimal digits.

The table below lists the ASCII characters that you can use to configure WEP Encryption Keys. It also lists the Hexadecimal equivalent for each ASCII character.

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
'	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Command Line Interface (CLI)

C

This section describes the AP's Command Line (CLI) Interface. CLI commands can be used to initialize, configure, and manage the Access Point.

- CLI commands may be entered in real time through a keyboard or submitted with CLI scripts.
- The CLI is available through both the Serial Port interface and over the Ethernet interface using Telnet.

NOTE

All CLI commands and parameters are case-sensitive.

- General Notes
- Command Line Interface (CLI) Variations
- CLI Command Types
- Using Tables & User Strings
- Configuring the AP using CLI commands
- Set Basic Configuration Parameters using CLI Commands
- Other Network Settings
- CLI Monitoring Parameters
- Parameter Tables

General Notes

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts, network access infrastructures, and client-server relationships. In addition, you should be familiar with software setup procedures for typical network operating systems and servers.

Notation Conventions

- Computer prompts are shown as constant width type. For example: `[Device-Name]>`
- Information that you input as shown is displayed in bold constant width type. For example: `[Device name]> set ipaddr 10.0.0.12`
- The names of keyboard keys, software buttons, and field names are displayed in bold type. For example: Click the **Configure** button.
- Screen names are displayed in bold italics. For example, the ***System Status*** screen.

Important Terminology

- Configuration Files - Database files containing the current Access Point configuration. Configuration items include the IP Address and other network-specific values. Config files may be downloaded to the Access Point or uploaded for backup or troubleshooting.
- Download vs. Upload - Downloads transfer files to the Access Point. Uploads transfer files from the Access Point. The TFTP server performs file transfers in both directions.
- Group - A logical collection of network parameter information. For example, the System Group is composed of several related parameters. Groups can also contain Tables. All items for a given Group can be displayed with a **show <Group>** CLI Command.

- Image File - The Access Point software executed from RAM. To update an Access Point you typically download a new Image File. This file is often referred to as the “AP Image”.
- Parameter - A fundamental network value that can be displayed and may be changeable. For example, the Access Point must have a unique IP Address and the Wireless interface must be assigned an SSID. Change parameters with the CLI **set** Command, and view them with the CLI **show** Command.
- Table - Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP Table. All items for a given Table can be displayed with a **show <Table>** CLI Command.
- TFTP - Refers to the TFTP Server, used for file transfers.

Navigation and Special Keys

This CLI supports the following navigation and special key functions to move the cursor along the prompt line.

Key Combination	Operation
Delete or Backspace	Delete previous character
Ctrl-A	Move cursor to beginning of line
Ctrl-E	Move cursor to end of line
Ctrl-F	Move cursor forward one character
Ctrl-B	Move cursor back one character
Ctrl-D	Delete the character the cursor is on
Ctrl-U	Delete all text to left of cursor
Ctrl-P	Go to the previous line in the history buffer
Ctrl-N	Go to the next line in the history buffer
Tab	Complete the command line
?	List available commands

CLI Error Messages

The following table describes the error messages associated with improper command inputs.

Error Message	Description
Syntax Error	Invalid syntax entered at the command prompt.
Invalid Command	A non-existent command has been entered at the command prompt.
Invalid Parameter Name	An invalid parameter name has been entered at the command prompt.
Invalid Parameter Value	An invalid parameter value has been entered at the command prompt.
Invalid Table Index	An invalid table index has been entered at the command prompt.
Invalid Table Parameter	An invalid table parameter has been entered at the command prompt.
Invalid Table Parameter Value	An invalid table parameter value has been entered at the command prompt.
Read Only Parameter	User is attempting to configure a read-only parameter.
Incorrect Password	An incorrect password has been entered in the CLI login prompt.
Download Unsuccessful	The download operation has failed due to incorrect TFTP server IP Address or file name.
Upload Unsuccessful	The upload operation has failed due to incorrect TFTP server IP Address or file name.

Command Line Interface (CLI) Variations

Administrators use the CLI to control Access Point operation and monitor network statistics. The AP supports two types of CLI: the Bootloader CLI and the normal CLI. The Bootloader CLI provides a limited command set, and is used when the current AP Image is bad or missing. The Bootloader CLI allows you to assign an IP Address and download a new image. Once the image is downloaded and running, the Access Point uses the normal CLI. This guide covers the normal CLI unless otherwise specified.

Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI used to perform initial configuration of the AP. This interface is only accessible by way of the serial interface if the AP does not contain a software image or a download image command over TFTP has failed.

The Bootloader CLI provides you with the ability to configure the initial setup parameters as well as download a software image to the device.

The following functions are supported by the Bootloader CLI:

- configuration of initial device parameters using the **set** command
- **show** command to view the device's configuration parameters
- **help** command to provide additional information on all commands supported by the Bootloader CLI
- **reboot** command to reboot the device

The parameters supported by the Bootloader CLI (for viewing and modifying) are:

- System Name
- IP Address Assignment Type
- IP Address
- IP Mask
- Gateway IP Address
- TFTP Server IP Address
- Image File Name (including the file extension)

The following lists display the results of using the **help** command in the Bootloader CLI:

```
[Device name]> help

Command List        Description
============        ===========
set                 Set system parameters
show                Show running system information
help                Description of commands, command usage and parameters
reboot              reboot the target

Command Usage
=============
set <parameter name> <parameter value> <cr>
show <cr>
help <cr>
reboot <cr>

Parameter List      Description
==============      ===========
sysname             System Name
ipaddr              System IP Address
ipsubmask           System Subnet Mask
ipgw                System Default Gateway IP Address
tftpipaddr          TFTP Server IP Address
tftpfilename        Image or Binary File name
ipaddrtype          System IP Address Type - STATIC or DYNAMIC

[Device name]>
```

Figure C-1 Results of "help" bootloader CLI command

The following lists display the results of using the **show** command in the Bootloader CLI:

```
[Device name]> show


sysname          Device name          System Name
ipaddr           10.0.0.1             System IP Address
ipsubmask        255.0.0.0            System Subnet Mask
ipgw             10.0.0.1             System Default Gateway IP Address
ipaddrtype       DYNAMIC              IP Address type
tftpipaddr       10.0.0.2             TFTP Server IP Address
tftpfilename     FILENAME             Image or Binary File Name

[Device name]>
```

Figure C-2 Results of "show" bootloader CLI command

CLI Command Types

This guide divides CLI Commands into two categories: Operational and Parameter Controls.

Operational CLI Commands

These commands affect Access Point behavior, such as downloading, rebooting, and so on. After entering commands (and parameters, if any) press the **Enter** key to execute the Command Line.

Operational commands include:

- **?:** Typing a question mark lists CLI Commands or parameters, depending on usage (you do not need to type Enter after typing this command)
- **done, exit, quit:** Terminates the CLI session
- **download:** Uses TFTP server to download “image”, “config”, or “bootloader upgrade” files to Access Point
- **help:** Displays general CLI help information or command help information, such as command usage and syntax
- **history:** Remembers commands to help avoid re-entering complex statements
- **passwd:** Sets the Access Point’s CLI password
- **reboot:** Reboots the Access Point in the specified time
- **search:** Lists the parameters in a specified Table
- **upload:** Uses TFTP server to upload “config” files from Access Point to TFTP default directory or specified path

? (List Commands)

This command can be used in a number of ways to display available commands and parameters.

The following table lists each operation and provides a basic example. Following the table are detailed examples and display results for each operation.

Operation	Basic Example
Display the Command List (Example 1)	`[Device-Name]>?`
Display commands that start with specified letters (Example 2)	`[Device-Name]>s?`
Display parameters for set and show commands (Examples 3a and 3b)	`[Device-Name]>set ?` `[Device-Name]>show ipa?`
Prompt to enter successive parameters for Commands (Example 4)	`[Device-Name]>download ?`

Example 1. Display Command list

To display the Command List, enter **?**.

`[Device-Name]>?`

```
[Device Name]>
show
set
download
upload
reboot
passwd
help
quit
done
exit
history
search
[Device Name]> _
```

Figure C-3 Result of “?” CLI command

Example 2. Display specific Commands

To show all commands that start with specified letters, enter one or more letters, then **?** with no space between letters and **?**.

`[Device-Name]>s?`

```
[Device Name]> s
show                set                 search
```

Figure C-4 Result of "s?" CLI command

Example 3. Display parameters for set and show

Example 3a allows you to see every possible parameter for the set (or show) commands. Notice from example 3a that the list is very long. Example 3b shows how to display a subset of the parameters based on initial parameter letters.

Example 3a. Display every parameter that can be changed

```
[Device-Name]>set ?
```

```
[Device Name]> set
Command Description:
The set command modifies the value of a given scalar parameter or table entry.

Command Usage:
set <parameter> <parameter value> <CR>
set <table> <index> <arg1> <value1> ..... <argN> <valueN> <CR>

Example:
set sysname "My Wireless Device" <CR>
set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0 cmt "Test WorkStation"
 <CR>

[Device Name]> set
broadcastflttbl
dhcpgw
dhcpippooltbl
dhcppridnsipaddr
dhcpsecdnsipaddr
dhcpstatus
dnsdomainname
dnsprisvripaddr
dnssecsvripaddr
dnsstatus
etherfltifbitmask
.
.
.
.
telsessiontout
tftpfilename
tftpfiletype
tftpipaddr
vlanidtbl
vlanmgmtid
vlanstatus
wdstbl
wif
wifsec
[Device Name]> set _
```

Figure C-5 Result of "set ?" CLI command

Example 3b. Display parameters based on letter sequence

This example shows entries for parameters that start with the letter "i". The more letters you enter, the fewer the results returned. Notice that there is no space between the letters and the question mark.

```
[Device-Name]>show ipa?
```

```
[Device Name]> show ipa
ipaddr              ipaddrtype          iparp
iparpfltipaddr      iparpfltstatus      iparpfltsubmask
```

Figure C-6 Result of "show ipa?" CLI command

```
[Device-Name]>show iparp?
```

```
[Device Name]> show iparp
iparp               iparpfltipaddr      iparpfltstatus
iparpfltsubmask
[Device Name]> show iparp_
```

Figure C-7 Result of "show iparp?" CLI command

Example 4. Display Prompts for Successive Parameters

Enter the command, a space, and then **?**. Then, when the parameter prompt appears, enter the parameter value. Result: The parameter is changed and a new CLI line is echoed with the new value (in the first part of the following example, the value is the IP Address of the TFTP server).

After entering one parameter, you may add another **?** to the new CLI line to see the next parameter prompt, and so on until you have entered all of the required parameters. The following example shows how this is used for the **download** Command. The last part of the example shows the completed **download** Command ready for execution.

```
[Device-Name]> download ?
<TFTP IP Address>
[Device-Name]> download 192.168.0.101 ?
<File Name>
[Device-Name]> download 192.168.0.101 apimage ?
<file type (config/img/bootloader)>
[Device-Name]> download 192.168.0.101 apimage img <CR>
```

done, exit, quit

Each of the following commands ends a CLI session:

```
[Device-Name]> done
[Device-Name]> exit
[Device-Name]> quit
```

download

Downloads the specified file from a TFTP server to the Access Point. Executing **download** in combination with the asterisks character (“*”) will make use of the previously set TFTP parameters. Executing download without parameters will display command help and usage information.

1. Syntax to download a file:
   `Device-Name]>download <tftp server address> <path and filename> <file type>`

   Example:
   `[Device-Name]>download 192.168.1.100 APImage2 img`

2. Syntax to display help and usage information:
   `[Device-Name]>download`

3. Syntax to execute the download command using previously set (stored) TFTP Parameters:
   `[Device-Name]>download *`

help

Displays instructions on using control-key sequences for navigating a Command Line and displays command information and examples.

1. Using help as the only argument:
   `[Device-Name]>help`

```
[Device Name]> help
Type ? at the command prompt for a command list.

Complete command description and command usage can be provided by:
help <command name> <CR>
<command name> help <CR>

Special keys supported:
Arrow Keys
DEL, BS .... delete previous character
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W ..... delete previous word
Ctrl-T ..... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer

Tab     .... will attempt command completion
# .... Comment Character
?       .... will provide command listing

Examples:
 '?'              list all the supported commands
'sh?'             list all commands that start with sh
'show ?'          list all arguments to the show command
'sh<TAB>'         complete the 'show' command

[Device Name]>
```

Figure C-8 Results of "help" CLI command

2. Complete command description and command usage can be provided by:
   `[Device-Name]>`**`help <command name>`**
   `[Device-Name]>`**`<command name> help`**

history

Shows content of Command History Buffer. The Command History Buffer stores command statements entered in the current session. To avoid re-entering long command statements, use the keyboard "up arrow" (Ctrl-P) and "down arrow" (Ctrl-N) keys to recall previous statements from the Command History Buffer. When the desired statement reappears, press the **Enter** key to execute, or you may edit the statement before executing it.

`[Device-Name]>` **`history`**

passwd

Changes the CLI Password.

`[Device-Name]>` **`passwd oldpassword newpassword newpassword`**

reboot

Reboots Access Point after specified number of seconds. Specify a value of 0 (zero) for immediate reboot.

`[Device-Name]>` **`reboot 0`**
`[Device-Name]>` **`reboot 30`**

search

Lists the parameters supported by the specified table. This list corresponds to the table information displayed in the HTTP interface. In this example, the CLI returns the list of parameters that make up an entry in the IP Access Table.

`[Device-Name]>` **`search mgmtipaccesstbl`**

```
[Device Name]> search mgmtipaccesstbl
The supported elements are:
index
ipaddr
ipmask
cmt
status
```

Figure C-9 Results of "search mgmtipaccesstbl" CLI command

upload

Uploads a text-based configuration file from the AP to the TFTP Server. Executing **upload** with the asterisk character ("*") will make use of the previously set/stored TFTP parameters. Executing **upload** without parameters will display command help and usage information.

1. Syntax to upload a file:
   ```
   [Device-Name]>upload <tftp server address> <path and filename> <filetype>
   ```
   Example:
   ```
   [Device-Name]>upload 192.168.1.100 APconfig.sys config
   ```
2. Syntax to display help and usage information:
   ```
   [Device-Name]>help upload
   ```
3. Syntax to execute the upload command using previously set (stored) TFTP Parameters:
   ```
   [Device-Name]>upload *
   ```

Parameter Control Commands

The following sections cover the two Parameter Control Commands (**show** and **set**) and include several tables showing parameter properties. These commands allow you to view (**show**) all parameters and statistics and to change (**set**) parameters.

- **show:** To see any Parameter or Statistic value, you can specify a single parameter, a Group, or a Table.
- **set:** Use this CLI Command to change parameter values. You can use a single CLI statement to modify Tables, or you can modify each parameter separately.

"show" CLI Command

Displays the value of the specified parameter, or displays all parameter values of a specified group (parameter table). Groups contain Parameters and Tables. Tables contain parameters for a series of similar entities.

To see a definition and syntax example, type only **show** and then press the **Enter** key. To see a list of available parameters, enter a question mark (**?**) after **show** (example: **show ?**).

