9160 G2
Wireless Gateway

User Manual

November 24, 2006   Part No. 8100117.A

ISO 9001 Certified
Quality Management System

PSION TEKLOGIX

Return-To-Factory Warranty

Psion Teklogix Inc. provides a return to factory warranty on this product for a period of twelve (12) months in accordance with the Statement of Limited Warranty and Limitation of Liability provided at www.psionteklogix.com/warranty. (If you are not already a member of Teknet and you attempt to view this warranty, you will be asked to register. As a member of Teknet, you will have access to helpful information about your Psion Teklogix products at no charge to you.) In some regions, this warranty may exceed this period. Please contact your local Psion Teklogix office for details. For a list of offices, see Appendix A: "Support Services And Worldwide Offices". The warranty on Psion Teklogix manufactured equipment does not extend to any product that has been tampered with, altered, or repaired by any person other than an employee of an authorized Psion Teklogix service organization. See Psion Teklogix terms and conditions of sale for full details.

Important: ***Psion Teklogix warranties take effect on the date of shipment.***

Service

Psion Teklogix provides a complete range of product support services to its customers. For detailed information, please refer to Appendix A: "Support Services And Worldwide Offices". This section also provides information about accessing support services through the Psion Teklogix web site.

Waste Electrical and Electronic Equipment (WEEE) Directive 2002/96/EC

This Product, and its accessories, comply with the requirements of the Waste Electrical and Electronic Equipment (WEEE) Directive 2002/96/EC. If your end-of-life Psion Teklogix product or accessory carries a label as shown here, please contact your local country representative for details on how to arrange recycling.

For a list of international subsidiaries, please go to:

***www.psionteklogix.com/public.aspx?s=us&p=Contacts*.**

Restriction On Hazardous Substances (RoHS) Directive 2002/95/EC

What is RoHS?

The European Union has mandated that high environmental standards be met in the design and manufacture of electronic and electrical products sold in Europe, to reduce hazardous substances from entering the environment. The "Restriction on Hazardous Substances Directive (RoHS)" prescribes the maximum trace levels of lead, cadmium, mercury, hexavalent chromium, and flame retardants PBB and PBDE that may be contained in a product. Only products meeting these high environmental standards may be "placed on the market" in EU member states after July 1, 2006.

RoHS Logo

Although there is no legal requirement to mark RoHS-compliant products, Psion Teklogix Inc. indicates its compliance with the directive as follows:

The RoHS logo located either on the back of the product or underneath the battery in the battery compartment (or on a related accessory such as the charger or docking station) signifies that the product is RoHS-compliant as per the EU directive. Other than as noted below, a Psion Teklogix product that does not have an accompanying RoHS logo signifies that it was placed on the EU market prior to July 1, 2006, and is thereby exempt from the directive.

Note: *Not all accessories or peripherals will have a RoHS logo due to physical space limitations or as a result of their exempt status.*

Disclaimer

Every effort has been made to make this material complete, accurate, and up-to-date. In addition, changes are periodically added to the information herein; these changes will be incorporated into new editions of the publication.

Psion Teklogix Inc. reserves the right to make improvements and/or changes in the product(s) and/or the program(s) described in this document without notice, and shall not be responsible for any damages, including but not limited to consequential damages, caused by reliance on the material presented, including but not limited to typographical errors.

TABLE OF CONTENTS

Chapter 3: PreLaunch Checklist

Chapter 4: Quick Steps For Setup And Launch

Chapter 5: Configuring Basic Settings

Chapter 6: Managing Access Points & Clusters

Chapter 7: Managing User Accounts

Chapter 8: Channel Management

Chapter 9: Wireless Neighborhood

Chapter 10: Configuring Security

Chapter 11: Maintenance And Monitoring

Chapter 12: The Ethernet (Wired) Interface

Chapter 13: Setting the Wireless Interface

Chapter 14: Setting up Guest Access

Chapter 15: Configuring VLANs

Chapter 16: Configuring 802.11 Radio Settings

Chapter 17: MAC Address Filtering

Chapter 18: Load Balancing

Chapter 19: Quality of Service (QoS)

Chapter 20: Wireless Distribution System

Chapter 21: Configuring SNMP

Chapter 22: The 9160 G2 As Base Station

Chapter 23: Network Time Protocol Server

Chapter 24: Backing Up & Restoring Configuration

Chapter 25: Specifications

Appendices

Appendix A: Support Services And Worldwide Offices

Appendix B: Port Pinouts And Cable Diagrams

Appendix C: Security Settings On Wireless Clients And RADIUS Server Setup

Appendix D: Troubleshooting

Approvals and Safety Summary

Declaration Of Conformity

Product:	**9160 G2 Wireless Gateway**
Application of Council Directives:	EMC Directive:89/336/EEC Low Voltage Directive:73/23/EEC R&TTE Directive: 1999/5/EEC
Conformity Declared to Standards:	EN 55022: 2003 Class B EN 61000-3-2; EN 61000-3-3 EN 55024:2003 ETSI EN 300 328:2003 ETSI EN 301 489-17:2002 EN 60950-1: 2001
Manufacturer:	PSION TEKLOGIX INC. 2100 Meadowvale Blvd. Mississauga, Ontario; Canada L5N 7J9
Year of Manufacture:	2005
Manufacturer's Address in the European Community:	PSION TEKLOGIX S.A. La Duranne 135 Rue Rene Descartes; BP 421000 13591 Aix-En-Provence Cedex 3; France
Type of Equipment:	Information Technology Equipment
Equipment Class:	Commercial and Light Industrial

FCC Statement

FCC Declaration Of Conformity (DoC)

Applicant’s Name & Address:
PSION TEKLOGIX
2100 Meadowvale Blvd.
Mississauga, Ontario, Canada L5N 7J9
Telephone No.: (905) 813-9900

US Representative’s Name & Address:
Psion Teklogix Corp.
1810 Airport Exchange Blvd., Suite 500
Erlanger, Kentucky, 41018, USA
Telephone No.: (859) 372-4329

Equipment Type/ Environment Use: Computing Devices

Trade Name / Model No.: **9160 G2 Wireless Gateway**

Year of Manufacture: 2005

Standard(s) to which Conformity is Declared:

The **9160 G2 Wireless Gateway**, supplied by Psion Teklogix, has been tested and found to comply with **FCC PART 15, SUBPART B - UNINTENTIONAL RADIATORS, CLASS B COMPUTING DEVICES FOR HOME & OFFICE USE**.

Applicant:
Psion Teklogix Inc.
Mississauga, Ontario, Canada

Legal Representative in US:
Psion Teklogix Corp.
Erlanger, Kentucky, USA

The 9160 G2 Wireless Gateway has been tested and found to comply with the specifications for a Class B digital device, pursuant to 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.

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 according to 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 is found 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 or devices.
- Connect the equipment to an outlet other than the receiver's.
- Consult a dealer or an experienced radio/TV technician for assistance.

FCC Caution: ***Any change or modification to the product not expressly approved by Psion Teklogix could void the user's authority to operate the device.***

RF Radiation Exposure Statement

To comply with the FCC and ANSI C95.1 RF exposure limits, the antenna(s) for this device must comply with the following:

- All Access Point antennas must operate with a separation distance of at least 25 cm (9.8 in.) from all persons using the cable provided, and must not be co-located or operating in conjunction with any other antenna or transmitter.
- The Gabriel dish antenna (P/N 9002006) requires a minimum separation distance of 63.2 cm (24.9 in.).