Syntax:
```
[Device-Name]>show <parameter>
[Device-Name]>show <group>
[Device-Name]>show <table>
```

Examples:
```
[Device-Name]>show ipaddr
[Device-Name]>show network
[Device-Name]>show mgmtipaccesstbl
```

"set" CLI Command

Sets (modifies) the value of the specified parameter. To see a definition and syntax example, type only **set** and then press the **Enter** key. To see a list of available parameters, enter a space, then a question mark (**?**) after **set** (example: **set?**).

Syntax:
```
[Device-Name]>set <parameter> <value>
[Device-Name]>set <table> <index> <argument 1> <value 1> ... <argument N> <value N>
```

Example:

```
[Device-Name]>set sysloc "Main Lobby"
[Device-Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

Configuring Objects that Require Reboot

Certain objects supported by the Access Point require a device reboot in order for the changes to take effect. In order to inform the end-user of this behavior, the CLI provides informational messages when the user has configured an object that requires a reboot. The following messages are displayed as a result of the configuring such object or objects.

Example 1: Configuring objects that require the device to be rebooted

The following message is displayed every time the user has configured an object that requires the device to be rebooted.

```
[Device-Name]>set ipaddr 135.114.73.10
The following elements require reboot
The following elements require reboot
ipaddr
```

Example 2: Executing the "exit", "quit", or "done" commands when an object that requires reboot has been configured

In addition to the above informational message, the CLI also provides a message as a result of the **exit**, **quit**, or **done** command if changes have been made to objects that require reboot. If you make changes to objects that require reboot and execute the exit command the following message is displayed:

`[Device-Name]>exit<CR>` OR `quit<CR>` OR `done<CR>`

```
Modifications have been made to parameters that require the device to be rebooted. These
changes will only take effect after the next reboot.
```

"set" and "show" Command Examples

In general, you will use the CLI **show** Command to view current parameter values and use the CLI **set** Command to change parameter values. As shown in the following examples, parameters may be set individually or all parameters for a given table can be set with a single statement.

Example 1 - Set the Access Point IP Address Parameter

Syntax:

```
[Device-Name]>set <parameter name> <parameter value>
```

Example:

```
[Device-Name]> set ipaddr 10.0.0.12
```

Result: IP Address will be changed when you reboot the Access Point. The CLI reminds you when rebooting is required for a change to take effect. To reboot immediately, enter **reboot 0** (zero) at the CLI prompt.

Example 2 - Create a table entry or row

Use 0 (zero) as the index to a table when creating an entry. When creating a table row, only the mandatory table elements are required (comment is usually an optional table element). For optional table elements, the default value is generally applied if you do not specify a value.

Syntax:

```
[Device-Name]>set <table name> <table index> <element 1> <value 1> …
      <element n> <value n>
```

Example:

```
[Device-Name]> set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0
```

Result: A new table entry is created for IP address 10.0.0.10 with a 255.255.0.0 subnet mask.

Example 3 - Modify a table entry or row

Use the index to be modified and the table elements you would like to modify. For example, suppose the IP Access Table has one entry and you wanted to modify the IP address:

```
[Device-Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.11
```

You can also modify several elements in the table entry. Enter the index number and specific table elements you would like to modify. (Hint: Use the search Command to see the elements that belong to the table.)

```
[Device-Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.12 ipmask 255.255.255.248
      cmt "First Row"
```

Example 4 - Enable, Disable, or Delete a table entry or row

The following example illustrates how to manage the second entry in a table.

Syntax:

```
[Device-Name]>set <Table> index status <enable, disable, delete>
[Device-Name]>set <Table> index status <1=enable, 2=disable, 3=delete>
```

Example:

```
[Device-Name]>set mgmtipaccesstbl 2 status enable
[Device-Name]>set mgmtipaccesstbl 2 status disable
[Device-Name]>set mgmtipaccesstbl 2 status delete
[Device-Name]>set mgmtipaccesstbl 2 status 2
```

NOTE

You may need to enable a disabled table entry before you can change the entry's elements.

Example 5 - Show the Group Parameters

This example illustrates how to view all elements of a group or table.

Syntax:

```
[Device-Name]> show <group name>
```

Example:

```
[Device-Name]>show network
```

Result: The CLI displays network group parameters. Note **`show network`** and **`show ip`** return the same data.

```
[Device Name]> show network
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

Figure C-10 Results of "show network" and "show ip" CLI Commands

Example 6 - Show Individual and Table Parameters

1. View a single parameter.

   Syntax:
   `[Device-Name]>`**`show <parameter name>`**

   Example:
   `[Device-Name]>` **`show ipaddr`**

   Result: Displays the Access Point IP address.

```
[Device Name]> show ipaddr
ipaddr

10.0.0.1

[Device Name]> _
```

Figure C-11 Result of "show ipaddr" CLI Command

2. View all parameters in a table.

   Syntax:
   `[Device-Name]>` **`show <table name>`**
   Example: `[Device-Name]>` **`show mgmtipaccesstbl`**

   Result: Displays the IP Access Table and its entries.

Using Tables & User Strings

Working with Tables

Each table element (or parameter) must be specified, as in the example below.

`[Device-Name]>`**`set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0`**

Below are the rules for creating, modifying, enabling/disabling, and deleting table entries.

- Creation
  - The table name is required.
  - The table index is required – for table entry/instance creation the index is always zero (0).
  - The order in which the table arguments or objects are entered in not important.
  - Parameters that are not required can be omitted, in which case they will be assigned the default value.
- Modification
  - The table name is required.
  - The table index is required – to modify the table, "index" must be the index of the entry to be modified.
  - Only the table objects that are to be modified need to be specified. Not all the table objects are required.
  - If multiple table objects are to be modified the order in which they are entered is not important.
  - If the entire table entry is to be modified, all the table objects have to be specified.
- Enabling/Disabling
  - The table name is required.
  - The table index is required – for table enabling/disabling the index should be the index of the entry to be enabled/disabled.
  - The entry's new state (either "enable" or "disable") is required.
- Deletion
  - The table name is required.
  - The table index is required – for table deletion the index should be the index of the entry to be deleted.
  - The word "delete" is required.

Using Strings

Since there are several string objects supported by the AP, a string delimiter is required for the strings to be interpreted correctly by the command line parser. For this CLI implementation, the single quote or double quote character can be used at the beginning and at the end of the string.

For example:

`[Device-Name]>` **set sysname Lobby** - Does not need quote marks
`[Device-Name]>` **set sysname "Front Lobby"** - Requires quote marks.

The scenarios supported by this CLI are:

"My Desk in the office"	Double Quotes
'My Desk in the office'	Single Quotes
"My 'Desk' in the office"	Single Quotes within Double Quotes
'My "Desk" in the office'	Double Quotes within Single Quotes
"Daniel's Desk in the office"	One Single Quote within Double Quotes
'Daniel"s Desk in the office'	One Double Quote within Single Quotes

The string delimiter does not have to be used for every string object. The single quote or double quote only has to be used for string objects that contain blank space characters. If the string object being used does not contain blank spaces, then the string delimiters, single or double quotes, mentioned in this section are not required.

Configuring the AP using CLI commands

Log into the AP using HyperTerminal

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
   - Com Port: <COM1, COM2, and so forth, depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
2. Under **File -> Properties -> Settings -> ASCII Setup**, enable the **Send line ends with line feeds** option.
   Result: HyperTerminal sends a line return at the end of each line of code.
3. Enter the CLI password (default is **public**).

NOTE

We recommend changing your default passwords immediately. To perform this operation using CLI commands, refer to Change Passwords.

Log into the AP using Telnet

The CLI commands can be used to access, configure, and manage the AP using Telnet. Follow these steps:

1. Confirm that your computer's IP address is in the same IP subnet as the AP.

NOTE

If you have not previously configured the Access Point's IP address and do not have a DHCP server on the network, the Access Point will default to an IP address of 10.0.0.1.

2. Go to the DOS command prompt on your computer.
3. Type **telnet <IP Address of the unit>**.
4. Enter the CLI password (default is **public**).

NOTE

We recommend changing your default passwords immediately. To perform this operation using CLI commands, refer to Change Passwords.

Set Basic Configuration Parameters using CLI Commands

There are a few basic configuration parameters that you may want to setup right away when you receive the AP. For example:

- Set System Name, Location and Contact Information
- Set Static IP Address for the AP
- Change Passwords
- Set Network Names for the Wireless Interface
- Enable and Configure TX Power Control for the Wireless Interface(s)
- Set WEP Encryption for the Wireless Interface
- Download an AP Configuration File from your TFTP Server
- Backup your AP Configuration File
- Set up Auto Configuration

Set System Name, Location and Contact Information

```
[Device-Name]>set sysname <system name> sysloc <Unit Location>
[Device-Name]>set sysctname <Contact Name (person responsible for system)>
[Device-Name]>set sysctphone <Contact Phone Number> sysctemail <Contact E-mail address>
[Device-Name]>show system
```

```
[Device Name]> show system
System Parameters
=================

sysname                    :       Device Name
sysloc                     :       System Location
sysctname                  :       Contact Name
sysctemail                 :       name@Organization.com
sysctphone                 :       Contact Phone Number
sysuptime (DD:HH:MM:SS)    :        0:11: 6:40
sysoid                     :       1.3.6.1.4.1.11898.2.4.6
sysdescr                   :        AP v2.1.0  SN-02UI16570004 v2.0.10
sysservices                :       2
sysflashupdate             :       0
sysflashbckint             :       120
sysresettodefaults         :       0

[Device Name]> _
```

Figure C-12 Result of "show system" CLI Command

Set Static IP Address for the AP

NOTE

The IP Subnet Mask of the AP must match your network's Subnet Mask.

```
[Device-Name]>set ipaddrtype static
[Device-Name]>set ipaddr <fixed IP address of unit>
[Device-Name]>set ipsubmask <IP Mask>
[Device-Name]>set ipgw <gateway IP address>
[Device-Name]>show network
```

Change Passwords

```
[Device-Name]>passwd <Old Password> <New Password> <Confirm Password> (CLI password)
[Device-Name]>set httppasswd <New Password> (HTTP interface password)
[Device-Name]>set snmprpasswd <New Password> (SNMP read password)
[Device-Name]>set snmprwpasswd <New Password> (SNMP read/write)
[Device-Name]>set snmpv3authpasswd <New Password> (SNMPv3 authentication password)
```

```
[Device-Name]>set snmpv3privpasswd <New Password> (SNMPv3 privacy password)
[Device-Name]>reboot 0
```

CAUTION

We strongly urge you to change the default passwords to restrict access to your network devices to authorized personnel. If you lose or forget your password settings, you can always perform the Reset to Factory Default Procedure.

Set Network Names for the Wireless Interface

```
[Device-Name]>set wif <index 3 (Slot A) or 4 (Slot B)> netname <Network Name (SSID) for wireless interface>
[Device-Name]>show wif
```

```
[Device Name]> show wif
Wireless Interface Table
========================


Index                          :       3
Network Name                   :       My Wireless Network A
Distance Between APs           :       large
Interference Robustness        :       disable
DTIM Period                    :       1
Automatic Channel Selection    :       enable
Frequency Channel              :       56
RTS/CTS Medium Reservation     :       2347
Multicast Rate                 :       2 MBps
Closed System                  :       disable
Load Balancing                 :       enable
Medium Density Distribution    :       disable
MAC Address                    :       00:30:F1:65:09:E9
Supported Data Rates           :       6 9 12 18 24 36 48 54
Supported Frequency Channels   :       52 56 60 64 36 40 44 48 149 153 157 161
Physical Layer Type            :       OFDM
Regulatory Domain List         :       USA (FCC)
Transmit Rate                  :       0
TurboMode                      :       disable
```

Figure C-13 Results of "show wif" CLI command for an AP

Enable and Configure TX Power Control for the Wireless Interface(s)

The TX Power Control feature lets the user configure the transmit power level of the card in the AP at one of four levels:

- 100% of the maximum transmit power level of the card
- 50%
- 25%
- 12.5%

Perform the following commands to enable TX Power Control and set the transmit power level:

```
[Device-Name]>set txpowercontrol enable

[Device-Name]>set wif <interface number> currenttxpowerlevel <value>
Allowed values are: 1 (100%), 2 (50%), 3 (25%), 4 (12.5%)
```

Set WEP Encryption for the Wireless Interface

CAUTION

Wireless clients must be configured with the same encryption key to be able to communicate with the AP. The AP can only support one Key Length (so each of the configured keys must have the same length). The available key sizes vary based on the Access Point's model. See Security Encryption Key Length Table for more information.

You can set up to four encryption keys. This example describes setting encryption Key 1 on the wireless card in Slot A (if applicable; a Single-radio AP uses index 3; a Dual-radio AP uses index 3 for Slot A and index 4 for Slot B).

```
[Device-Name]>set wifsec 3 encryptstatus enable encryptkey1 <WEP key (number of characters
              vary depending on AP model)> encryptkeytx key1
[Device-Name]>show wifsec
```

```
[Device Name]> show wifsec
Wireless Security table
==============


Index                    :              3
EnableEncryption         :        disable
EncryptionKey1           :       ********
EncryptionKey2           :       ********
EncryptionKey3           :       ********
EncryptionKey4           :       ********
Encryption Key in Use    :           key1
Deny Non Encrypted Data  :         enable
```

Figure C-14 Result of "show wifsec" CLI Command

Download an AP Configuration File from your TFTP Server

Begin by starting your TFTP program. It must be running and configured to transmit and receive.

[Device-Name]>**set tftpfilename <file name> tftpfiletype config tftpipaddr <IP address of your TFTP server>**
[Device-Name]>**show tftp** (to ensure the filename, file type, and the IP address are correct)
[Device-Name]>**download ***
[Device-Name]>**reboot 0**

After following the complete process (above) once, you can download a file of the same name (so long as all the other parameters are the same), with the following command:

[Device-Name]>**download ***

Backup your AP Configuration File

Begin by starting your TFTP program. It must be running and configured to transmit and receive.

[Device-Name]>**upload <TFTP Server IP address> <tftpfilename** (such as "config.sys")**> config**
[Device-Name]>**show tftp** (to ensure the filename, file type, and the IP address are correct)

After setting the TFTP parameters, you can backup your current file (so long as all the other parameters are the same), with the following command:

[Device-Name]>**upload ***

Set up Auto Configuration

The Auto Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Perform the following commands to enable and set up automatic configuration:

NOTE

The configuration filename and TFTP server IP address are configured only when the AP is configured for Static IP. If the AP is configured for Dynamic IP these parameters are not used and obtained from DHCP. The default filename is "config". The default TFTP IP address is "10.0.0.2".

[Device-Name]>**set autoconfigstatus <enable/disable>**

[Device-Name]>**set autoconfigfilename <filename>**
Enter the filename of the configuration file that is used if the AP is configured for Static IP.

[Device-Name]>**set autoconfigTFTPaddr <IP address>**
Enter the TFTP server address that is used if the AP is configured for Static IP.