Note: *Dual antennas used for diversity operation are not considered co-located.*

Industry Canada (IC) Department Of Communications Notice

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210. “To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.”

Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada. “Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence.”

Safety Approvals

CSA, NRTL/C and CB.

CE Marking

When used in a residential, commercial or light industrial environment, the product and its approved UK and European peripherals fulfill all requirements for CE marking.

R&TTE Directive 1999/5/EC

This equipment complies with the essential requirements of EU Directive 1999/5/EC (Declaration available: *www.psionteklogix.com*).

Cet équipement est conforme aux principales caractéristiques définies dans la Directive européenne RTTE 1999/5/CE. (Déclaration disponible sur le site: *www.psionteklogix.com*).

Die Geräte erfüllen die grundlegenden Anforderungen der RTTE-Richtlinie (1999/5/EG). (Den Wortlaut der Richtlinie finden Sie unter: *www.psionteklogix.com*).

Questa apparecchiatura è conforme ai requisiti essenziali della Direttiva Europea R&TTE 1999/5/CE. (Dichiarazione disponibile sul sito: *www.psionteklogix.com*).

Este equipo cumple los requisitos principales de la Directiva 1995/5/CE de la UE, “Equipos de Terminales de Radio y Telecomunicaciones”. (Declaración disponible en: *www.psionteklogix.com*).

Este equipamento cumpre os requisitos essenciais da Directiva 1999/5/CE do Parlamento Europeu e do Conselho (Directiva RTT). (Declaração disponível no endereço: *www.psionteklogix.com*).

Ο εξοπλισμός αυτός πληροί τις βασικές απαιτήσεις της κοινοτικής οδηγίας EU R&TTE 1999/5/EK. (Η δήλωση συμμόρφωσης διατίθεται στη διεύθυνση: *www.psionteklogix.com*)

Deze apparatuur voldoet aan de noodzakelijke vereisten van EU-richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur 199/5/EG. (verklaring beschikbaar: *www.psionteklogix.com*).

Dette udstyr opfylder de Væsentlige krav i EU's direktiv 1999/5/EC om Radio- og teleterminaludstyr. (Erklæring findes på: *www.psionteklogix.com*).

Dette utstyret er i overensstemmelse med hovedkravene i R&TTE-direktivet (1999/5/EC) fra EU. (Erklæring finnes på: *www.psionteklogix.com*).

Utrustningen uppfyller kraven för EU-direktivet 1999/5/EC om ansluten teleutrustning och ömsesidigt erkännande av utrustningens överensstämmelse (R&TTE). (Förklaringen finns att läsa på: *www.psionteklogix.com*).

Tämä laite vastaa EU:n radio- ja telepäätelaitedirektiivin (EU R&TTE Directive 1999/5/EC) vaatimuksia. (Julkilausuma nähtävillä osoitteessa: *www.psionteklogix.com*).

Psion Teklogix tímto prohlašuje, že 9160 G2 Wireless Gateway je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1995/5/ES (NV č. 426/2000 Sb.) a Prohlášení o shodě je k dispozici na *www.psionteklogix.com*.

Toto zarízení lze provozovat v České republice na základě generální licence č. GL-12/R/2000.

Psion Teklogix týmto vyhlasuje, že 9160 G2 Wireless Gateway spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1995/5/ES (NV č. 443/2001 Z.z.) a Vyhlásenie o zhode je k dispozícii na *www.psionteklogix.com*.

Toto zariadenie je možné prevádzkovat' v Slovenskej republike na základe Všeobecného povolenia č. VPR-01/2001.

Important Safety Instructions

This safety information is for the protection of both operating and service personnel.

- The 9160 G2 must be installed by a qualified Psion Teklogix installer—failure to have the 9160 G2 properly installed will void the Manufacturer’s warranty.
- The mains power cord (if sold separately) shall comply with National safety regulations of the country where the equipment is to be used.
- Use of an attachment not recommended or sold by manufacturer may result in fire, electric shock, or personal injury.
- To reduce risk of damage to the electric plug and cord when unplugging the 9160 G2, pull the plug rather than the cord.
- Make sure the cord is positioned so that it is not stepped on, tripped over, or otherwise subjected to damage or stress.
- Do not operate the 9160 G2 with a damaged cord or plug. Replace immediately.

- Do not operate the 9160 G2 if it has received a sharp blow, been dropped, or otherwise damaged in any way; it should be inspected by qualified service personnel.
- Do not disassemble the 9160 G2; it should be repaired by qualified service personnel. Incorrect reassembly may result in electric shock or fire.
- To reduce risk of electric shock, unplug the 9160 G2 from the outlet before attempting any maintenance or cleaning.
- An extension cord should not be used unless absolutely necessary. Use of an improper extension cord could result in fire or electric shock. If an extension cord must be used, make sure:
    - The plug pins on the extension cord are the same number, size, and shape as those on the adaptor.
    - The extension cord is properly wired, in good electrical condition, and that the wire size is larger than 16 AWG.
- The 9160 G2 is designed for indoor use only; do not expose the 9160 G2 to rain or snow.

Do Not Operate In An Explosive Atmosphere

Operating Psion Teklogix equipment where explosive gas is present may result in an explosion.

Do Not Remove Covers Or Open Enclosures

To avoid injury, the equipment covers and enclosures should only be removed by qualified service personnel. Do not operate the equipment without the covers and enclosures properly installed.

Do Not Hold Antenna

To avoid discomfort due to the local heating effect of radio frequency energy, do not touch the antenna when a 9160 G2 is transmitting.

Connection to Outdoor Antenna

The outdoor antenna shall only be installed by Psion Teklogix service professionals.

INTRODUCTION 1

1.1 About This Manual

This manual describes the setup, configuration, administration, and maintenance of one or more 9160 G2 Wireless Gateways on a wireless network.

Chapter 1: Introduction
provides an overview of this manual and 9160 G2 Wireless Gateway features.

Chapter 2: Installation Requirements
explains the physical installation of the 9160 G2 Wireless Gateway, and how to connect to the 9160 G2 for diagnostics.

Chapter 3: PreLaunch Checklist
provides a quick check of required hardware components, software, client configurations, and compatibility issues.

Chapter 4: Quick Steps For Setup And Launch
is a step-by-step guide to setting up your 9160 G2 Wireless Gateways and the resulting wireless network.

Chapter 5: Configuring Basic Settings
provides instructions on configuring administrator access settings and new access point settings.

Chapter 6: Managing Access Points & Clusters
describes access point clusters and how to navigate to specific access points within clusters.

Chapter 7: Managing User Accounts
illustrates the user management capabilities for controlling client access to access points.

Chapter 8: Channel Management
describes how the 9160 G2 Wireless Gateway automatically assigns radio channels used by clustered access points to reduce mutual interference or interference with other access points outside of its cluster.

Chapter 9: Wireless Neighborhood
provides a detailed view of neighborhood access points, including identifying information, cluster status, and statistical information.

Chapter 10: Configuring Security
provides a number of authentication and encryption schemes to ensure that your wireless infrastructure is accessed only by the intended users. The details of each security mode are described.

Chapter 11: Maintenance And Monitoring
describes the maintenance and monitoring tasks for individual access points (not for cluster configurations).

Chapter 12: The Ethernet (Wired) Interface
describes how to configure the wired interface settings on the 9160 G2 Wireless Gateway.