Other Network Settings

There are other configuration settings that you may want to set for the AP. Some of them are listed below.

- Configure the AP as a DHCP Server
- Configure the DNS Client
- Maintain Client Connections using Link Integrity
- Change your Wireless Interface Settings
- Set Ethernet Speed and Transmission Mode
- Set Interface Management Services
- Configure MAC Access Control
- Set RADIUS Parameters
- Set Rogue Access Point Detection (RAD) Parameters
- Set VLAN/SSID Parameters

NOTE

Refer to Advanced Configuration for more information on these settings.

Configure the AP as a DHCP Server

NOTE

You must have at least one entry in the DHCP Server IP Address Pool Table before you can set the DHCP Server Status to Enable.

```
[Device-Name]>set dhcpstatus disable
[Device-Name]>set dhcpippooltbl 0 startipaddr <start ip address>
              endipaddr <end ip address>
[Device-Name]>set dhcpgw <gateway ip address>
[Device-Name]>set dhcppridnsipaddr <primary dns ip address>
[Device-Name]>set dhcpsecdnsipaddr <secondary dns ip address>
[Device-Name]>set dhcpstatus enable
[Device-Name]>reboot 0
```

CAUTION

Before enabling this feature, confirm that the IP address pools you have configured are valid addresses on the network and do not overlap the addresses assigned by any other DHCP server on the network. Enabling this feature with incorrect address pools will cause problems on your network.

Configure the DNS Client

```
[Device-Name]>set dnsstatus enable
[Device-Name]>set dnsprisvripaddr <IP address of primary DNS server>
[Device-Name]>set dnssecsvripaddr <IP address of secondary DNS server>
[Device-Name]>set dnsdomainname <default domain name>
[Device-Name]>show dns
```

```
[Device Name]> show dns
DNS Client Group
================

dnsstatus       :       disable
dnsprisvripaddr :       0.0.0.0
dnssecsvripaddr :       0.0.0.0
dnsdomainname   :
```

Figure C-15 Results of “show dns” CLI command

Maintain Client Connections using Link Integrity

```
[Device-Name]>show linkinttbl (this shows the current links)
[Device-Name]>set linkinttbl <1-5 (depending on what table row you wish to address)>
              ipaddr <ip address of the host computer you want to check>
[Device-Name]>set linkintpollint <the interval between link integrity checks>
[Device-Name]>set linkintpollretx <number of times to retransmit before considering
              the link down>
[Device-Name]>set linkintstatus enable
[Device-Name]>show linkinttbl (confirm new settings)
[Device-Name]>reboot 0
```

Change your Wireless Interface Settings

See Interfaces for information on the parameters listed below. Dual-radio APs use index 3 for Slot A and index 4 for Slot B.

Operational Mode

```
[Device-Name]>set wif <index> mode <see table>
```

mode	Operational Mode
1	dot11b-only
2	dot11g-only
3	dot11bg
4	dot11a-only
5	dot11g-wifi

Autochannel Select (ACS)

ACS is enabled by default. Reboot after disabling or enabling ACS.

```
[Device-Name]>set wif <index> autochannel <enable/disable>
[Device-Name]>reboot 0
```

Enable/Disable Closed System

```
[Device-Name]>set wif <index> closedsys <enable/disable>
```

Enable/Disable Interference Robustness (802.11b Only)

```
[Device-Name]>set wif <index> interrobust <enable/disable>
```

Enable/Disable Load Balancing (802.11b Only)

```
[Device-Name]>set wif <index> ldbalance <enable/disable>
```

Enable/Disable Medium Density Distribution (802.11b Only)

```
[Device-Name]>set wif <index> meddendistrib <enable/disable>
```

Set the Distance Between APs (802.11b Only)

```
[Device-Name]>set wif <index> distaps <large, medium, small, minicell, microcell>
[Device-Name]>reboot 0
```

NOTE

The distance between APs should not be approximated. It is calculated by means of a manual Site Survey, in which an AP is set up and clients are tested throughout the area to determine signal strength and coverage, and local limits such as physical interference are investigated. From these measurements the appropriate cell size and density is determined, and the optimum distance between APs is calculated to suit your particular business requirements.

Set the Multicast Rate (802.11b Only)

```
[Device-Name]>set wif <index> multrate <1,2,5.5,11 (Mbits/sec)>
```

NOTE

The Distance Between APs **must be set before** the Multicast Rate.

Set Ethernet Speed and Transmission Mode

```
[Device-Name]>set etherspeed <value (see below)>
[Device-Name]>reboot 0
```

Ethernet Speed and Transmission Mode	Value
10 Mbits/sec - half duplex	10halfduplex
10 Mbits/sec - full duplex	10fullduplex
10 Mbits/sec - auto duplex	10autoduplex
100 Mbits/sec - half duplex	100halfduplex
100 Mbits/sec - full duplex	100fullduplex
Auto Speed - half duplex	autohalfduplex
Auto Speed - auto duplex	autoautoduplex (default)

Set Interface Management Services

Edit Management IP Access Table

```
[Device-Name]>set mgmtipaccesstbl <index> ipaddr <IP address> ipmask <subnet mask>
```

Configure Management Ports

```
[Device-Name]>set snmpifbitmask <(see below)>
[Device-Name]>set httpifbitmask <(see below)>
[Device-Name]>set telifbitmask <(see below)>
```

Choose from the following values:

Interface bitmask	Description
0 or 2 = disable (all interfaces)	All management channels disabled
1 or 3 = Ethernet only	Ethernet only enabled
4 or 6 = Wireless A only	Wireless A only enabled
8 or 10 = Wireless B only	Wireless B only enabled
12 = Wireless A and Wireless B	Wireless A and Wireless B enabled
13 or 15 = all interfaces	All management channels enabled

Set Communication Ports

```
[Device-Name]>set httpport <HTTP port number (default is 80)>
[Device-Name]>set telport <Telnet port number (default is 23)>
```

Configure Secure Socket Layer (HTTPS)

Enabling SSL and configuring a passphrase allows encrypted Secure Socket Layer communications to the AP through the HTTPS interface.

```
[Device-Name]>set sslstatus <enable/disable>
```

The user must change the SSL passphrase when uploading a new certificate/private key pair, which will have a corresponding passphrase.

```
[Device-Name]>set sslpassphrase <SSL certificate passphrase>
[Device-Name]>show http
To view all HTTP configuration information including SSL.
HTTP Group Parameters
=====================
httpifbitmask           :       15
httppasswd              :       ********
httpport                :       80
httphelplink            :       c:/Program Files/HP/AP_520wl/Help/English/Index.htm
httpsetupwiz            :       disable
sslstatus               :       enable
sslpassphrase           :       ********
```

Set Telnet Session Timeouts

```
[Device-Name]>set tellogintout <time in seconds between 1 and 300 (default is 30)>
[Device-Name]>set telsessiontout <time in seconds between 1 and 36000 (default is 900)>
```

Configure Serial Port Interface

NOTE

To avoid unexpected performance issues, leave Flow Control at the default setting (none) unless you are sure what this setting should be.

```
[Device-Name]>set serbaudrate <2400, 4800, 9600, 19200, 38400, 57600>
[Device-Name]>set serflowctrl <none, xonxoff>
[Device-Name]>show serial
```

```
[Device Name]> show serial
Serial Interface Group Parameters
=================================

serbaudrate             :       9600
serdatabits             :       8
serparity               :       none
serstopbits             :       1
serflowctrl             :       none
```

Figure C-16 Result of "show serial" CLI Command

Configure Syslog

```
[Device-Name]>set syslogpriority <1-7 (default is 6)>
[Device-Name]>set syslogstatus <enable/disable>
```

Configure Intra BSS

```
[Device-Name]>set intrabssoptype <passthru (default)/block)>
```

Configure MAC Access Control

Setup MAC (Address) Access Control

```
[Device-Name]>set macaclstatus enable
[Device-Name]>set macacloptype <passthru, block>
[Device-Name]>reboot 0
```

Add an Entry to the MAC Access Control Table

```
[Device-Name]>set macacltbl <index> macaddr <MAC Address> status enable
[Device-Name]>show macacltbl
```

Disable or Delete an Entry in the MAC Access Control Table

```
[Device-Name]>set macacltbl <index> status <disable/delete>
[Device-Name]>show macacltbl
```

NOTE

For larger networks that include multiple Access Points, you may prefer to maintain this list on a centralized location using the RADIUS parameters (see Set RADIUS Parameters).

Configure Authentication Mode

Dual-radio APs use index 3 for Slot A and index 4 for Slot B.

```
[Device-Name]>set secconfigtbl <index> authmode <none, 802.1x, mixed, wpa, wpa-psk>
[Device-Name]>set secconfigtbl <index> enckeylen <64bits, 128bits>
[Device-Name]>set secconfigtbl <index> rekeyint <60 – 65535 seconds; default is 900
sec>
```

`[Device-Name]>show secconfigtbl` (to review your settings)

```
[Device-Name]>reboot 0
```

NOTE

If you set Authentication Mode to 802.1x, WPA, or Mixed, you also need to configure the RADIUS Authentication parameters. If you set Authentication Mode to Mixed, you also need to configure WEP Encryption settings.

For Dual-radio APs: WPA is available for APs with an 11a Upgrade Kit or 802.11b/g Kit. WPA is NOT available for APs with an 802.11b PC Card or a 5 GHz Upgrade Kit.

Set Pre-Shared Key (WPA-PSK Mode)

```
[Device-Name]>set wpaconfigtbl <index> pskey <64 hexadecimal digits>
```

or

```
[Device-Name]>set wpaconfigtbl <index> passphrase <8-64 characters; a minimum of 13
characters is recommended>
```

`[Device-Name]>show wpaconfigtbl` (to review your settings)

```
[Device-Name]>reboot 0
```

Set RADIUS Parameters

Configure RADIUS Authentication server

```
[Device-Name]>set radiustbl <index> status enable seraddrfmt <ipaddr or name>
              ipaddr <RADIUS IP address or name> port <user defined>
              ssecret <user defined> responsetm <1 to 10 seconds>
              maxretx <0 to 4 times>
[Device-Name]>show radiustbl
```

```
[OCO-AP-2000]> show radiustbl
RADIUS Authentication Group Table
=========================

Index                    :              1
Server type              :       MAC Authentication
RADIUS Auth Server Status:        disable
IP Address/Host Name     :       0.0.0.0
Authentication Port      :           1812
Response Time            :              3
Shared Secret            :       ********
Server Addressing Format:          ipaddr
Maximum Retransmission   :              3

Index                    :              2
Server type              :       MAC Authentication
RADIUS Auth Server Status:        disable
IP Address/Host Name     :       0.0.0.0
Authentication Port      :           1812
Response Time            :              3
Shared Secret            :       ********
Server Addressing Format:          ipaddr
Maximum Retransmission   :              3

Index                    :              3
Server type              :       EAP/802.1x Authentication
RADIUS Auth Server Status:        disable
IP Address/Host Name     :       0.0.0.0
Authentication Port      :           1812
Response Time            :              3
Shared Secret            :       ********
Server Addressing Format:          ipaddr
Maximum Retransmission   :              3

Index                    :              4
Server type              :       EAP/802.1x Authentication
RADIUS Auth Server Status:        disable
IP Address/Host Name     :       0.0.0.0
Authentication Port      :           1812
Response Time            :              3
```

Figure C-17 Results of "show radiustbl" CLI command

Enable RADIUS MAC Access Control

```
[Device-Name]>set radmacaccctrl enable
[Device-Name]>reboot 0
```

Set MAC Address Format Type

```
[Device-Name]>set radmacaddrformat <dashdelimited, colondelimited, singledashdelimited,
              nodelimiter>
```

Set Authorization Lifetime (MAC-based authentication only)

```
[Device-Name]>set radauthlifetm <900-43200 seconds; default is 900>
```

Enable RADIUS Accounting

```
[Device-Name]>set radaccstatus enable
[Device-Name]>set radaccinactivetmr <inactivity timer in minutes>
[Device-Name]>show radius
```

```
[Device Name]> show radius
RADIUS Group

RADIUS Authentication
=====================
radcliinvsvraddr                :       0
radmacaccctrl                   :       disable
radauthlifetm                   :       900
radmacaddrformat                :       dashdelimited

RADIUS Accounting
=================
radaccstatus                    :       disable
radaccinactivetmr               :       5
```

Figure C-18 Result of "show radius" CLI Command

Configure RADIUS Accounting server

```
[Device-Name]>set radacctbl <index> status <enable> seraddrfmt <ipaddr or name> ipaddr
              <RADIUS IP address or name> port <user defined> ssecret <user defined>
              responsetm <1 to 4 seconds> maxretx <1 to 10 times>
[Device-Name]>show radacctbl
```

```
[Device Name]> show radacctbl
RADIUS Accounting Group Table

========================
Index                   :             1
RADIUS Acc Server Status:        disable
IP Address/Host Name    :        0.0.0.0
Accounting Port         :           1813
Response Time           :              3
Shared Secret           :         ******
Server Addressing Format:         ipaddr
Maximum Retransmission  :              3

Index                   :             2
RADIUS Acc Server Status:        disable
IP Address/Host Name    :        0.0.0.0
Accounting Port         :           1813
Response Time           :              3
Shared Secret           :         ******
Server Addressing Format:         ipaddr
Maximum Retransmission  :              3
```

Figure C-19 Results of "show radacctbl" CLI command

Set Rogue Access Point Detection (RAD) Parameters

The Rogue AP Detection (RAD) feature enables an additional security level for wireless LAN deployments. The RAD feature provides a mechanism for detecting Rogue Access Points by utilizing the coverage of the trusted Access Point deployment.

The Rogue AP Scan employs background scanning using low-level 802.11 scanning functions for effective wireless detection of Access Points in its coverage area with minimal impact on the normal operation of the Access Point.

The **set radstatus** command enables Rogue Access Point Detection. The scan repetition duration **(radscanint)** is also configurable.If the Access Point uses directional antennas to provide directional coverage, then the interface bitmask (**radifbitmask**) can be configured to maximize the scanning coverage area.

```
[Device-Name]>set radstatus enable
[Device-Name]>set radscanint <15-1440>
[Device-Name]>set radifbitmask <4 (WiF A), 8 (WiF B), or 12 (both interfaces)>
[Device-Name]>show rad

 [OCO-AP-2000]> show rad
 Rogue AP Detect Group
 ===============
 radstatus              :       disable
 radifbitmask           :       4
 radscanint             :       15
```

Figure C-20 Results of "show rad" CLI command

Set VLAN/SSID Parameters

Enable VLAN Management

```
[Device-Name]>set vlanstatus enable
[Device-Name]>set vlanmgmtid <1-4094>
```

[Device-Name]>**show vlandidtbl** (to review your settings)

```
[Device-Name]>reboot 0
```

Disable VLAN Management

[Device-Name]>**set vlanstatus disable** or

```
[Device-Name]>set vlanmgmtid 0
[Device-Name]>reboot 0
```

Add an Entry to the VLAN ID Table

[Device-Name]>**set vlanidtbl** <index number; see table> **id** <1-4094, -1=untagged> **ssid** <enter network name>

[Device-Name]>**show vlandidtbl** (to review your settings)

```
[Device-Name]>reboot 0
```

NOTE

16 VLAN/SSID pairs are available for 802.11b/g AP Cards only.

CLI Monitoring Parameters

Using the **show** command with the following table parameters will display operating statistics for the AP (these are the same statistics that are described in Monitor Information for the HTTP Web interface).