Chapter 13: Setting the Wireless Interface
describes how to configure the wireless address and related settings on the 9160 G2 Wireless Gateway.

Chapter 14: Setting up Guest Access
allows you to configure the 9160 G2 Wireless Gateway for controlled guest access to an isolated network.

Chapter 15: Configuring VLANs
describes how to configure multiple wireless networks on Virtual LANs (VLANs).

Chapter 16: Configuring 802.11 Radio Settings
describes how to configure Radio Settings on the 9160 G2 Wireless Gateway

Chapter 17: MAC Address Filtering
instructs how you can use MAC address filtering to control client access to your wireless network.

Chapter 18: Load Balancing
describes how to configure Load Balancing on your wireless network, to allow you to balance the distribution of wireless client connections across multiple access points.

Chapter 19: Quality of Service (QoS)
provides instructions on configuring the parameters on multiple queues to improve the throughput and performance of differentiated wireless traffic.

Chapter 20: Wireless Distribution System
describes how to configure the Wireless Distribution System (WDS) on the 9160 G2 Wireless Gateway, enabling you to connect multiple access points which can then communicate with one another wirelessly in a standardized way.

Chapter 21: Configuring SNMP

describes how to configure SNMP and related settings on the 9160 G2 Wireless Gateway Enterprise-Manager API.

Chapter 22: The 9160 G2 As Base Station

describes how to configure the 9160 G2 Wireless Gateway as either a wired or wireless Base Station, or as a Remote Radio Module (RRM). This chapter also describes narrow band radio configuration settings.

Chapter 23: Network Time Protocol Server

describes how to configure the 9160 G2 Wireless Gateway to use a specified Network Time Protocol (NTP) server to synchronize computer clock times on your network.

Chapter 24: Backing Up & Restoring Configuration

shows how to backup a configuration file that can be used at a later date to restore the access point to the previously saved configuration.

Chapter 25: Specifications

details the physical, environmental, and various operating specifications for the 9160 G2 Wireless Gateway and its radios.

Appendix A: Support Services And Worldwide Offices

presents information for technical support, contacts, and the Psion Teklogix worldwide web address.

Appendix B: Port Pinouts And Cable Diagrams

includes pinouts and diagrams of the ports and cables for the 9160 G2.

Appendix C: Security Settings On Wireless Clients And RADIUS Server Setup

details how to configure security settings on the client to match the security mode being used by each network (AP) connection.

Appendix D: Troubleshooting

describes how to solve common problems possibly encountered while updating network configurations on networks served by multiple, clustered access points.

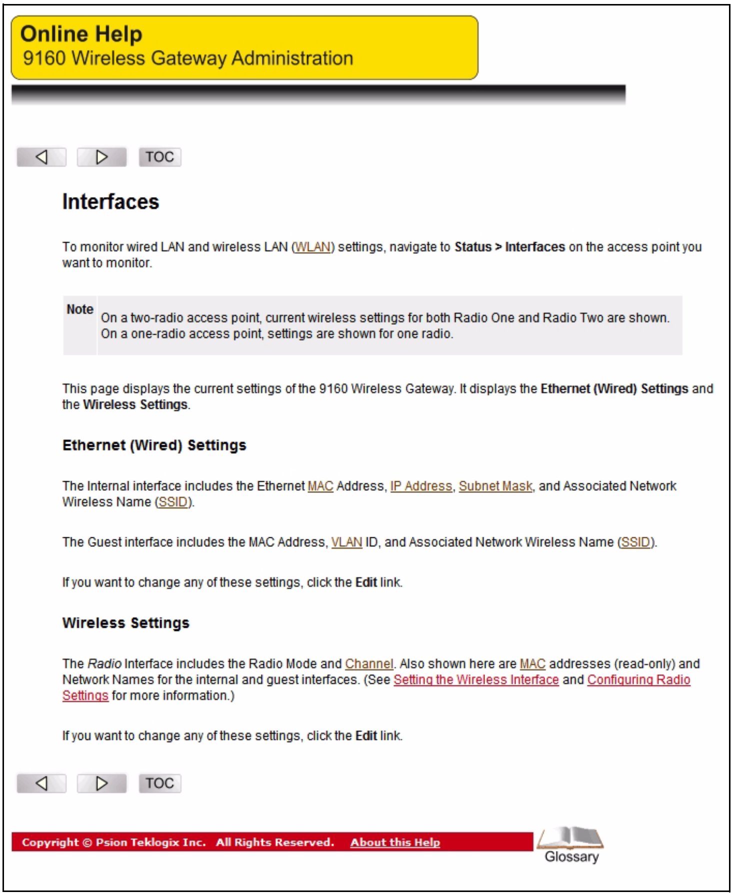
Appendix E: Glossary

provides definitions and further details on terms featured in bold italics throughout the manual.

1.2 Online Help Features, Supported Browsers, And Limitations

Online Help for the 9160 G2 Wireless Gateway provides information about all fields and features available on the user interface. The information in the Online Help is a subset of the information available in the full User Manual.

Online Help information corresponds to each tab on the 9160 G2 Wireless Gateway Administration user interface. Click the **Help** button on a tab or the “More. . .” link at the bottom of the online help panel on the UI for help information for the settings on the current tab.



Online Help
9160 Wireless Gateway Administration

Interfaces

To monitor wired LAN and wireless LAN (WLAN) settings, navigate to **Status > Interfaces** on the access point you want to monitor.

Note On a two-radio access point, current wireless settings for both Radio One and Radio Two are shown. On a one-radio access point, settings are shown for one radio.

This page displays the current settings of the 9160 Wireless Gateway. It displays the **Ethernet (Wired) Settings** and the **Wireless Settings**.

Ethernet (Wired) Settings

The Internal interface includes the Ethernet MAC Address, IP Address, Subnet Mask, and Associated Network Wireless Name (SSID).

The Guest interface includes the MAC Address, VLAN ID, and Associated Network Wireless Name (SSID).

If you want to change any of these settings, click the **Edit** link.

Wireless Settings

The *Radio* Interface includes the Radio Mode and Channel. Also shown here are MAC addresses (read-only) and Network Names for the internal and guest interfaces. (See Setting the Wireless Interface and Configuring Radio Settings for more information.)

If you want to change any of these settings, click the **Edit** link.

Copyright © Psion Teklogix Inc. All Rights Reserved. About this Help

1.3 Text Conventions

Note: *Notes highlight additional helpful information.*

Important: ***These statements provide particularly important instructions or additional information that is critical to the operation of the computer and other equipment.***

Warning: ***These statements provide important information that may prevent injury, damage to the equipment, or loss of data.***

▶ An arrow next to field description information (usually in tables) indicates a recommended or suggested configuration setting for an option on the ***Access Point*** (AP).

Bold Italics When you see a term written in ***bold italics***, there is an entry for it in Appendix E: Glossary, providing a definition and further details. Not all terms are highlighted in the manual, but the Glossary is extensive, therefore please check there for any unfamiliar words or expressions.

1.4 Overview Of The 9160 G2 Wireless Gateway

The 9160 G2 Wireless Gateway provides continuous, high-speed access between your wireless and Ethernet devices. It is an advanced, standards-based solution for wireless networking in small and medium-sized businesses. The 9160 G2 Wireless Gateway enables zero-administration wireless local area network (***WLAN***) deployment while providing state-of-the-art wireless networking features.

The 9160 G2 Wireless Gateway provides best-of-breed security, ease-of-administration and industry standards—providing a standalone and fully-secured wireless network without the need for additional management and security server software.

The 9160 G2 Wireless Gateway is designed to support a wide variety of system configurations. Using the IEEE 802.11 Wireless LAN Standards, the 9160 G2 is capable of operating as a transparent bridge (access point) between wireless and wired networks. This allows wireless clients to access the network and also move seamlessly between the 9160 G2s in the network. The 9160 G2 can also operate as a base station, a remote radio module (RRM), and become part of a mapRF system.

The following sections list features and benefits of the 9160 G2 Wireless Gateway, and tell you what's next for when you're ready to get started using the AP.

1.4.1 Radios

The 9160 G2 is capable of supporting single or dual radio operation. Available radio modules are the 802.11a/g radio, the 802.11g radio, and the RA1001A Narrow Band radio. For detailed specifications on these radios please see “Radios” on page 262.

Depending on the installed radio(s), the access point is capable of operating in the following modes:

- IEEE ***802.11b*** mode.
- IEEE ***802.11g*** mode.
- IEEE ***802.11a*** mode.
- Atheros Turbo 5 GHz.
- Atheros Dynamic Turbo 5 GHz.
- Atheros Turbo 2.4 GHz.
- Atheros Dynamic Turbo 2.4 GHz.
- Extended Range.
- Psion Teklogix Narrow Band Polling Protocol.

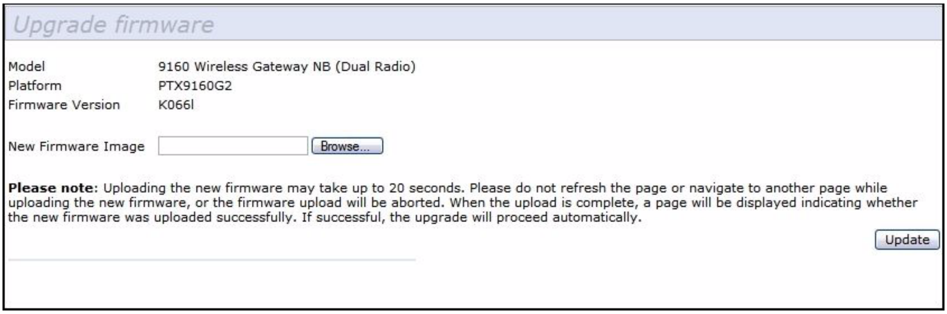
Important: ***Psion Teklogix terminals do not support Atheros Turbo modes and to prevent unnecessary radio overhead the use of Turbo mode is not recommended.***

The 9160 G2 Wireless Gateway supports four different radio configurations: *802.11g*, *802.11g + 802.11ag*, *NB* (narrow band), and *NB + 802.11ag*.

These different variants are identified by the “Model” value, which is shown on the *Maintenance > Upgrade* web page (see Figure 1.1 on page 9). The models are defined as follows:

- *9160 Wireless Gateway* = 802.11g.
- *9160 Wireless Gateway (Dual Radio)* = 802.11g + 802.11ag.
- *9160 Wireless Gateway NB* = NB.
- *9160 Wireless Gateway NB (Dual Radio)* = NB + 802.11ag.

Note: *For the 'NB only' case, the web page may show the configuration page for a single 802.11 radio. You can disregard it, however, if you should attempt to configure this non-existent radio, this will not cause problems in the 9160 G2.*



Upgrade firmware

Model	9160 Wireless Gateway NB (Dual Radio)
Platform	PTX9160G2
Firmware Version	K066l

New Firmware Image

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

Figure 1.1 Upgrade Firmware Web Page

1.4.2 Access Point Functions

As an access point connected to a wired network, the 9160 G2 Wireless Gateway forms a communication link between Psion Teklogix RF terminals or wireless access point clients and a Psion Teklogix Network Controller or a host computer. It communicates over an IEEE 802.11 RF data link with terminals, and over a cable with the network controller or a host computer. The 9160 G2 can be connected to the network through an Ethernet connection.

1.4.3 Base Station Functions

As a base station or Remote Radio Module (RRM), the 9160 G2 provides a link between the local area network and wireless mobile terminals using proprietary Psion Teklogix radio protocols. On the local area network the 9160 G2 base station (or RRM) communicates with a 9500 network controller (or host using a Psion Teklogix Software Development Kit) using the proprietary 9010 protocol over TCP/IP.

For information on configuring the 9160 G2 as a base station or RRM, see Chapter 22: "The 9160 G2 As Base Station".

1.5 Features and Benefits

1.5.1 IEEE Standards Support And Wi-Fi Compliance

- Support for ***IEEE 802.11a***, IEEE ***802.11b***, IEEE ***802.11g***, IEEE ***802.11i***, and IEEE ***802.3af*** wireless networking standards.
- Provides bandwidth of up to 54 Mbps for IEEE ***802.11a*** or IEEE ***802.11g*** (11 Mbps for IEEE ***802.11b***, 108 Mbps for Atheros ***802.11a Turbo***).
- Wi-Fi certification.

1.5.2 Wireless Features

- Auto channel selection at startup.
- Transmit power adjustment.
- Wireless Distribution System (***WDS***) for connecting multiple access points wirelessly. Extends your network with less cabling.
- Quality of Service (***QoS***) for enhanced throughput and better performance of time-sensitive wireless traffic like Video, Audio, Voice over IP (VoIP) and streaming media. Our QoS is Wi-Fi Multimedia (WMM) compliant.
- Load Balancing.
- Built-in support for multiple ***SSID***s (network names) and multiple ***BSSID***s (basic service set IDs) on the same access point.
  Two special-purpose BSSIDs are supported, one for the Internal (primary and management) network, and the other for the guest network. Six additional general-purpose BSSIDs (called Virtual Wireless Networks or VWNs) are supported using VLANs.
- Channel management for automatic coordination of radio channel assignments to reduce AP-to-AP interference on the network and maximize Wi-Fi bandwidth.
- Neighboring access point detection (also known as “rogue” AP detection).
- Support for ***IEEE 802.11d*** Regulatory Domain selection (country codes for global operation).

- Support for ***IEEE 802.11h***, incorporating TPC and DFS.
  IEEE 802.11h is a standard that provides two services required to satisfy certain regulatory domains for the 5 GHz band. These two services are Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS).
- Support for Extended Range (XR).
- SpectraLink Voice Priority (SVP).
  SpectraLink Voice Priority (SVP) is a QoS approach for Wi-Fi deployments. SVP is an open specification that is compliant with the IEEE 802.11b standard. SVP minimizes delay and prioritizes voice packets over data packets on the Wireless LAN, thus increasing the probability of better network performance.

1.5.3 Security Features

- Inhibit SSID Broadcast.
- Ignore SSID Broadcast.
- Weak IV avoidance.
- Wireless Equivalent Privacy (***WEP***).
- Wi-Fi Certified for the following standards:
  - IEEE Standards: 802.11b, 802.11g, 802.11d
  - Security:
    WPA™ - Personal
    WPA™ - Enterprise
    WPA2™ - Personal
    WPA2™ - Enterprise
  - EAP Types:
    EAP-TLS
    EAP-TTLS/MSCHAPv2
    PEAPv0/EAP-MSCHAPv2
    PEAPv1/EAP-GTC
    EAP-SIM
- Advanced Encryption Standard (***AES***).
- User-based access control with local authentication server.