- **staticmp:** Displays the ICMP Statistics.
- **statarptbl:** Displays the IP ARP Table Statistics.
- **statbridgetbl:** Displays the Learn Table.
- **statiapp:** Displays the IAPP Statistics.
- **statradius:** Displays the RADIUS Authentication Statistics.
- **statif:** Displays information and statistics about the Ethernet and wireless interfaces.
- **stat802.11:** Displays additional statistics for the wireless interfaces.
- **statethernet:** Displays additional statistics for the Ethernet interface.
- **statmss:** Displays station statistics and Wireless Distribution System links.

Parameter Tables

Objects contain groups that contain both parameters and parameter tables. Use the following tables to configure the Access Point. Columns used on the tables include:

- Name - Parameter, Group, or Table Name
- Type - Data type
- Values - Value range, and default value, if any
- Access = access type, R = Read Only (show), RW = Read-Write (can be “set”), W = Write Only
- CLI Parameter - Parameter name as used in the Access Point

Access Point network objects are associated with groups. The network objects are listed below and associated parameters are described in the following Parameter Tables:

- System Parameters - Access Point system information
  - Inventory Management Information - Hardware, firmware, and software version information
- Network Parameters - IP and Network Settings
  - IP Configuration Parameters - Configure the Access Point’s IP settings
    - DNS Client for RADIUS Name Resolution - Configure the Access Point as a DNS client

  - DHCP Server Parameters - Enable or disable dynamic host configuration
  - Link Integrity Parameters - Monitor link status
- Interface Parameters - Configure Wireless and Ethernet settings
  - Wireless Interface Parameters
    - Wireless Distribution System (WDS) Parameters - Configure the WDS partnerships
  - Ethernet Interface Parameters - Set the speed and duplex of the Ethernet port
- Management Parameters - Control access to the AP's management interfaces
  - SNMP Parameters - Set read and read/write passwords
  - HTTP (web browser) Parameters - Set up the graphical web browser interface. If required, enable SSL and configure the SSL certificate passphrase.
  - Telnet Parameters - Telnet Port setup
  - Serial Port Parameters - Serial Port setup
  - TFTP Server Parameters - Set up for file transfers; specify IP Address, file name, and file type
  - IP Access Table Parameters - Configure range of IP addresses that can access the AP
  - Auto Configuration Parameters - Configure the Auto Configuration feature which allows an AP to be automatically configured by downloading a configuration file from a TFTP server during boot up.
- Filtering Parameters
  - Ethernet Protocol Filtering Parameters - Control network traffic based on protocol type
  - Static MAC Address Filter Table - Enable and disable specific addresses
  - Proxy ARP Parameters - Enable or disable proxy ARP for wireless clients
  - IP ARP Filtering Parameters - Control which ARP messages are sent to wireless clients based on IP settings
  - Broadcast Filtering Table - Control the type of broadcast packets forwarded to the wireless network
  - TCP/UDP Port Filtering - Filter IP packets based on TCP/UDP port
- Alarms Parameters
  - SNMP Table Host Table Parameters - Enter the list of IP addresses that will receive alarms from the AP
  - Syslog Parameters - Configure the AP to send Syslog information to network servers
- Bridge Parameters
  - Spanning Tree Parameters - Used to help prevent network loops
  - Storm Threshold Parameters - Set threshold for number of broadcast packets
  - Intra BSS Subscriber Blocking - Enable or disable peer to peer traffic on the same AP
  - Packet Forwarding Parameters - Redirect traffic from wireless clients to a specified MAC address
- Security Parameters - Access Point security settings
  - Wireless Interface Security Parameters - Configure WEP encryption settings
  - MAC Access Control Parameter - Control wireless access based on MAC address
- RADIUS Parameters
  - Primary and Backup RADIUS Server Table Parameters - RADIUS Authentication and Accounting information
- Rogue Access Point Detection (RAD) Parameters - Enable and configure Rogue Access Point Detection.
- VLAN/SSID Parameters - Configure mutiple subnetworks based on VLAN ID and SSID pairs.
- Other Parameters
  - IAPP Parameters - Enable or disable the Inter-Access Point Protocol
  - SpectraLink VoIP Parameters (802.11b Only) - Enable or disable SpectraLink Voice over IP feature

System Parameters

Name	Type	Values	Access	CLI Parameter
System	Group	N/A	R	system
Name	DisplayString	User Defined	RW	sysname
Location	DisplayString	User Defined	RW	sysloc
Contact Name	DisplayString	User Defined	RW	sysctname
Contact E-mail	DisplayString	User Defined	RW	sysctemail
Contact Phone	DisplayString	User Defined max 254 characters	RW	sysctphone
FLASH Backup Interval	Integer	0 - 65535 seconds	RW	sysflashbckint
Flash Update		0 1	RW	sysflashupdate
System OID	DisplayString	N/A	R	sysoid
Descriptor	DisplayString	System Name, flash version, S/N, bootloader version	R	sysdescr
Up Time	Integer	dd:hh:mm:ss dd – days hh – hours mm – minutes ss – seconds	R	sysuptime
Emergency Restore to defaults		Resets all parameters to default factory values	RW	sysresettodefaults Note: You must enter the following command twice to reset to defaults: **set sysresettodefaults 1**

Inventory Management Information

Name	Type	Values	Access	CLI Parameter
System Inventory Management	Subgroup	N/A	R	sysinvmgmt
Component Table	Subgroup	N/A	R	sysinvmgmtcmptbl
Component Interface Table	Subgroup	N/A	R	sysinvmgmtcmpiftbl

NOTE

The inventory management commands display advanced information about the AP's installed components. You may be asked to report this information to a representative if you contact customer support.

Network Parameters

IP Configuration Parameters

Name	Type	Values	Access	CLI Parameter
Network	Group	N/A	R	network
IP Configuration	Group	N/A	R	ip (Note: The **network** and **ip** parameters display the same information)
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Default Router IP Address	IpAddress	User Defined	RW	ipgw
Default TTL	Integer	User Defined (seconds) 64 (default)	RW	ipttl
Address Type	Integer	static dynamic (default)	RW	ipaddrtype

NOTE

The IP Address Assignment Type (ipaddrtype) must be set to static before the IP Address (ipaddr), IP Mask (ipmask) or Default Gateway IP Address (ipgw) values can be entered.

DNS Client for RADIUS Name Resolution

Name	Type	Values	Access	CLI Parameter
DNS Client	Group	N/A	R	dns
DNS Client status	Integer	enable disable (default)	RW	dnsstatus
Primary DNS Server IP Address	IpAddress	User Defined	RW	dnspridnsipaddr
Secondary DNS Server IP Address	IpAddress	User Defined	RW	dnssecdnsipaddr
Default Domain Name	Integer32	User Defined (up to 254 characters)	RW	dnsdomainname

DHCP Server Parameters

Name	Type	Values	Access	CLI Parameter
DHCP Server	Group	N/A	R	dhcp
DHCP Server Status	Integer	enable (1) (default) disable (2) delete (3)	RW	dhcpstatus
Gateway IP Address	IpAddress	User Defined	RW	dhcpgw
Primary DNS IP Address	IpAddress	User Defined	RW	dhcppridnsipaddr
Secondary DNS IP Address	IpAddress	User Defined	RW	dhcpsecdnsipaddr
Number of IP Pool Table Entries	Integer32	N/A	R	dhcpippooltblent

NOTE

The DHCP Server (dhcpstatus) can only be enabled after a DHCP IP Pool table entry has been created.

DHCP Server table for IP pools

Name	Type	Values	Access	CLI Parameter
DHCP Server IP Address Pool Table	Table	N/A	R	dhcpippooltbl
Table Index	Integer	User Defined	N/A	index
Start IP Address	IpAddress	User Defined	RW	startipaddr
End IP Address	IpAddress	User Defined	RW	endipaddr
Width	Integer	User Defined	RW	width
Default Lease Time (optional)	Integer32	> 0 86400 sec (default)	RW	defleasetm
Maximum Lease Time (optional)	Integer32	> 0 86400 sec (default)	RW	maxleasetm
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

NOTE

Set either End IP Address or Width (but not both) when creating an IP address pool.

Link Integrity Parameters

Name	Type	Values	Access	CLI Parameter
Link Integrity	Group	N/A	R	linkint
Link Integrity Status	Integer	enable disable (default)	RW	linkintstatus
Link Integrity Poll Interval	Integer	500 - 15000 ms (in increments of 500ms) 500 ms (default)	RW	linkintpollint
Link Integrity Poll Retransmissions	Integer	0 - 255 5 (default)	RW	linkintpollretx

Link Integrity IP Target Table

Name	Type	Values	Access	CLI Parameter
Link Integrity IP Target Table	Table	N/A	R	linkinttbl
Table Index	Integer	1-5	N/A	index
Target IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined (up to 254 characters)	RW	cmt
Status (optional)	Integer	enable disable (default) delete	RW	status

Interface Parameters

Wireless Interface Parameters

The wireless interface group parameter is **wif**. For Dual-radio APs, Slot A uses table index 3 and Slot B uses table index 4.

Common Parameters to 802.11a, 802.11b, and 802.11b/g APs

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Table Index	Integer	3 (Slot A) or 4 (Slot B)	R	index
Network Name	DisplayString	2 – 31 characters My Wireless Network (default)	RW	netname
Auto Channel Select (ACS)[1]	Integer	enable (default) disable	RW	autochannel
DTIM Period	Integer	1 – 255 1 = default	RW	dtimperiod
RTS/CTS Medium Reservation	Integer	0 – 2347 Default is 2347 (off)	RW	medres
MAC Address	PhyAddress	12 hex digits	R	macaddr
Closed System	Integer	enable disable (default)	RW	closedsys
Supported Frequency Channels	Octet String	Depends on Regulatory Domain	R	suppchannels
Load Balancing	Integer	enable (default) disable	RW	ldbalance

Note 1: For 802.11a APs in Europe, Auto Channel Select is a read-only parameter; it is always enabled.

802.11a Only Parameters

Name	Type	Values	Access	CLI Parameter
Operating Frequency Channel	Integer	Varies by regulatory domain and country. See 802.11a Channel Frequencies	RW	channel
Supported Data Rates	Octet String	See Transmit Rate, below	R	suppdatarates
Transmit Rate	Integer32	0 - Auto Fallback (default) 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec	RW	txrate
Physical Layer Type	Integer	ofdm (orthogonal frequency division multiplexing) for 802.11a	R	phytype

802.11b Only Parameters

Name	Type	Values	Access	CLI Parameter
Distance between APs	Integer	large (default) medium small minicell microcell	RW	distaps
Interference Robustness	Integer	enable (default) disable	RW	interrobust
Operating Frequency Channel	Integer	1 - 14; available channels vary by regulatory domain/country; see 802.11b Channel Frequencies	RW	channel
Multicast Rate	Integer	1 Mbits/sec (1) 2 Mbits/sec (2) (default) 5.5 Mbits/sec (3) 11 Mbits/sec (4)	RW	multrate
Closed Wireless System	Integer	enable disable (default)	RW	closedsys
Medium Distribution	Integer	enable (default) disable	RW	meddendistrib
MAC Address	PhyAddress	12 hex digits	R	macaddr
Supported Data Rates	Octet String	1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	R	suppdatarates
Transmit Rate	Integer32	0 (auto fallback - default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	RW	txrate
Supported Frequency Channels	Octet String	Depends on Regulatory Domain	R	suppchannels
Physical Layer Type	Integer	dsss (direct sequence spread spectrum) for 802.11b	R	phytype
Regulatory Domain List	DisplayString	U.S./Canada -- FCC Europe -- ETSI Japan -- MKK	R	regdomain

NOTE

There is an inter-dependent relationship between the Distance between APs and the Multicast Rate. In general, larger systems operate a lower average transmit rates.

Distance between APs	Multicast Rate
Large	1 and 2 Mbits/sec
Medium	1, 2, and 5.5 Mbits/sec
Small	1, 2, 5.5 and 11 Mbits/sec
Minicell	1, 2, 5.5 and 11 Mbits/sec
Microcell	1, 2, 5.5 and 11 Mbits/sec

802.11b/g Only Parameters

Name	Type	Values	Access	CLI Parameter
Wireless Operational Mode	Integer	dot11b-only dot11g-only dot11bg (default) dot11g-wifi	RW	mode
Operating Frequency Channel	Integer	1 - 14; available channels vary by regulatory domain/country; see 802.11g Channel Frequencies	RW	channel
Supported Data Rates	Octet String	See Transmit Rate, below	R	suppdatarates
Transmit Rate	Integer32	For 802.11b-only mode: 0 (auto fallback - default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec For 802.11g-only mode: 0 (auto fallback - default) 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec For 802.11g-wifi and 802.11bg modes: 0 (auto fallback - default) 1 Mbits/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec 6 Mbits/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec	RW	txrate
Physical Layer Type	Integer	ERP (Extended Rate Protocol)	R	phytype

Wireless Distribution System (WDS) Parameters

Name	Type	Values	Access	CLI Parameter
WDS Table	Table	N/A	R	wdstbl
Port Index	Integer	3.1 - 3.6 (Wireless)	R	portindex
Status	Integer	enable, disable	RW	status
Partner MAC Address	PhysAddress	User Defined	RW	partnermacaddr

Ethernet Interface Parameters

Name	Type	Values	Access	CLI Parameter
Ethernet Interface	Group	N/A	R	ethernet
Speed	Integer	10halfduplex 10fullduplex 10autoduplex 100halfduplex 100fullduplex autohalfduplex autoautoduplex (default)	RW	etherspeed
MAC Address	PhyAddress	N/A	R	ethermacaddr

Management Parameters

Secure Management Parameters

Name	Type	Values	Access	CLI Parameter
Secure Management	Integer	Enable/Disable	RW	securemgmtstatus

SNMP Parameters

Name	Type	Values	Access	CLI Parameter
SNMP	Group	N/A	R	snmp
SNMP Management Interface Bitmask	Interface Bitmask	0 or 2 - no interfaces (disable) 1 or 3 - Ethernet 4 or 6 - Wireless A 8 or 10 - Wireless B 12 = Wireless A & B 13 or 15 - all interfaces (default is 15)	RW	snmpifbitmask
Read Password	DisplayString	User Defined public (default) max 63 characters	W	snmprpasswd
Read/Write Password	DisplayString	User Defined public (default) max 63 characters	W	snmprwpasswd
SNMPv3 Authentication Password	DisplayString	User Defined public (default) max 63 characters	W	snmpv3authpasswd
SNMPv3 Privacy Password	DisplayString	User Defined public (default) max 63 characters	W	snmpv3privpasswd

HTTP (web browser) Parameters

Name	Type	Values	Access	CLI Parameter
HTTP	Group	N/A	R	http
HTTP Management Interface Bitmask	Interface Bitmask	0 or 2 - no interfaces (disable) 1 or 3 - Ethernet 4 or 6 - Wireless A 8 or 10 - Wireless B 12 = Wireless A & B 13 or 15 - all interfaces (default is 15)	RW	httpifbitmask
HTTP Password	DisplayString	User Defined max 64 characters	W	httppasswd
HTTP Port	Integer	User Defined Default = 80	RW	httpport
Help Link	DisplayString	User Defined	RW	httphelplink
SSL Status	Integer	Enable/Disable	RW	sslstatus
SSL Certificate Passphrase	DisplayString	User Defined	Write-only	sslpassphrase

NOTE

The default path for the Help files is **c:/Program Files/HP/AP_520wl/Help/English/index.htm**. (Use the forward slash character ("/") rather than the backslash character ("\") when configuring the **Help Link** location.) The AP Help information is available in English.