- Local user database and user life cycle management.
- MAC address filtering.
- WPA/WPA2 over ***WDS***.
- Secure Sockets Shell (SSH).
- Secure Sockets Layer (SSL).

1.5.4 Out-of-the-Box Guest Interface

- Unique network name (***SSID***) for the Guest interface.
- Captive portal to guide guests to customizable, guest-only Web page.
- VLAN and ethernet options.

1.5.5 Clustering And Auto-Management

- Provisioning and auto-configuration of APs through clustering and cluster rendezvous.

  The administrator can specify how new access points should be configured before they are added to the network. When new access points are added, they can automatically rendezvous with the cluster, and securely download the correct configuration. The process does not require manual intervention, but is under the control of the administrator.
- Single universal view of clustered access points and cluster configuration settings.

  Configuration for all access points in a cluster can be managed from a single interface. Changes to common parameters are automatically reflected in all members of the cluster.
- Self-managed access points with automatic configuration synchronization.

  The access points in a cluster periodically check that the cluster configuration is consistent, and check for the presence and availability of the other members of the cluster. The administrator can monitor this information through the user interface.

- Enhanced local authentication using 802.1x without additional IT setup.

  A cluster can maintain a user authentication server and database stored on the access points. This eliminates the need to install, configure, and maintain a ***RADIUS*** infrastructure, and simplifies the administrative task of deploying a secure wireless network.

1.5.6 Networking

- Dynamic Host Configuration Protocol (***DHCP***) support for dynamically obtaining network configuration information.
- Virtual Local Area Network (VLAN) support.
- Virtual Wireless Networks (Dynamic VLANs).
- Spanning Tree Protocol (***STP***).
- ***802.1p***.

1.5.7 SNMP Support

The 9160 G2 Wireless Gateway includes the following standard Simple Network Management Protocol (***SNMP***) Management Information Bases (***MIB***s):

- Bridge MIB 802.1d (RFC 1493).
- SNMPv2 MIB (RFC 3418).
- IEEE Std 802.11 MIB (base).
- Interfaces Group MIB (RFC 2233).
- Two proprietary MIBs (Wireless MIB and System MIB), based on the upcoming IEEE 802.11k MIB. They provide information about the 9160 G2 Wireless Gateway client association list and AP detection table, respectively. The proprietary System MIB provides maintenance functionality such as system reboot or firmware upgrade.

1.5.8 Maintainability

- Status, monitoring, and tracking views of the network including session monitoring, client associations, transmit/receive statistics, and event log.
- Link integrity monitoring to continually verify connection to the client, regardless of network traffic activity levels.
- Reset configuration option.
- Firmware upgrade.
- Backup and restore of access point configuration.
- Backup and restore of user database for built-in RADIUS server (applicable with IEEE 802.1x and WPA/WPA2 Enterprise (RADIUS) security modes.

1.6 What’s Next?

Ready to get started with wireless networking? Once your 9160 G2 Wireless Gateway is installed (see Chapter 2: “Installation Requirements”), read through Chapter 3: “PreLaunch Checklist” and then follow the steps in Chapter 4: “Quick Steps For Setup And Launch”.

INSTALLATION REQUIREMENTS 2

Warning: ***The 9160 G2 must be installed by qualified Psion Teklogix personnel.***

2.1 Choosing The Right Location

Typically, Psion Teklogix conducts a site survey in the plant and then recommends the preferred locations for the 9160 G2s. These locations provide good radio coverage, minimize the distance to the host computer or network controller, and meet the environmental requirements.

2.1.1 Environment

2.1.1.1 9160 G2 Wireless Gateway

The 9160 G2 should be located in a well-ventilated area and should be protected from extreme temperature fluctuations (i.e. direct heater output, shipping doors or direct sunlight). If a protective cover is required, it must have enough ventilation to maintain the 9160 G2's surface at or near room temperature.

Refer to Chapter 25: "Specifications" for a more detailed description of environmental requirements. Keep in mind that the long term stability of this equipment will be enhanced if the environmental conditions are less severe than those listed in this manual.

The 9160 G2 should be situated away from the path of vehicles and free from water or dust spray. The 9160 G2 should only be mounted in the upright position, as shown in Figure 2.1 on page 18. This orientation minimizes the risk of water entering the 9160 G2, should the unit accidentally be sprayed.

The 9160 G2 is attached to a vertical surface using four fasteners on the rear plate (type of fasteners are dependent on mounting surface). The top two holes in the rear plate are slots, allowing the unit to be hung in position before the remaining bolts are installed, thus easing installation. The bolts used for installation are SAE 1/4-20.

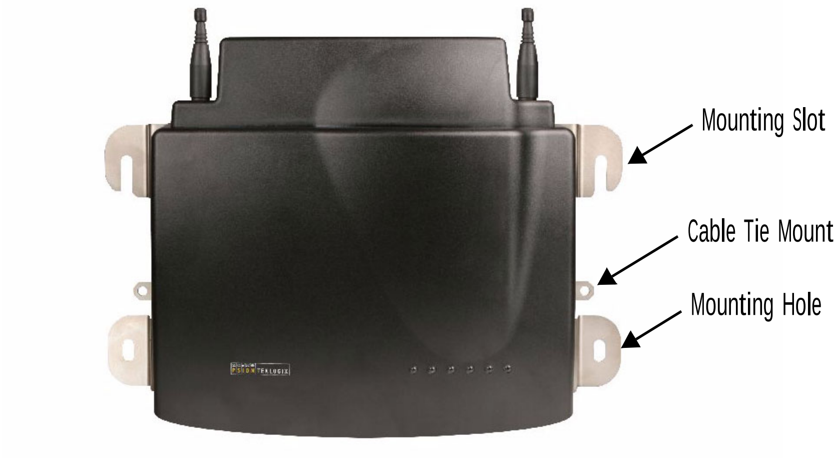


Figure 2.1 9160 G2 Installation Position

2.1.2 Maintenance

The 9160 G2 has no internal option switches and does not require physical access; all configuration settings are done remotely (see “Navigating To Basic Settings” on page 47). Environmental and radio communication considerations do still apply.

2.1.3 Radios

- 802.11g radio without integrated antenna (standard).
- 802.11a/g radio without integrated antenna (optional second radio).
- RA1001A - Narrow Band (NB) Radio.

2.1.4 Power And Antenna Cables

2.1.4.1 Power

To prevent accidental disconnection and stress on the 9160 G2, antenna and power cables should be secured within 30 cm of the unit. Secure the cables with ties to the cable tie mounts on the 9160 G2 (see Figure 2.1). A single phase power outlet (range 100 to 240 VAC rated 1.0A minimum) should be installed within one metre (3.1 feet) of the 9160 G2. The 9160 G2 automatically adjusts to input within that power range. The power cable is removable and is available in the power type specific to your location. The 9160 G2 AC power supply has a universal input via a standard IEC320 connector.

To eliminate the need for AC wiring, the 9160 G2 Wireless Gateway is compliant with IEEE 802.3af and can be powered over its Ethernet connection. For detailed information, please see “Power Over Ethernet Requirements” on page 262.

Warning: ***To avoid electric shock, the power cord protective grounding conductor must always be connected to ground.***

2.1.4.2 Antennas

The type of antenna required for each installation depends on the coverage requirements and the frequencies used. A maximum of four antenna elements can be used. These antennas can be a combination of reverse thread SMA “screw-on” diversity or high-gain WDS antennas. There are several omnidirectional antennas and special, directional antennas available from Psion Teklogix. Generally, a site survey determines the appropriate antenna. Consult Psion Teklogix service personnel for more information.

Warning: ***Never operate the 9160 G2 without a suitable antenna or a dummy load.***

Connection To Outdoor Antenna (Kit P/N 1916641)

The antenna must be installed by a qualified service person and installed according to local electrical installation codes. The antenna should be located such that it is always at least 15 ft (4.6 m) high and 10 ft (3 m) from the user and other people working in the area.

For a 9160 G2 connecting to an outdoor antenna, all the following notes are applicable:

1. The shield of the outdoor antenna coaxial cable is to be connected to earth (independent of the 9160 G2) in the building installation, provided the installation is acceptable to the authorities in the country of usage.
2. A supplementary equipment earthing conductor is to be installed between the 9160 G2 and earth—that is, in addition to the equipment earthing conductor in the power supply cord.

3. The supplementary equipment earthing conductor may not be smaller in size than the unearthed branch-circuit supply conductors (min 0.75 sq. mm nominal cross-sectional area or 18AWG). The supplementary equipment earthing conductor is to be connected to the 9160 G2 at the terminal provided, and connected to earth in a manner that will retain the earth connection when the power supply cord is unplugged. The connection to earth of the supplementary earthing conductor shall be in compliance with the appropriate rules for terminating bonding jumpers in the country of usage. Termination of the supplementary equipment earthing conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any earthed item that is permanently and reliably connected to the electrical service equipment earthed.
4. Bare, covered, or insulated earthing conductors are acceptable. A covered or insulated earthing conductor shall have a continuous outer finish that is either green (Canada and USA only), or green-and-yellow (all countries).
5. Avoid servicing during an electrical storm. There may be a remote risk of electrical shock from lightning.
6. For Finland, Norway, and Sweden, the equipment is to be used in a RESTRICTED ACCESS LOCATION where equipotential bonding has been applied. The permanently connected PROTECTIVE EARTHING CONDUCTOR is to be installed by a SERVICE PERSON.

Warning: ***For RF safety considerations, users are not allowed to approach close to the antenna.***

Psion Teklogix supplies the coaxial cable required to connect the 9160 G2 to the antenna. When determining the location of the antenna, coverage requirements of the antenna are considered in conjunction with the environmental requirements of the 9160 G2.

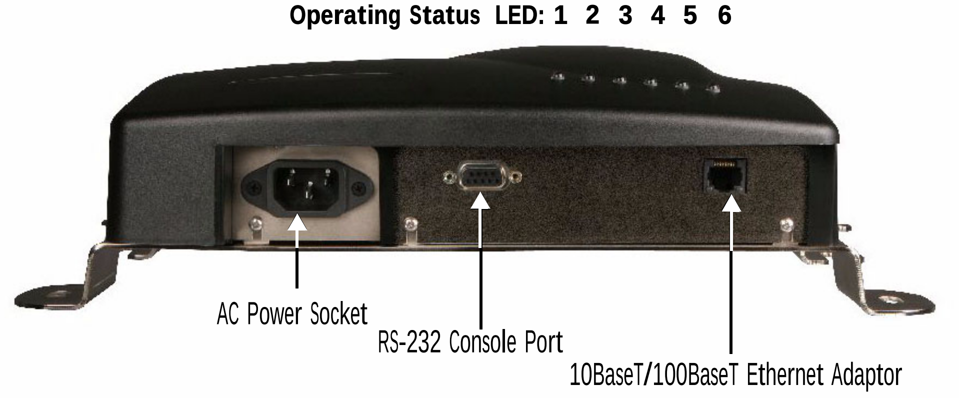
The coaxial cable must be routed and secured using wire anchors and/or coaxial nail clips. A few extra inches of cable are required near the antenna and the 9160 G2 to make disconnection easier.

2.2 Connecting To External Devices

This section contains general guidelines for connecting the 9160 G2 to external devices such as network controllers, base stations, host computers, PCs, and video display terminals.

2.2.1 Ports

Figure 2.2 shows the locations of the port and power connectors on the base of the 9160 G2. The port pinouts are described in Appendix B: "Port Pinouts And Cable Diagrams".


Operating Status LED: 1 2 3 4 5 6
AC Power Socket
RS-232 Console Port
10BaseT/100BaseT Ethernet Adaptor

** Note: Older versions of the 9160 G2 do not have a fiber port.*

Figure 2.2 9160 G2 Port And LED Locations

2.2.2 LAN Installation: Overview

Because the 9160 G2 provides Ethernet connectivity, it can be added to an existing LAN. Generally, LAN installations are handled with the help of the network administrators, as they are familiar with their network and its configuration. Once the 9160 G2 is installed, connected and powered on, the system administrator can access the unit to check the configuration and to assign the 9160 G2 its unique IP address. This may be done through the network (see "Changing The Configuration With A Web Browser" on page 23). Subsequent changes in the network, such as the addition of stations or users, would also require that the 9160 G2 configuration be changed.

Important: ***Once the 9160 G2 is configured and rebooted the first time, the DHCP should be disabled unless the 9160 G2 obtains its IP address from a server.***

2.2.3 LAN Installation: Ethernet

The 9160 G2 is a high-performance Access Point that supports 100Mb/s Fast Ethernet LANs, as well as 10Mb/s, with both full and half duplex operation. It comes equipped with: a 10BaseT/100BaseT card (using a category-5 twisted pair cable, an RJ-45 connector, running at a rate of 10 or 100Mb/s). For port pinouts, please refer to Appendix B: “Port Pinouts And Cable Diagrams”.

Note: *The 9160 G2 does not support any connection type other than Ethernet 10BaseT and 100BaseT.*

2.2.3.1 Ethernet Cabling

The maximum cable segment length allowed between repeaters for the 9160 G2 (10BaseT/100BaseT Ethernet cabling) is 100 m.

2.2.4 Status Indicators (LEDs)

The high-performance 9160 G2 has six status indicators on the front of the enclosure, as shown in Figure 2.2 on page 21. The numbered and coloured LEDs on the front of the unit indicate the operating status for each port, as described in Table 2.1.

LED Number	Name	Function	Colour
1	Ethernet link	Link indicator for 10BaseT/100BaseT: ON = good link; OFF = no link	yellow[*]
2	Ethernet activity	Ethernet LAN activity (Rx/Tx)	green
3	1st 802.11 radio status	1st 802.11 radio activity (Rx/Tx)	green
4	2nd 802.11 radio status	2nd 802.11 radio activity (Rx/Tx)	green
5	NB radio status	NB radio activity (Rx/Tx)	green
6	Power	LED On solid = Unit powered LED Off = No power to unit	green

[*] *LED 1 colour shows orientation of LEDs when viewed from a distance.*

Table 2.1 9160 G2 LED Functions: Front Enclosure

2.1.5 Connecting A Video Display Terminal

An ANSI compatible video display terminal (e.g., DEC VT220 or higher), or a PC running terminal emulation, is used for diagnostic purposes.

The terminal is connected to the RS-232 port on the 9160 G2 (see Figure 2.2 on page 21). This port is normally set to operate at 115,200 baud, 8 bits, 1 stop bit, no parity. To comply with Part 15 of the FCC rules for a Class B computing device, only the cable supplied (P/N 19387) should be used.