Telnet Parameters

Name	Type	Values	Access	CLI Parameter
Telnet	Group	N/A	R	telnet
Telnet Management Interface Bitmask	Interface Bitmask	0 or 2 - no interfaces (disable) 1 or 3 - Ethernet 4 or 6 - Wireless A 8 or 10 - Wireless B 12 = Wireless A & B 13 or 15 - all interfaces (default is 15)	RW	telifbitmask
Telnet Port	Integer	User Defined 23 (default)	RW	telport
Telnet Login Inactivity Time-out	Integer	1 – 300 seconds 30 sec (default)	RW	tellogintout
Telnet Session Idle Time-out	Integer	1 - 900 seconds 900 sec (default)	RW	telsessiontout

Serial Port Parameters

Name	Type	Values	Access	CLI Parameter
Serial	Group	N/A	R	serial
Baud Rate	Integer	2400, 4800, 9600 (default), 19200, 38400, 57600	RW	serbaudrate
Data Bits	Integer	8	R	serdatabits
Parity	Integer	none	R	serparity
Stop Bits	Integer	1	R	serstopbits
Flow Control	Value	none (default) xonxoff	RW	serflowctrl

Auto Configuration Parameters

These parameters relate to the Auto Configuration feature which allows an AP to be automatically configured by downloading a specific configuration file from a TFTP server during the boot up process.

Name	Type	Values	Access	CLI Parameter
Auto Configuration	Group	N/A	R	autoconfig
Auto Configuration Status	Integer	enable (default) disable	RW	autoconfigstatus
Auto Config File Name	DisplayString	User Defined	RW	autoconfigfilename
Auto Config TFTP Server IP Address	IpAddress	User Defined	RW	autoconfigTFTPaddr

TFTP Server Parameters

These parameters relate to upload and download commands.

When a user executes an upload and/or download command, the specified arguments are stored in TFTP parameters for future use. If nothing is specified in the command line when issuing subsequent upload and/or download commands, the stored arguments are used.

Name	Type	Values	Access	CLI Parameter
TFTP	Group	N/A	R	tftp
TFTP Server IP Address	IpAddress	User Defined	RW	tftpipaddr
TFTP File Name	DisplayString	User Defined	RW	tftpfilename
TFTP File Type	Integer	img config bootloader	RW	tftpfiletype

IP Access Table Parameters

When creating table entries, you may either specify the argument name followed by argument value or simply entering the argument value. When only the argument value is specified, then enter the values in the order depicted by the following table. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Values	Access	CLI Parameter
IP Access Table	Table	N/A	R	mgmtipaccesstbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Filtering Parameters

Ethernet Protocol Filtering Parameters

Name	Type	Values	Access	CLI Parameter
Ethernet Filtering	Group	N/A	R	etherflt
Filtering Interface Bitmask	Interface Bitmask	0 or 2 - no interfaces (disable) 1 or 3 - Ethernet 4 or 6 - Wireless A 8 or 10 - Wireless B 12 = Wireless A & B 13 or 15 - all interfaces (default is 15)	RW	etherfltifbitmask
Operation Type		passthru block	RW	etherfltoptype

Ethernet Filtering Table

Identify the different filters by using the table index.

Name	Type	Values	Access	CLI Parameter
Ethernet Filtering Table	Table	N/A	R	etherflttbl
Table Index	N/A	N/A	R	index
Protocol Number	Octet String	N/A	RW	protonumber
Protocol Name (optional)	DisplayString		RW	protoname
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

NOTE

The filter Operation Type (passthru or block) applies **only** to the protocol filters that are **enabled** in this table.

Static MAC Address Filter Table

Name	Type	Values	Access	CLI Parameter
Static MAC Address Filter Table	Table	N/A	R	staticmactbl
Table Index	N/A	N/A	R	index
Static MAC Address on Wired Network	PhysAddress	User Defined	RW	wiredmacaddr
Static MAC Address Mask on Wired Network	PhysAddress	User Defined	RW	wiredmask
Static MAC Address on Wireless Network	PhysAddress	User Defined	RW	wirelessmacaddr
Static MAC Address Mask on Wireless Network	PhysAddress	User Defined	RW	wirelessmask
Comment (optional)	DisplayString	max 255 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Proxy ARP Parameters

Name	Type	Values	Access	CLI Parameter
Proxy ARP	Group	N/A	R	parp
Status	Integer	enable disable (default)	RW	parpstatus

IP ARP Filtering Parameters

Name	Type	Values	Access	CLI Parameter
IP ARP Filtering	Group	N/A	R	iparp
Status	Integer	enable disable (default)	RW	iparpfltstatus
IP Address	IpAddress	User Defined	RW	iparpfltipaddr
Subnet Mask	IpAddress	User Defined	RW	iparpfltsubmask

Broadcast Filtering Table

Name	Type	Values	Access	CLI Parameter
Broadcast Filtering Table	Table	N/A	R	broadcastflttbl
Index	Integer	1-5	N/A	index
Protocol Name	DisplayString	N/A	R	protoname
Direction	Integer	ethertowireless wirelesstoether both (default)	RW	direction
Status	Integer	enable disable (default)	RW	status

TCP/UDP Port Filtering

The following parameters are used to enable/disable the Port filter feature.

Name	Type	Values	Access	CLI
Port Filtering	Group	N/A	R	portflt
Port Filter Status	Integer	enable (default) disable	RW	portfltstatus

TCP/UDP Port Filtering Table

The following parameters are used to configure TCP/UDP Port filters.

Name	Type	Values	Access	CLI
Port Filtering Table	Table	N/A	R	portflttbl
Table Index	N/A	User Defined (there are also 4 pre-defined indices, see Port Number below for more information)	R	index
Port Type	Octet String	tcp udp tcp/udp	RW	porttype

Port Number	Octet String	User Defined (there are also 4 pre-defined protocols: Index 1: NetBios Name Service – 137, Index 2: NetBios Datagram Service – 138, Index 3: NetBios Session Service – 139, Index 4: SNMP Service – 161)	RW	portnum
Protocol Name	DisplayString	User Defined (there are also 4 pre-defined protocols, see Port Number above)	RW	protoname
Interface Bitmask	Integer32	0 or 2 - no interfaces (disable) 1 or 3 - Ethernet 4 or 6 - Wireless A 8 or 10 - Wireless B 12 = Wireless A & B 13 or 15 - all interfaces (default is 15)	RW	ifbitmask
Status (optional)	Integer	enable (default for new entries) disable (default for pre-defined entries) delete	RW	status

Alarms Parameters

SNMP Table Host Table Parameters

When creating table entries, you may either specifying the argument name followed by argument value. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Values	Access	CLI Parameter
SNMP Trap Host Table	Table	N/A	R	snmptraphosttbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Password	DisplayString	User Defined (up to 64 characters)	W	passwd
Comment (optional)	DisplayString	User Defined (up to 254 characters)	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Syslog Parameters

The following parameters configure the Syslog settings.

Name	Type	Values	Access	CLI
Syslog	Group	N/A	R	syslog
Syslog Status	Integer	enable disable (default)	RW	syslogstatus
Syslog Port	Octet String	514	R	syslogport

Syslog Lowest Priority Logged	Integer	1 – 7 1 = LOG_ALERT 2 = LOG_CRIT 3 = LOG_ERR 4 = LOG_WARNING 5 = LOG_NOTICE 6 = LOG_INFO (default) 7 = LOG_DEBUG	RW	syslogpritolog
Heartbeat Status	Integer	enable (1) disable (2) (default)	RW	sysloghbstatus
Heartbeat Interval (seconds)	Integer	1 – 604800 seconds; 900 sec. (default)	RW	sysloghbinterval

NOTE

The Heartbeat parameters are advanced settings not available by way of the HTTP interface. When Heartbeat is enabled, the AP periodically sends a message to the Syslog server to indicate that it is active. The frequency with which the heartbeat message is sent depends upon the setting of the Heartbeat Interval.

Syslog Host Table

The table described below configures the Syslog hosts that will receive message from the AP. You can configure up to ten Syslog hosts.

Name	Type	Values	Access	CLI Parameter
Syslog Host Table	Table	N/A	R	sysloghosttbl
Table Index	Integer	1 – 10	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Bridge Parameters

Spanning Tree Parameters

Name	Type	Values	Access	CLI Parameter
Spanning Tree	Group	N/A	R	stp
Spanning Tree Status	Integer	enable (default) disable	RW	stpstatus
Bridge Priority	Integer	0 – 65535 32768 (default)	RW	stppriority
Maximum Age	Integer	600 – 4000 (in 0.01 sec intervals; that is, 6 to 40 seconds) 2000 (default)	RW	stpmaxage
Hello Time	Integer	100 – 1000 (in 0.01 sec intervals; that is, 1 to 10 seconds) 200 (default)	RW	stphellotime
Forward Delay	Integer	400 – 3000 (in 0.01 sec intervals; that is, 4 to 30 seconds) 1500 (default)	RW	stpfwddelay

Spanning Tree Priority and Path Cost Table

Name	Type	Values	Access	CLI Parameter
Spanning Tree Table	Table	N/A	R	stpbl
Table Index (Port)	N/A	1 – 15	R	index

Priority	Integer	0 – 255 128 (default)	RW	priority
Path Cost	Integer	1 – 65535 100 (default)	RW	pathcost
State	Integer	disable blocking listening learning forwarding broken	R	state
Status	Integer	enable disable	RW	status

Storm Threshold Parameters

Name	Type	Values	Access	CLI Parameter
Storm Threshold	Group	N/A	N/A	stmthres
Broadcast Threshold	Integer	0 – 255 packets/sec (default is 0)	RW	stmbrdthres
Multicast Threshold	Integer	0 – 255 packets/sec (default is 0)	RW	stmmultithres

Storm Threshold Table

Name	Type	Values	Access	CLI Parameter
Storm Threshold Table	Table	N/A	R	stmthrestbl
Table Index	Integer	1 = Ethernet 3 = Wireless	R	index
Broadcast Threshold	Integer	0 – 255 packets/sec (default is 0)	RW	bcast
Multicast Threshold	Integer	0 – 255 packets/sec (default is 0)	RW	mcast

Intra BSS Subscriber Blocking

The following parameters control the Intra BSS traffic feature, which prevent wireless clients that are associated with the same AP from communicating with each other:

Name	Type	Values	Access	CLI
Intra BSS Traffic	Group	N/A	R	intrabss
Intra BSS Traffic Operation	Integer	passthru (default) block	RW	intrabssoptype

Packet Forwarding Parameters

The following parameters control the Packet Forwarding feature, which redirects wireless traffic to a specific MAC address:

Name	Type	Values	Access	CLI
Packet Forwarding MAC Address	Group	N/A	R	pktfwd
Packet Forwarding MAC Address	MacAddress	User Defined	RW	pktfwdmacaddr
Packet Forwarding Status	Integer	enable disable (default)	RW	pktfwdstatus
Packet Forwarding Interface Port	Integer	0 (any) (default) 1 (Ethernet) 2 (WDS 1) 3 (WDS 2) 4 (WDS 3) 5 (WDS 4) 6 (WDS 5) 7 (WDS 6)	RW	pktfwdif

Security Parameters

For Dual-radio APs: WPA is available for APs with an HP ProCurve Wireless 802.11g AP Card 170wl.

Name	Type	Values	Access	CLI Parameter
Security	Table	N/A	R	secconfigtbl
Index	Integer	3 (Single-radio APs) 3 or 4 (Dual-radio APs)	R	index
Authentication Mode	Integer	none (default) 802.1x mixed wpa wpa-psk	RW	authmode
Re-keying Interval	Integer	60 – 65535 seconds default is 900 sec	RW	rekeyint
Encryption Key Length	Integer	64bits 128bits	RW	enckeylen

Pre-Shared Key Configuration Table (WPA-PSK Mode)

Name	Type	Values	Access	CLI Parameter
WPA-PSK Pre-Shared Key Table	Table	N/A	R	wpaconfigtbl
Index	Integer	3 (Slot A) or 4 (Slot B)	N/A	index
Pre-Shared Key[1]	DisplayString	64 hex digits	WO	pskey
PSK Pass Phrase[1]	DisplayString	8 to 64 characters[2]	WO	passphrase

Note 1: Configure either the **Pre-Shared Key** or the **PSK Pass Phrase** (but not both) to create a pre-shared key for WPA-PSK mode. Setting **Pre-Shared Key** will override a previous **PSK Pass Phrase** setting. Similarly, setting **PSK Pass Phrase** will override a previous **Pre-Shared Key** setting.

Note 2: We recommend using a **PSK Pass Phrase** of at least 13 characters to ensure that the generated key cannot be easily deciphered by network infiltrators.

Wireless Interface Security Parameters

The following table details the WEP encryption parameters for the AP.

Name	Type	Values	Access	CLI Parameter
Wireless Interface Security	Group		R	wifsec
Encryption Status	Integer	enable, disable (default)	RW	encryptstatus
Index	Integer	3 (Single-radio APs) 3 or 4 (Dual-radio APs)	R	index
Encryption Key 1	DisplayString	User Defined	W	encryptkey1
Encryption Key 2	DisplayString	User Defined	W	encryptkey2
Encryption Key 3	DisplayString	User Defined	W	encryptkey3
Encryption Key 4	DisplayString	User Defined	W	encryptkey4
Data Transmission Encryption Key	Integer	key1 (default), key2, key3, key4	RW	encryptkeytx

NOTE

See WEP Encryption for information on the supported WEP Key lengths.

Security Encryption Key Length Table

The following table details how to set the Encryption Key Length for the wireless interfaces.