2.2 Changing The Configuration With A Web Browser

The 9160 G2 Flash memory can be reconfigured remotely via the network using a standard HTML Web Browser such as MS Internet Explorer (version 4.0 or later) or Firefox. See Chapter 4: “Quick Steps For Setup And Launch” for instructions on changing the parameters and general configuration settings.

PRELAUNCH CHECKLIST 3

Before you plug in and boot a new ***Access Point***, review the following sections for a quick check of required hardware components, software, client configurations, and compatibility issues. Make sure you have everything you need ready to go for a successful launch and test of your new (or extended) wireless network.

3.1 The 9160 G2 Wireless Gateway

The 9160 G2 Wireless Gateway is a wireless communications hub for devices on your network. It provides continuous, high-speed access between your wireless and Ethernet devices in ***IEEE 802.11a***, ***802.11b***, ***802.11g***, and ***802.11a Turbo*** modes.

The 9160 G2 Wireless Gateway offers an out-of-the-box *Guest Interface* feature that allows you to configure access points for controlled guest access of the wireless network using Virtual LANs.

For more information on the Guest interface, see Chapter 14: “Setting up Guest Access” and “A Note About Setting Up Connections For A Guest Network” on page 40.

3.1.1 Default Settings For The 9160 G2 Wireless Gateway

Option	Default Settings	Related Information
System Name	PTX9160-Wireless-AP	“Setting The DNS Name” on page 134 in “The Ethernet (Wired) Interface” on page 131
User Name	admin The user name is read-only. It cannot be modified.	
Password	admin	“Provide Network Settings” on page 49 in “Configuring Basic Settings” on page 45

Table 3.1 9160 G2 Default Settings

Option	Default Settings	Related Information
Network Name (SSID)	"TEKLOGIX" for the Internal interface "TEKLOGIX Guest" for the Guest interface	"Review / Describe The Access Point" on page 48 in "Configuring Basic Settings" on page 45 "Configuring "Internal" Wireless LAN Settings" on page 145 in "Setting the Wireless Interface" on page 139 "Configuring "Guest" Network Wireless Settings" on page 146 in "Setting the Wireless Interface" on page 139
Network Time Protocol (NTP)	None	"Network Time Protocol Server" on page 247
IP Address	192.168.1.10 The default IP address is used if you do not use a *Dynamic Host Configuration Protocol* (***DHCP***) server. You can assign a new static IP address through the Administration Web pages. If you have a ***DHCP*** server on the network, then an IP address will be dynamically assigned by the server at AP startup.	"Understanding Dynamic And Static IP Addressing On The 9160 G2 Wireless Gateway" on page 33
Connection Type	*Dynamic Host Configuration Protocol* (***DHCP***) If you do not have a ***DHCP*** server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is to change the Connection Type from "DHCP" to "Static IP". The Guest network must have a DHCP server.	"Understanding Dynamic And Static IP Addressing On The 9160 G2 Wireless Gateway" on page 33 For information on how to re-configure the Connection Type, see "Configuring LAN Or Internal Interface Ethernet Settings" on page 136.
Subnet Mask	None This is determined by your network setup and DHCP server configuration.	"The Ethernet (Wired) Interface" on page 131
Radio	On	"Configuring 802.11 Radio Settings" on page 161

Table 3.1 9160 G2 Default Settings

Option	Default Settings	Related Information
IEEE 802.11 Mode	802.11g or 802.11a+g	"Configuring 802.11 Radio Settings" on page 161
802.11g Channel	Auto	"Configuring 802.11 Radio Settings" on page 161
Beacon Interval	100	"Configuring 802.11 Radio Settings" on page 161
DTIM Period	2	"Configuring 802.11 Radio Settings" on page 161
Fragmentation Threshold	2346	"Configuring 802.11 Radio Settings" on page 161
RTS Threshold	2347	"Configuring 802.11 Radio Settings" on page 161
MAX Stations	2007	"Configuring 802.11 Radio Settings" on page 161
Transmit Power	100 percent	"Configuring 802.11 Radio Settings" on page 161
Rate Sets Supported (Mbps)	• IEEE 802.1a: 54, 48, 36, 24, 18, 12, 9, 6 • IEEE 802.1g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 • IEEE 802.1b: 11, 5.5, 2, 1	"Configuring 802.11 Radio Settings" on page 161
Rate Sets (Mbps) (Basic/Advertised)	• IEEE 802.1a: 24, 12, 6 • IEEE 802.1g: 11, 5.5, 2, 1 • IEEE 802.1b: 2, 1	"Configuring 802.11 Radio Settings" on page 161
Broadcast SSID	Allow	"Configuring Security Settings" on page 99.
Security Mode	None (plain-text)	"Configuring Security Settings" on page 99.
Authentication Type	None	
MAC Filtering	Allow any station unless in list	"MAC Address Filtering" on page 171
Guest Login and Management	Disabled	"Setting up Guest Access" on page 147
Load Balancing	Disabled	"Load Balancing" on page 175
WDS Settings	None	"Wireless Distribution System" on page 197

Table 3.1 9160 G2 Default Settings

3.1.2 What The Access Point Does Not Provide

The 9160 G2 Wireless Gateway is not designed to function as a ***Gateway*** to the Internet. To connect your Wireless LAN (***WLAN***) to other ***LAN***s or the Internet, you need a gateway device.

3.2 Administrator's Computer

Configuration and administration of the 9160 G2 Wireless Gateway is accomplished through a Web-based user interface (UI). The Table 3.2 describes the minimum requirements for the administrator's computer.

Required Components	Description
Ethernet Connection to the First Access Point	The computer used to configure the first access point must be connected to the access point (either directly or through a hub) by an Ethernet cable. For more information, see "Connect The Access Point To Network And Power" on page 38 in "Quick Steps For Setup And Launch".
Wireless Connection to the Network	After initial configuration and launch of the first access points on your new wireless network, you can make subsequent configuration changes through the Administration Web pages using a wireless connection to the "Internal" network. For wireless connection to the access point, your administration device will need Wi-Fi capability similar to that of any wireless client: • Portable or built-in Wi-Fi client adaptor that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE ***802.11a***, ***802.11b802.11a***, ***802.11g802.11b***, ***802.11a Turbo802.11g 802.11a Turbo*** modes are supported.) • Wireless client software such as Microsoft® Windows® XP or Funk Odyssey wireless client configured to associate with the 9160 G2 Wireless Gateway. For more details on Wi-Fi client setup, see "Wireless Client Computers" on page 31.

Table 3.2 Required AP Administrator Software And Hardware

Required Components	Description
Web Browser / Operating System	Configuration and administration of the 9160 G2 Wireless Gateway is provided through a Web-based user interface hosted on the access point. We recommend using one of the following supported Web browsers to access the access point Administration Web pages: • Microsoft Internet Explorer version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000 • Netscape® Mozilla 1.7.x on Redhat Linux version 2.4 The administration Web browser must have JavaScript enabled to support the interactive features of the administration interface. It must also support HTTP uploads to use the firmware upgrade feature.
Security Settings	Ensure that security is disabled on the wireless client used to initially configure the access point.

Table 3.2 Required AP Administrator Software And Hardware

3.3 Wireless Client Computers

The 9160 G2 Wireless Gateway provides wireless access to any client with a properly configured Wi-Fi client adaptor for the 802.11 mode in which the access point is running.