Name	Type	Values	Access	CLI Parameter
Security Encryption Key Length Table	Table	N/A	R	secenckeylentbl
Index	Integer	3 (Slot A) or 4 (Slot B)	N/A	index
Encryption Key Length	Integer	64bits 128bits	RW	enckeylen

MAC Access Control Parameter

Name	Type	Values	Access	CLI Parameter
MAC Address Control	Group	N/A	R	macacl
Status	Integer	enable disable (default)	RW	macaclstatus
Operation Type	Integer	passthru (default) block	RW	macacloptype

MAC Access Control Table

Name	Type	Values	Access	CLI Parameter
MAC Address Control Table	Table	N/A	R	macacltbl
Table Index	N/A	N/A	R	index
MAC Address	PhysAddress	User Defined	RW	macaddr
Comment (optional)	DisplayString	User Defined max 254 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

RADIUS Parameters

Primary and Backup RADIUS Server Table Parameters

The HP ProCurve Wireless Access Point uses RADIUS authentication and/or accounting support a primary and backup RADIUS server for MAC-based authentication and a primary and backup RADIUS server for EAP/802.1x authentication. The configuration parameters and statistics are the same for both primary and backup servers.

The CLI differentiates the primary and backup RADIUS parameters by using the table index:

- Index 1: Primary MAC-based authentication server
- Index 2: Backup MAC-based authentication server
- Index 3: Primary EAP/802.1x authentication server
- Index 4: Backup EAP/802.1x authentication server

General RADIUS Parameters

Name	Type	Values	Access	CLI Parameter
RADIUS	Group	N/A	R	radius
MAC Access Control Status	Integer	enable disable (default)	R	radmacacctrl
Authorization Lifetime	Integer32	900 – 43200 seconds 900 sec. (default)	RW	radauthlifetm

MAC Address Format	Integer	dashdelimited (default) colondelimited singledashdelimited no delimiter	RW	radmacaddrformat
RADIUS Accounting Status	Integer	enable disable (default)	RW	radaccstatus
Accounting Inactivity Timer	Integer32	0 – 2147483647 minutes; default is 5 min.	RW	radaccinactivetmr

RADIUS Authentication

NOTE

Use a server name only if you have enabled the DNS Client functionality. See DNS Client for RADIUS Name Resolution.

Name	Type	Values	Access	CLI Parameter
RADIUS Authentication	Table	N/A	R	radiustbl
Primary MAC-based authentication server	Integer	1	R	index
Backup MAC-based authentication server	Integer	2	R	index
Primary EAP/802.1x authentication server	Integer	3	R	index
Backup EAP/802.1x authentication server	Integer	4	R	index
RADIUS Server Status	Integer	enable disable (default)	RW	status
Server Addressing Format (see note)	Integer	ipaddr (default) name	RW	seraddrfmt
Server IP Address or Name	IpAddress DisplayString	User Defined (enter an IP address if seraddrfmt is ipaddr or a name if set to name; up to 254 characters if using a name)	RW	ipaddr
Port (optional)	Integer	User Defined 1812 (default)	RW	port
Shared Secret	DisplayString	User Defined max 63 characters	W	ssecret
Response Time (sec)	Integer	1 – 4 seconds 3 sec (default)	RW	responsetm
Maximum Retransmissions (optional)	Integer	1 – 10 3 (default)	RW	maxretx

RADIUS Accounting

NOTE

Use a server name only if you have enabled the DNS Client functionality. See DNS Client for RADIUS Name Resolution.

Name	Type	Values	Access	CLI Parameter
RADIUS Accounting	Table	N/A	R	radacctbl
Primary RADIUS	Integer	1	R	index
Backup RADIUS	Integer	2	R	index
RADIUS Server Status	Integer	enable disable (default)	RW	status
Server Addressing Format (see note)	Integer	ipaddr (default) name	RW	seraddrfmt

Name	Type	Values	Access	CLI Parameter
Server IP Address or Name	IpAddress Display String	User Defined (enter an IP address if seraddrfmt is ipaddr or a name if set to name; up to 254 characters if using a name)	RW	ipaddr
Port (optional)	Integer	User Defined 1813 (default)	RW	port
Shared Secret	DisplayString	User Defined max 63 characters	W	ssecret
Response Time (sec)	Integer	1 – 4 seconds 3 sec (default)	RW	responsetm
Maximum Retransmissions (optional)	Integer	1 – 10 3 (default)	RW	maxretx

Rogue Access Point Detection (RAD) Parameters

Name	Type	Values	Access	CLI Parameter
Rogue Access Point Detection (RAD)	Group	N/A	R	rad
Status	Integer	enable disable (default)	RW	radstatus
Scan Interval	Integer	15-1440 (minutes)	RW	radscanint
Interface Bitmask	Interface Bitmask	4 (WiF A), 8 (WiF B), or 12 (both).	RW	radifbitmask

VLAN/SSID Parameters

Name	Type	Values	Access	CLI Parameter
VLAN	Group	N/A	R	vlan
Status	Integer	enable disable (default)	RW	vlanstatus
Management ID	VlanId	-1 (untagged) or 1-4094	RW	vlanmgmtid

VLAN ID Table

NOTE

16 VLAN/SSID pairs are available for APs with an HP ProCurve Wireless 802.11g AP Card 170wl only.

Name	Type	Values	Access	CLI Parameter
VLAN ID Table	Table	N/A	R	vlanidtbl
Index[1]	Integer32	3.1 - 3.16 (Wireless A); 4.1 - 4.16 (Wireless B; Dual-radio APs only)	R	index
Identifier (ID)	VlanId	-1 or 0 (both correspond to untagged) or 1-4094	RW	id
Network Name (SSID)	DisplayString	2-31 characters	RW	ssid
Status	Integer	enable (default when new entry created) disable delete	RW	status

Note 1: When adding a new entry to the table, you must specify the index instance you want to configure, such as **3.5**; the **0** index value is not applicable to this table and does not create a new entry.

Other Parameters

IAPP Parameters

Name	Type	Values	Access	CLI Parameter
IAPP	Group	N/A	R	iapp
IAPP Status	Integer	enable (default) disable	RW	iappstatus
Periodic Announce Interval (seconds)	Integer	80 120 (default) 160 200	RW	iappannint
Announce Response Time	Integer	2 seconds	R	iappannresp
Handover Time-out	Integer	410 ms 512 ms (default) 614 ms 717 ms 819 ms	RW	iapphandtout
Max. Handover Retransmissions	Integer	1 - 4 (default 4)	RW	iapphandretx
Send Announce Request on Startup	Integer	enable (default) disable	RW	iappannreqstart

NOTE

These parameters configure the Inter Access Point Protocol (IAPP) for roaming. Leave these settings at their default value unless a technical representative asks you to change them.

SpectraLink VoIP Parameters (802.11b Only)

Name	Type	Values	Access	CLI Parameter
Spectralink VoIP	Group	N/A	R	spectralink
Spectralink VoIP Status	Integer	enable disable (default)	RW	speclinkstatus

Index

Symbols

" (double quote) characters ... C-12

Numerics

104-bit encryption ... 4-34
128-bit encryption ... 2-10, 2-12, 4-34
152-bit encryption ... 2-10, 2-12
40-bit encryption ... 4-34
520wl *See* HP ProCurve Wireless
64-bit encryption ... 2-10, 2-12, 4-34
802.11 wireless connectivity ... 1-4, 4-34
802.11a AP configuration options ... 2-10, 4-9
802.11b AP configuration options ... 2-10, 4-10
802.11b/g AP configuration options ... 4-14
802.11b/g configuration options ... 2-12
? command ... C-4

A

AP cards
  coverage area for ... 1-7
  installing ... 1-1, 1-4, 1-8
  setting transmit power levels for ... C-15
  upgrade kits for ... 2-2
AP-to-AP communications ... 4-7
ARP configurations ... C-37
ARP information table ... 5-3
ARP requests ... 4-27
ASCII formats (encryption) ... B-1
Access Point 520wl *See* HP ProCurve Wireless
Address Resolution Protocol *See* ARP
Address Threshold parameter ... 4-33
Advanced IP configuration options ... 4-4
Alarm Host Table ... 4-31
Authentication Password parameter ... C-33
Auto Channel Select parameter ... 4-9, 4-16
Auto Configuration Parameters Table ... C-35
Auto Fallback feature ... 2-10

B

Basic Service Set (BSS) ... 4-33
Baud Rate parameter ... 4-20
Boot Server Host Name parameter ... 4-22, 4-23
Bootfile Name parameter ... 4-22, 4-23
Bootloader CLI ... 7-8, C-2, C-3
Bootloader files ... 6-4, 6-5
Bridge MIB alarms ... 4-30
Bridge screen ... 4-32
Broadcast Filtering Table ... C-37
Broadcast Storms ... 4-32

C

CLI *See* Command Line Interface
Closed Wireless System parameter ... C-31
Command History Buffer ... C-7
Command Line Interface (CLI)
  changing IP addresses with ... 7-10
  command types described ... C-4
  displaying subset of parameters ... C-5
  ending sessions ... C-6
  error messages listed ... C-2
  executing command line for ... C-4
  initializing IP addresses with ... 7-9
  navigational keys for ... C-2
  overview ... 1-2, C-1
  prompting for available parameters ... C-6
  setting RAD management options for ... 4-41
  types described ... C-2
  viewing available commands ... 6-1, C-4
command statements
  See also Command Line Interface
Commands screen ... 6-2
Configure main screen ... 4-2

D

DFS compliance ... 4-10
DHCP Client messages ... 4-3
DHCP Server Configuration screen ... 4-5, 4-6
DHCP Server Parameters Table ... C-28
DHCP servers
  assigning as clients ... 4-4
  configuring ... 4-5, C-17, C-28
  dynamic IP addresses and ... 4-22
  getting assigned IP addresses from ... 2-6
  virtual LANs and ... 4-48
DNS Client Default Domain Name parameter ... 4-4
DNS Client for RADIUS Name Resolution Table ... C-27
DNS Primary Server IP Address parameter ... 4-4
DNS Secondary Server IP Address parameter ... 4-4
DNS clients ... 4-4, C-17
DNS database ... 4-3
DNS hosts ... 4-3

DNS servers ... 4-3
DTIM values ... 4-9
Deferred Traffic Indicator Map (DTIM) ... 4-9
Distance Between APs parameter ... 4-11
Distance Between Cells parameter ... 4-12
Domain Name Service (DNS) ... 4-4
Download Unsuccessful message ... C-2
Dynamic Frequency Selection (DFS) ... 4-9
Dynamic Host Configuration Protocol *See* DHCP

E

EAP types ... 4-34, 4-35
EAP/802.1x authentication ... 5-5, C-42
Edit Management IP Access Table ... C-19
Enable DNS Client parameter ... 4-4
Enable IP/ARP Filtering parameter ... 4-27
Enable Proxy ARP parameter ... 4-27
Enable Syslog parameter ... 4-32
Encryption Key Length parameter ... C-42
Enterprise MIB configurations ... 1-2
Ethernet Filtering Table ... C-36
Ethernet Interface Parameters Table ... C-33
Ethernet Protocol Filter Table ... 4-24
Ethernet Protocol Filtering Parameters Table ... C-36
Ethernet Threshold parameter ... 4-33
Ethernet cables ... 1-2, 2-5
Ethernet connections
  assigning IP addresses to ... 4-5
  checking link integrity for ... 4-6
  configuration options for ... 4-16
  failing ... 4-6
  getting information about ... 5-6
  speed and transmission parameters for ... C-19
  troubleshooting ... 7-2, 7-5
  wireless distribution system for ... 4-15
Ethernet interface ... A-4
Ethernet networks ... 4-33
Extensible Authentication Protocol (EAP) ... 4-34

F

FLASH memory alarms ... 4-29
File Download dialog box ... 6-9
Filter Operation Type parameter ... 4-24
Flow Control parameter ... 4-20, C-20

G

Gateway IP Address field ... 2-8
Gateway IP Address parameter ... 4-4, C-28
General RADIUS Parameters Table ... C-42

H

HP ProCurve Wireless Access Point 520wl
  assigning IP addresses to ... 2-6, 2-7, 7-10
  backing up configurations for ... C-16
  changing interface settings for ... C-18
  configuring ... 4-1, C-12, C-13, C-16
  features listed ... 1-4, A-1
  getting information about ... 5-2, 5-3, C-27
  initializing ... 1-1, 2-6
  installation prerequisites ... 2-1
  installing hardware for ... 2-3
  locating device ... 1-1, 4-11, C-19, C-31
  logging into ... C-12
  monitoring system status for ... 2-8
  naming conventions for ... 4-3
  overview ... 1-1
  product components of ... 2-2
  rebooting ... 6-10, C-7, C-9
  recovery procedures for ... 7-5
  resetting factory defaults for ... 6-11, 7-1, 7-6
  security options for ... 4-34
  specifications for ... A-1
  system requirements for ... 2-2
  troubleshooting ... 7-1
  updating ... 2-13, 6-4, 6-5
  viewing operating statistics for ... C-24
HTTP (Web) Password parameter ... 4-17
HTTP (web browser) Parameters Table ... C-34
HTTP Management Interface Bitmask parameter ... C-34
HTTP Password parameter ... C-34
HTTP Port parameter ... C-34
HTTP access parameters ... 4-18
HTTP file transfers ... 6-3, 6-5, 6-8
HTTP interface
  accessing ... 7-1
  configuring AP 520wl from ... 4-1
  displaying available commands for ... 6-1
  displaying configuration information for ... C-20
  getting table information for ... C-7
  logging into ... 2-8, 6-1
  monitoring system status with ... 2-8
  overview ... 1-2
  setting RAD management options for ... 4-41
  setting Syslog notifications from ... 4-32
  specifications for ... A-4
  transferring files with ... 2-13
  troubleshooting ... 7-3
HTTP port ... 4-18
HTTPS access parameters ... 4-19
HTTPS interface ... 1-2, 4-1, C-20
Heartbeat parameters ... C-39
Help Link parameter ... C-34
Help Link screen ... 6-12
Hexadecimal formats (encryption) ... B-1
HyperTerminal ... C-12
HyperText Transfer Protocol *See* HTTP

Index

I

IAPP Parameters Table ... C-45
IAPP configurations ... C-45
IAPP screen ... 5-4
ICMP Monitoring screen ... 5-3
ICMP statistics ... 5-3
IP ARP Filtering Parameters Table ... C-37
IP Access Table ... 4-17, C-35
IP Address Assignment Type parameter ... 4-4, C-27
IP Address parameter ... 4-4
IP Configuration Parameters Table ... C-27
IP Configuration screen ... 4-4
IP Pool Table ... 4-6
IP Subnet Masks ... 1-1, 4-17, C-13
IP address pool ... 2-1, 4-5, C-17, C-28
IP addresses
- Telenet connections and ... C-12
- assigning ... 2-6, 2-7, 4-5, 4-6, 7-10
- changing ... 4-3, 7-10, C-9, C-10
- configuring ... 7-9, C-16
- defining TFTP server ... 4-22
- defining dynamic ... 4-4
- defining static ... 1-1, 2-7, C-13
- displaying ... C-11
- filtering ... 4-17
- finding ... 2-6
- getting information about ... 5-3
- host names compared to ... 4-4
- initializing ... 7-9
- installation prerequisites for ... 2-1
- managing VLAN ... 4-48
- manually setting ... 4-4
- resetting ... 7-6
- resetting AP and ... 6-11
- setting from CLI ... 7-9
- setting gateway ... 4-4
- specifying target ... 4-6
- troubleshooting ... 7-1, 7-2
- verifying ... 7-10

IP/ARP Table screen ... 5-3
IP/ARP filtering ... 4-27
Incorrect Password message ... C-2
Initiator Station ... 5-7
Installation program ... 2-6
Inter Access Point Protocol *See* IAPP
Interface Management Services ... C-19
Interfaces screen ... 4-7, 5-6
Interference Robustness parameter ... C-31
Internet Control Message Protocol *See* ICMP
Internet proxy settings ... 2-8, 4-1, 6-1
Intra BSS Subscriber Blocking parameters ... C-40
Intra BSS Traffic Operation parameter ... 4-33
Intra BSS configurations ... C-21
Invalid Command message ... C-2
Invalid Parameter Name message ... C-2
Invalid Parameter Value message ... C-2
Invalid Table Index message ... C-2
Invalid Table Parameter Value message ... C-2
Invalid Table Parameter message ... C-2
Inventory Management Information Table ... C-27

L

LAN networks *See* networks
LED indicators ... 2-14
Learn Table ... 4-32, 5-1
Learn Table screen ... 5-4
Link Integrity Configuration screen ... 4-6, 4-7
Link Integrity IP Address Table ... 4-6
Link Integrity IP Target Table ... C-29
Link Integrity Parameters Table ... C-29
Link Test screen ... 5-7
Load Balancing feature ... 4-11
Load Balancing parameter ... C-30
Login Idle Timeout parameter ... 4-20

M

MAC Access Configuration screen ... 4-39, 4-40
MAC Access Control Table ... 4-39, C-21, C-42
MAC Access Control parameters ... C-21, C-22, C-42
MAC Address Format Type parameter ... 4-43, C-22
MAC Address filters ... 4-24–4-26
MAC Address parameter ... C-31, C-33
MAC Address/Mask pair ... 4-24
MAC addresses
- assigning ... 4-10
- displaying ... 5-4
- filtering ... C-36
- getting information about ... 5-3
- instability problems with ... 4-32
- locating ... 2-6
- recording ... 4-32
- redirecting to ... 4-33, C-40
- storing ... 4-43

MIB files ... 1-2, 1-3
Management Information Base (MIB) files ... 1-2, 1-3
Management Services Configuration screen ... 4-19
Media Access Control *See* MAC
Monitor screen ... 5-1
Multicast Rate parameter ... C-31
Multicast messages ... 2-12, 4-11, 4-26

N

Network Adapter Selection screen ... 2-7
Network Interface Cards (NICs) ... 4-49
Network Name (SSID) ... 4-47
Network Parameters Table ... C-27
Network screen ... 4-4

O

Operating Frequency Channel parameter ... C-30, C-31, C-32
Operation Type parameter ... 4-39, C-36
Operational Mode parameter ... 4-8
Operational Mode screen ... 4-8

P

PC cards ... 7-4
PSK Pass Phrase option ... 4-36
PSK Pass Phrase parameter ... C-41
Packet Filtering parameters ... 4-24
Packet Forwarding Configuration screen ... 4-33
Packet Forwarding Interface Port parameter ... 4-33
Packet Forwarding MAC Address parameter ... 4-33
Pre-Shared Key Configuration Table ... C-41
Pre-Shared Key Mode parameters ... C-21
ProCurve Wireless *See* HP ProCurve Wireless
Proxy ARP Parameters Table ... C-37

R

RAD feature ... 4-41
RAD parameters ... C-23, C-44
RADIUS Accounting Server Configuration screen ... 4-47
RADIUS Accounting Table ... C-43
RADIUS Accounting parameter ... C-22
RADIUS Auth screen ... 4-43, 4-44
RADIUS Authentication Table ... C-43
RADIUS MAC Access Control ... 4-43
RADIUS Monitoring screen ... 5-5
RADIUS accounting alternative ... 4-31
RADIUS accounting messages ... 4-46
RADIUS parameters ... C-22, C-42
RADIUS servers
  assigning host names to ... 4-4
  authentication modes and ... 4-35
  configuring ... 4-44, 4-46, C-22
  getting information about ... 5-5
  installation prerequisites for ... 2-1
  overview ... 4-43
  storing MAC addresses on ... 4-43
  troubleshooting ... 7-11
  virtual LANs and ... 4-48
RFC 1215-traps ... 4-30
RTS/CTS Medium Reservation parameter ... 4-10
RTS/CTS communications ... 4-10
Read Only Parameter message ... C-2
Read/Write Password field ... 2-8
Reboot screen ... 6-10
Regulatory Domain List parameter ... C-31
Re-keying Intervals ... 4-37, 4-38
Remote Link Test screen ... 5-7
Remote Station ... 5-7
Reset screen ... 6-11
Retrieve File by way of HTTP screen ... 6-8
Retrieve File by way of TFTP screen ... 6-7
Rogue Access Point Detection ... 4-41–4-42, C-23, C-44
Rogue Access Point Detection screen ... 4-42

S

SNMP Interface Bitmask parameter ... 4-18
SNMP Read Password parameter ... 4-17
SNMP Read/Write Password parameter ... 4-17
SNMP Trap Host Table parameters ... C-38
SNMP configurations ... 1-2, 1-3, 4-18, 4-41
SNMP management parameters ... C-33
SNMP manager programs ... 1-2
SNMP trap messages ... 4-31
SNMP traps ... 4-41
SNMPv3 Authentication Password parameter ... 4-17
SNMPv3 Privacy Password parameter ... 4-17
SNMPv3 Secure Management option ... 1-2, 1-3
SNR Report screen ... 5-8
SSID requirements ... 2-1
SSIDs ... 4-47, 4-48, 4-49
SSL Certificate Passphrase parameter ... 4-19, C-34
SSL Status parameter ... C-34
SSL configurations ... C-20
SSL file transfers ... 6-3, 6-6
SSL interface ... 1-2, 4-19
Save As dialog box ... 6-9
Scan List screen ... 2-6, 2-7
ScanTool ... 2-6–2-8, 7-7
Secure HTTP *See* HTTPS
Secure Socket Layers (SSL) ... 1-2, 4-19, 6-3
  See also HTTPS interface
Security Encryption Key Length Table ... C-42
Serial Data Bits parameter ... 4-20
Serial Parity parameter ... 4-20
Serial Port Parameters Table ... C-34
Serial Stop Bits parameter ... 4-20
Service Set IDentifier ... 2-1
Session Idle Timeout parameter ... 4-20
Setup Wizard ... 2-6, 2-9–2-13, 4-18
Signal to Noise ratio (SNR) ... 5-7
Simple Network Management Protocol (SNMP) ... 1-2
Software Image version ... 5-2
Spanning Tree ... 4-32
Spanning Tree Parameters Table ... C-39
Spanning Tree Priority and Path Cost Table ... C-39
SpectraLink VoIP Parameters Table ... C-45
Static MAC Address Filter Table ... C-36
Static MAC Address filter ... 4-24–4-26
Static MAC Configuration screen ... 4-25
Station Statistics screen ... 5-9
Storm Threshold ... 4-33
Storm Threshold Parameters Table ... C-40
Storm Threshold Table ... C-40
Subnet Mask field ... 2-8

Subnet Mask parameter ... 4-4
Supported Data Rates parameter ... C-30, C-31, C-32
Supported Frequency Channels parameter ... C-30, C-31
Syntax Error message ... C-2
Syslog Configuration screen ... 4-31
Syslog Host Table ... 4-32, C-39
Syslog Lowest Priority Logged parameter ... 4-32
Syslog Port Number parameter ... 4-32
Syslog configurations ... C-20
Syslog event notifications ... 4-31–4-32
Syslog messages ... 4-21, 4-31
Syslog parameters ... C-38
System Configuration screen ... 4-3
System Parameters Table ... C-26
System Status screen ... 2-8, 3-1, 6-1

T

TCP/UDP Port Filtering parameters ... C-37
TCP/UDP port filters ... 4-27
TFTP Server Parameter Table ... C-35
TFTP alarms ... 4-29
TFTP constant ... C-2
TFTP file transfers ... 6-3, 6-4, 6-7
TFTP servers
    defining IP addresses for ... 4-22, C-16
    downloading configuration files from ... C-16
    downloading software updates from ... 2-13, 6-4
    setting up ... 2-13
    troubleshooting ... 7-3, 7-11
    uploading configurations for ... 6-7, 6-8, C-8
TTL values ... 4-4
TX Power Control ... 4-8, C-15
Target IP Address Table ... 4-6
Technical Support ... 5-2
Telnet (CLI) Password parameter ... 4-17
Telnet Interface Bitmask parameter ... 4-20
Telnet Parameters Table ... C-34
Telnet Port parameter ... 4-20
Telnet configurations ... 4-20, 7-3
Telnet connections ... 7-3, C-12
Telnet session timeouts ... C-20
Time to Live (TTL) option ... 4-4
Transmission Mode ... C-19
Transmit Rate parameter ... C-30, C-31, C-32

U

UDP ports ... 4-27
Update AP by way of HTTP screen ... 6-5
Update AP by way of TFTP screen ... 6-4
Upgrade Kits ... A-4, A-8
Upload Unsuccessful message ... C-2

V

VLAN (defined) ... 4-47
VLAN ID Table ... C-24, C-44
VLAN Management IDs ... 4-50, 4-51
VLAN Management parameters ... C-24
VLAN User IDs ... 4-50, 4-51
VLAN assignments ... 4-48
VLAN configurations ... 4-47–4-51, 7-4, C-24
VLAN/SSID pairs ... 4-49, 4-50
VLAN/SSID parameters ... C-24, C-44
Version Information screen ... 5-2

W

WDS ports ... 4-15
WEP encryption ... 4-34, 4-35, 4-37, B-1, C-15
WEP encryption parameters ... C-41
WEP keys *See* encryption keys
WPA mode ... 4-36, 4-38
WPA security measures ... 4-35–4-36
WPA-PSK (Pre-Shared Key) option ... 4-36, 4-38
WPA-PSK Mode ... C-21, C-41
Web browsers ... 2-2, 7-3
Web interfaces ... 1-2, 4-18, 4-28
Wi-Fi Protected Access (WPA) ... 4-35
Windows operating systems ... 2-6
Wired Equivalent Privacy *See* WEP encryption
Wireless Distribution System (WDS) parameters ... C-32
Wireless Distribution Systems (WDS)
    configuring ... 4-7
    overview ... 4-15–4-16, 4-38
Wireless Interface Configuration screen ... 4-9, 4-10
Wireless Operational Mode parameter ... C-32
Wireless Threshold parameter ... 4-33

Z

access controls ... 4-27
access restrictions ... 4-17, 4-24
accessing networks ... 1-1, 4-39, 4-43
accounting information ... 5-5
accounting server (RADIUS) ... 4-43, 4-46, C-22, C-23
administrators ... 1-1
advanced filtering options ... 4-27
alarm groups ... 4-28
alarms ... 4-28–4-30, 4-41
alarms parameters ... C-38
antenna adapter ... 1-8
antennas ... 1-8, 4-41, A-7, C-23
assigning IP addresses ... 2-6, 2-7, 7-10
authentication ... 4-18, 4-34–4-35
authentication information ... 5-5
authentication modes ... 4-35, 4-36, C-21
authentication servers (RADIUS) ... 2-1, 4-43, 7-11, C-22
authorization lifetime ... 4-43, C-22

autochannel select (ACS) ... C-18, C-30
auto-duplex setting ... 4-16
automatic configurations ... 4-21–4-23, C-16
automatic key distribution ... 4-34
background scanning ... 4-41, C-23
backing up configurations ... C-16
backing up files ... 2-13
back-up servers ... 2-1, 4-43, 4-45
bandwidth ... 4-11, 4-26, 4-33, 4-49
blank space characters (strings) ... C-12
blocking access to services ... 4-27
bridge ... 4-32, 5-4
bridge parameters ... C-39
browsers *See* Web browsers
build numbers ... 5-2
calculating distance between APs ... C-19
cautions (documentation) ... 1-ii
cell capacities ... 4-11
certificate files ... 6-4, 6-5
certificates ... 1-2, 4-19, C-20
changing
  IP addresses ... 7-10, C-9, C-10
  TCP/UDP port filters ... 4-27
  encryption keys ... 4-37, 4-38
  interface settings ... C-18
  network adapters ... 2-7
  parameters ... C-6, C-8
  passwords ... 4-17, C-7, C-13
channel frequencies ... 1-6, A-4–A-7
channel restrictions ... 1-6
channel selection ... 4-9
client handovers ... 5-4
clients ... C-17
  assigning IP addresses to ... 4-5, 4-6
  assigning management access to ... 4-50
  assigning network names to ... 2-1
  assigning to workgroups ... 4-49
  blocking wireless ... 4-24, 4-25
  controlling access for ... 4-27
  getting information about ... 5-9
  limiting communications for ... 4-33
  operational modes for ... 4-8
  redirecting traffic for ... 4-33
  setting encryption keys for ... C-15
  setting host groups for ... 4-47
  setting up DHCP ... 4-4
  setting up DNS ... 4-4
  testing connection strength for ... 5-7
  tracking session lengths for ... 4-46
closed systems ... 4-9, C-18
coldStart trap ... 4-30
collisions ... 4-10
command list ... C-4
command reference ... C-4–C-11
command statements
  adding parameters to ... C-9, C-11
  adding strings to ... C-12
  entering ... C-1, C-7
  moving through ... C-2, C-6
  overview ... 1-2
comments ... C-9
communication ports ... C-20
communication requirements ... 2-1
communications information ... 5-4
configuration alarm ... 4-28
configuration files
  IP addresses and ... 4-22
  backing up ... C-16
  defined ... C-1
  downloading ... 6-4, 6-5, C-16
  uploading ... 2-13, 6-7, 6-8, C-8
configuration interface ... 1-2
configuration parameters ... 4-2, C-13, C-17, C-27
configurations
  defining with CLI commands ... C-12, C-13, C-17
  overwriting ... 6-11
  resetting ... 7-6
  saving ... 4-2, 6-9, 6-10, C-9
  setting DNS client ... C-17
  setting authentication server ... 4-43, 4-44, 4-46, C-22
  setting communication port ... C-20
  setting management port ... C-19
  setting through HTTP/HTTPS ... 4-1
  setting up automatic ... 4-21, C-16, C-35
  setting wireless interface ... 4-7
  troubleshooting ... 7-2, 7-4
connections
  configuring Ethernet ... C-19
  losing ... 4-6, 6-10, 7-4
  maintaining ... C-18
  setting properties for ... C-12
  testing ... 5-7
  troubleshooting ... 7-2, 7-4
conserving bandwidth ... 4-33, 4-49
control-key sequences ... C-2, C-6
conversion rules (system names) ... 4-3
copying help files ... 6-12
corrupted images ... 7-5, 7-6
coverage ... 4-12, 4-41, C-19
coverage area ... 1-7, C-23
creating
  filters ... 4-25
  parameter tables ... C-11
critical alarms ... 4-30
current IP address ... 4-4
current operating channel ... 4-9
customer assistance ... 5-2
data encryption *See* encryption
data overload ... 4-33
data packets *See* packets
data transmission rates ... 1-4, 1-7, 4-12, A-7

Index

default IP addresses ... 2-6, 4-4
default SSL passphrase ... 4-19
default TTL value ... 4-4
default configurations ... 4-3
default passwords ... 2-1
default ports ... 2-1, 4-18, 4-20
default router ... C-27
default subnet masks ... 4-4
defaults, resetting ... 6-11, 7-1, 7-6
deleting table entries ... C-10, C-11
delimiters (CLI strings) ... C-12
deployments ... 4-41, C-23
detecting Access Points ... 4-41
diagnostics ... 5-1
digital certificates ... 6-4, 6-5
directional antennas ... 4-41, C-23
disabling
  CLI table entries ... C-10, C-11
  VLAN Management IDs ... 4-51
  alarm groups ... 4-28
  proxy settings ... 2-8, 4-1, 6-1
displaying
  CLI commands ... 6-1, C-4
  CLI parameters ... C-4, C-5, C-8, C-11
  HTTP configuration information ... C-20
  IP addresses ... C-11
  MAC addresses ... 5-4
  on-line help ... 6-12, 7-3
  operating statistics ... 5-1, C-24
  station statistics ... 5-9
  system information ... 3-1, C-13
  version information ... 5-2, 6-7
documentation conventions ... 1-ii, C-1
domains ... C-27, C-31
done command ... C-6, C-9
double quote (") characters ... C-12
download (defined) ... C-1
download command ... C-6, C-35
downloading
  configuration files ... 6-4, 6-5, C-16
  help files ... 6-12
  image files ... 6-4, 6-5, 7-7, 7-8
  software ... 2-6, 2-13
  specified files ... C-6
drivers ... 7-4
dual-radio APs ... 4-35, C-18, C-21, C-41
dynamic DNS (DDNS) ... 4-3
dynamic IP addresses ... 4-3, 4-4, 4-22
electrical devices ... 4-11
encoding rules (names) ... 4-3
encrypted data ... 2-1
encryption ... 1-2, 4-18, 4-19, C-15
encryption certificates ... 4-19
encryption keys ... 2-10, 4-34, 4-37, B-1, C-15
encryption modes ... 4-34
encryption parameters ... C-41
environmental specifications ... A-3
error messages (CLI) ... C-2
event logs ... 4-31
event messages ... 4-31
event notifications ... 4-31–4-32
exit command ... C-6, C-9
factory defaults ... 6-11, 7-1, 7-6
file names ... 6-7
file sharing ... 4-33
file transfer ... 2-13, 6-3, C-1
file types ... 6-4, 6-5
files
  backing up configuration ... C-16
  downloading configuration ... 6-4, 6-5, C-16
  downloading specific ... C-6
  downloading updated software ... 2-13, 6-4, 6-5
  logging system messages to ... 4-31
  uploading configuration ... 6-7, 6-8, C-8
  uploading program ... 2-13
filtering parameters ... 4-24, 4-27, C-36
finding IP addresses ... 2-6
firewalls ... 4-33
forced reloads ... 7-6–7-7
forgetting passwords ... 7-1, 7-6
frequency bands ... A-4, A-6
frequency channels ... 1-6, A-4–A-7
full-duplex setting ... 4-16
gaming ... 4-33
gateways ... 4-33
groups ... C-1, C-10, C-24
half-duplex setting ... 4-16
hardware installation ... 2-3, 2-14
hardware specifications ... A-3
help ... C-34
help command ... C-3, C-6
help files ... 6-12, 7-3
high density areas ... 4-12
high-density cells ... 4-12
high-speed wireless layers ... 1-4
history command ... C-7
host groups ... 4-47
host names ... 4-3, 4-4
hosts ... 7-4, C-39
image alarms ... 4-30
image files
  defined ... C-2
  downloading ... 6-4, 6-5, 7-7, 7-8
  error checking for ... 6-3
  setting paths for ... 2-13
images
  deleting ... 7-5, 7-6
  replacing ... C-2
  upgrading ... 4-3
immediate reboots ... 6-10, C-7, C-9
in-band management access ... 4-17
informational alarms ... 4-30
informational messages ... C-9

initializing
AP 520wl ... 1-1, 2-6
IP addresses ... 7-9
installation ... 2-3, 2-14, 7-1
installation prerequisites ... 2-1
installed components ... C-27
interface detection ... 5-4
interface parameters ... C-30
interference ... 4-11, 5-8, A-7, C-18, C-19
interference controls ... 4-9
invalid image states ... 6-3
ipaddr parameter ... C-9
keyboard functions ... C-2, C-6
link integrity checks ... 4-6, C-18
linkDown trap ... 4-30
linkUp trap ... 4-30
links ... 4-15, 7-5
literal strings ... C-12
load balancing ... C-18
locale-specific help ... 6-12, C-34
locating IP addresses ... 2-6
logging into
HP Procurve Wireless ... C-12
HTTP interface ... 2-8, 6-1
logging system messages ... 4-31
logical WDS ports ... 4-15
loops ... 4-32
losing
connections ... 4-6, 6-10, 7-4
passwords ... 7-1, 7-2
low density areas ... 4-12
low-density cells ... 4-12
major alarms ... 4-30
management interfaces ... 1-2, 2-10
management parameters ... 4-17, C-27, C-33
management services ... 4-18, C-19
management stations ... 4-50
manual overrides ... 7-5
manual site surveys ... C-19
masks ... 4-24
See also subnet masks
medium density distribution ... C-18
memory alarms ... 4-29
messages ... 2-1, 2-12, 4-31, 5-3
missing images ... 7-7, 7-8
monitoring interfaces ... 1-2
monitoring parameters ... C-24
monitoring station statistics ... 5-9–5-10
monitoring system status ... 2-8, 4-31
mounting instructions ... 2-3
multicast rates ... 2-12, 4-12–4-13, C-19
multiple frame copies ... 4-32
naming conventions ... 4-3
naming host systems ... 4-3
navigation keys ... C-2, C-6
network adapters ... 2-7
network administrators ... 1-1
network bridging ... 4-32, 5-4, C-39
network objects ... C-24
networking concepts ... 1-1
networks
accessing ... 1-1, 4-39, 4-43
assigning IP addresses to ... 4-5
assigning host names to ... 4-4
caution for enabling DHCP servers and ... 4-5
configuration options for ... 4-4
data overload and ... 4-33
displaying parameter groups for ... C-10
installation prerequisites for ... 2-1
losing connections to ... 4-6, 6-10
monitoring ... 2-8
multiple Access Points and ... 4-39, C-21
nonexistent hosts and ... 7-4
optimizing performance for ... 4-24, 4-41
redundant communication loops in ... 4-32
resetting configurations for ... 7-6
segmenting ... 4-47
setting names for ... C-14
transferring files across ... 2-13, 6-3
troubleshooting connections for ... 7-2, 7-4
newRoot trap ... 4-30
noise ... 5-8
nonexistent hosts ... 7-4
notes (documentation) ... 1-ii
on-line help files ... 6-12, 7-3
operating channels ... 4-9
operating statistics ... 2-8, C-24
operating systems ... 2-6
operational alarms ... 4-29
operational commands ... C-4
operational mode ... C-18
operational modes (802.11b/g wireless) ... 2-12
optimizing network performance ... 4-24, 4-41
overload ... 7-5
overwriting configurations ... 6-11
packet forwarding ... 4-33, C-40
packet lifetime ... 4-4
packet size ... 4-10
packet transmission rates ... 4-12
packets ... 4-24, 4-49
parameter control commands ... C-8
parameter groups ... C-1, C-24
parameter tables ... C-2, C-24

Index

parameters
  adding to tables ... C-35
  case sensitivity for ... C-1
  changing ... C-6, C-8
  creating filters and ... 4-25
  defined ... C-2
  displaying ... C-4, C-5, C-8, C-11
  entering in statements ... C-9, C-11
  optional table elements and ... C-9
  resetting ... 7-6
  searching for ... C-7
  setting CLI monitoring ... C-24
  setting configuration ... 4-2, C-13, C-17
  setting with Bootloader CLI ... C-3
  viewing groups ... C-10
  viewing subset of ... C-5
  viewing values of ... C-8
passphrase ... 1-2, 4-19, C-20, C-41
passwd command ... C-7
passwords
  changing ... 4-17, C-7, C-13
  entering ... 2-8, 2-10
  forgetting ... 7-1, 7-6
  losing ... 7-1, 7-2
  requirements for ... 2-1
  setting ... 4-17
peer-to-peer file sharing ... 4-33
performance ... 4-24, 4-41, C-20
pinging ... 7-4
placing wireless devices ... 1-1, 4-11, C-19, C-31
plenum installations ... 2-14
point-to-point links ... 4-15
polling intervals ... 4-6
pool ... 2-1, 4-5, C-17, C-28
port filters ... 4-27, C-37
port-based filtering ... 4-27
ports
  IEEE specifications for ... 4-34
  configuring management ... C-19
  mapping WDS links to ... 4-15
  setting HTTP access ... 4-18
  setting IP addresses from serial ... 7-9
  setting authentication server ... 2-1
  setting communication ... C-20
power supply ... 2-3
private key files ... 6-4, 6-5
private keys ... 1-2, 4-19, C-20
prompts ... C-6
protocol filters ... C-36
proxy settings ... 2-8, 4-1, 6-1
quit command ... C-6, C-9
radiation ... 1-8
radio interfaces ... 4-15
radio parameters ... 4-14
radio specifications ... A-4
range ... A-7, A-9
reboot command ... C-3, C-7
reboots ... 6-10, C-7, C-9
recording MAC addresses ... 4-32
recovery procedures ... 7-5
redirecting traffic ... 4-33
registering host names ... 4-3
regulatory domains ... 4-9
removing table entries ... C-10, C-11
resets ... 6-10
resetting
  factory defaults ... 6-11, 7-1, 7-6
  network configurations ... 7-6
resources ... 4-49
roaming ... 1-1, 1-2, 4-46, C-45
router ... C-27
safety ... 1-ii, 2-14
saving configurations ... 4-2, 6-9, 6-10, C-9
scan repetition duration ... 4-41, C-23
scanning functions ... 4-41, C-23
scripts ... 1-2
search command ... C-7
secure management options ... 1-2, 1-3, 4-18
secure management parameters ... C-33
security ... 1-3, 2-1, 4-34, C-23
security alarms ... 4-28, 4-30
security modes ... 4-36–4-39
security parameters ... C-41
serial numbers ... 5-2
serial port cables ... 7-9
serial port interface ... 4-20, 7-1, A-4, C-20
serial ports ... 7-9
session timeouts (Telnet) ... C-20
set command ... C-3, C-8, C-9, C-11
setup parameters ... C-3
severity levels (alarms) ... 4-30
show command ... C-3, C-8, C-9, C-24
signal strength ... 5-7, 7-4, A-7, C-19
single quote (') characters ... C-12
site surveys ... 1-1, C-19
software downloads ... 2-6
software images *See* images
software updates ... 2-13, 6-4, 6-5
special key functions ... C-2, C-6
specifications ... A-1
static IP addresses ... 1-1, 2-7, C-13, C-16
static IP configurations ... 4-21
statistical information ... 2-8
status information ... 2-8
string delimiters ... C-12
strings ... C-12
subnet masks ... 4-4, 4-17, 7-6, C-13
sub-network configurations ... 4-47
subscriber blocking ... C-40
subscribers *See* wireless clients
support ... 5-2
system alarms ... 4-28–4-30
system information ... C-13
system messages ... 4-31

system names ... 2-1, 4-3
system requirements ... 2-2
system status ... 4-31
table names ... C-11
tables
See also parameters
adding entries to ... C-9, C-35
changing elements in ... C-10, C-11
creating ... C-11
deleting elements in ... C-10, C-11
displaying all elements in ... C-10
displaying parameters in ... C-8, C-11
inserting rows ... C-9
overview ... C-11, C-24
searching for parameters in ... C-7
telnet command ... C-12
terminal emulation programs ... 7-9, C-12
testing
connections ... 5-7
image downloads ... 6-3
text strings ... C-12
text-based configurations ... C-8
thresholds ... 4-33
throughput ... 4-16, 4-49
timed reboots ... C-7
topologyChange trap ... 4-30
transmission rates ... 1-4, 1-7, A-7
transmit power levels ... 4-8, C-15
transmitter ... 1-8
transmitting data packets ... 4-10, 4-12, 4-24, 4-49
traps ... 4-28–4-30, 4-41
troubleshooting ... 4-31, 7-1
unauthenticated client PCs ... 4-35
unauthorized communications ... 4-33
unauthorized users ... 2-10, 4-34
unavailable channels ... A-4, A-6
unexpected performance issues ... C-20
updating HP ProCurve Wireless AP 520wl ... 2-13, 6-4, 6-5
upgrades ... 2-2, 4-3
upload (defined) ... C-1
upload command ... C-8, C-35
uploading
SSL certificates ... 4-19
certificate/private key pairs ... C-20
configuration files ... 2-13, 6-7, 6-8, C-8
private keys ... 4-19
user authentication *See* authentication
verifying IP addresses ... 7-10
version information ... 5-2, 6-7
viewing
CLI commands ... 6-1, C-4
CLI parameters ... C-4, C-5, C-8, C-11
HTTP configuration information ... C-20
IP addresses ... C-11
MAC addresses ... 5-4
on-line help ... 6-12, 7-3
operating statistics ... 5-1, C-24
station statistics ... 5-9
system information ... 3-1, C-13
version information ... 5-2, 6-7
virtual LAN *See* VLAN
warranty ... 1-ii
wireless LANs (WLANs) ... 4-34
See also networks
wireless access point units *See* HP ProCurve Wireless
wireless alarms ... 4-28
wireless backbone setup ... 4-16
wireless clients
assigning IP addresses to ... 4-5, 4-6
assigning management access to ... 4-50
assigning network names to ... 2-1
blocking ... 4-24, 4-25
configuring DNS ... C-17
controlling access for ... 4-27
enabling subscriber blocking for ... C-40
getting information about ... 5-9
limiting communications for ... 4-33
operational modes for ... 4-8
redirecting traffic for ... 4-33
setting encryption keys for ... C-15
setting host groups for ... 4-47
testing connection strength for ... 5-7
tracking session lengths for ... 4-46
wireless interface
changing settings for ... C-18
configuring ... 2-10, 4-7
disabled ... 4-6
enabling TX Power Control for ... C-15
getting information about ... 5-4, 5-6
operational modes for ... 2-12
setting encryption for ... C-15
setting network names for ... C-14
setting security modes for ... 4-36
setting up virtual LANs for ... 4-48
wireless interface configuration parameters ... C-30–C-32
wireless interface security parameters ... C-41
wireless signal ... A-7
workgroups ... 4-49, 7-4
’ (single quote) characters ... C-12