Multiple client operating systems are supported. Clients can be laptops or desktops, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adaptor and supporting drivers.

In order to connect to the access point, wireless clients need the software and hardware described in Table 3.3, below.

Required Components	Description
Wi-Fi Client Adaptor	Portable or built-in Wi-Fi client adaptor that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, and 802.11g are supported.) Wi-Fi client adaptors vary considerably. The adaptor can be a PC card built in to the client device, a portable PCMCIA or PCI card (types of ***NIC***s), or an external device such as a USB or Ethernet adaptor that you connect to the client by means of a cable. The access point supports 802.11a/b/g modes, but you will probably make a decision during network design phase as to which mode to use. The fundamental requirement for clients is that they all have configured adaptors that match the 802.11 mode for which your access point(s) is configured.
Wireless Client Software	Client software such as Microsoft Windows Supplicant or Funk Odyssey wireless client configured to associate with the 9160 G2 Wireless Gateway.
Client Security Settings	Security should be disabled on the client used to do initial configuration of the access point. If the Security mode on the access point is set to anything other than plain-text, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid username and password, certificate, or similar user identity proof. Security modes are Static ***WEP***, IEEE ***802.1x***, ***WPA*** with ***RADIUS*** server, and ***WPA2PSK***. For information on configuring security on the access point, see “Configuring Security” on page 89.

Table 3.3 Required AP Client Software And Hardware

3.4 Understanding Dynamic And Static IP Addressing On The 9160 G2 Wireless Gateway

9160 G2 Wireless Gateways are designed to auto-configure, with very little setup required for the first access point and no configuration required for additional access points subsequently joining a pre-configured *cluster*.

3.4.1 How Does The Access Point Obtain An IP Address At Startup?

When you deploy the access point, it looks for a network ***DHCP*** server and, if it finds one, obtains an ***IP Address*** from the DHCP server. If no DHCP server is found on the network, the AP will continue to use its default ***Static IP Address*** (192.168.1.10) until you re-assign it a new static IP address (and specify a static IP addressing policy) or until a DHCP server is brought online.

Notes: *If you configure both an Internal and Guest network and plan to use a dynamic addressing policy for both, separate DHCP servers must be running on each network.*

A DHCP server is a requirement for the Guest network.

3.4.2 Dynamic IP Addressing

The 9160 G2 Wireless Gateway generally expects that a ***DHCP*** server is running on the network where the AP is deployed. Most home and small business networks already have DHCP service provided either via a gateway device or a centralized server. However, if no DHCP server is present on the Internal network, the AP will use the default ***Static IP Address*** for first time startup.

Similarly, wireless clients and other network devices (such as printers) will receive their IP addresses from the DHCP server, if there is one. If no DHCP server exists on the network, you must manually assign static IP addresses to your wireless clients and other network devices.

The Guest network must have a DHCP server.

3.4.3 Static IP Addressing

The 9160 G2 Wireless Gateway ships with a default ***Static IP Address*** of 192.168.1.10. (See “Default Settings For The 9160 G2 Wireless Gateway” on page 27.) If no ***DHCP*** server is found on the network, the AP retains this static IP address at first-
time startup.

After AP startup, you have the option of specifying a static IP addressing policy on 9160 G2 Wireless Gateways and assigning static IP addresses to APs on the Internal network via the access point Administration Web pages. (See information about the **Connection Type** field and related fields in “Configuring LAN Or Internal Interface Ethernet Settings” on page 136.)

Important: ***If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP. You can either assign a new Static IP address to the AP or continue using the default address. We recommend assigning a new Static IP address so that if later you bring up another 9160 G2 Wireless Gateway on the same network, the IP address for each AP will be unique.***

3.4.4 Recovering An IP Address

If you experience trouble communicating with the access point, you can recover a ***Static IP Address*** by resetting the AP configuration to the factory defaults (see “Resetting Factory Default Configuration” on page 253), or you can get a dynamically assigned address by connecting the AP to a network that has ***DHCP***.

QUICK STEPS FOR SETUP AND LAUNCH 4

Setting up and deploying one or more 9160 G2 Wireless Gateways is in effect creating and launching a *wireless network*. The *Basic Settings* Administration Web page simplifies this process. Here is a step-by-step guide to setting up your 9160 G2 Wireless Gateways and the resulting wireless network. Familiarize yourself with the Chapter 3: “PreLaunch Checklist” if you haven’t already.

The topics covered here are:

- Step 1: ***Unpack The 9160 G2 Wireless Gateway***.
- Step 2: ***Connect The Access Point To Network And Power***.
- Step 3: ***Power On The Access Point***.
- Step 5: ***Log On To The Administration Web Pages***.
- Step 6: ***Configure ‘Basic Settings’ And Start The Wireless Network***.
- ***What’s Next?***

4.1 Unpack The 9160 G2 Wireless Gateway

Unpack the 9160 G2 Wireless Gateway and familiarize yourself with its hardware ports, associated cables, and accessories.

4.1.1 9160 G2 Wireless Gateway Hardware And Ports

The 9160 G2 Wireless Gateway includes:

- Ethernet port for connection to the Local Area Network (LAN) via Ethernet network cable.
- Power port and power adaptor.
- Power on/off switch.
- Either one or two radios depending on which model of the product you have.

4.1.2 What's Inside The 9160 G2 Wireless Gateway?

The 9160 G2 Wireless Gateway, as an ***Access Point*** (AP), is a single-purpose computer designed to function as a wireless hub. Inside the access point is a Wi-Fi radio system and a microprocessor. The access point boots from FlashROM using powered firmware with the configurable, runtime features summarized in "Overview Of The 9160 G2 Wireless Gateway" on page 7.

As new features and enhancements become available, you can upgrade the firmware to add new functionality and performance improvements to the access points that make up your wireless network. (See "Upgrading The Firmware" on page 255.)

4.2 Connect The Access Point To Network And Power

The next step is to set up the network and power connections.

1. Do one of the following to create an Ethernet connection between the access point and the computer:

   Connect one end of an Ethernet cable to the network port on the access point and the other end to the same hub where your PC is connected. (See Figure 4.1 on page 39.)

   Or

   Connect one end of a crossover[1] cable to the network port on the access point and the other end of the cable to the Ethernet port on the PC. (See Figure 4.2 on page 40.)

Notes: *If you use a hub, the device you use must permit broadcast signals from the access point to reach all other devices on the network. A standard hub should work fine. Some switches, however, do not allow directed or subnet broadcasts through. You may have to configure the switch to allow directed broadcasts.*

[1] If the access point hardware supports ***MDI and MDI-X*** auto functions, you can use a regular Ethernet cable for a direct connection from PC to AP. A crossover cable will work also, but is not necessary if you have MDI and MDI-X auto sensing.ports.

For initial configuration with a direct Ethernet connection and no DHCP server, be sure to set your PC to a static IP address in the same subnet as the default IP address on the access point. (The default IP address for the access point is 192.168.1.10.)

If for initial configuration you use a direct Ethernet (wired) connection (via crossover cable) between the access point and the computer, you will need to reconfigure the cabling for subsequent startup and deployment of the access point so that the access point is no longer connected directly to the PC but instead is connected to the LAN (either via a Hub as shown in Figure 4.1, or directly).

ETHERNET CONNECTIONS WHEN USING DHCP FOR INITIAL CONFIGURATION

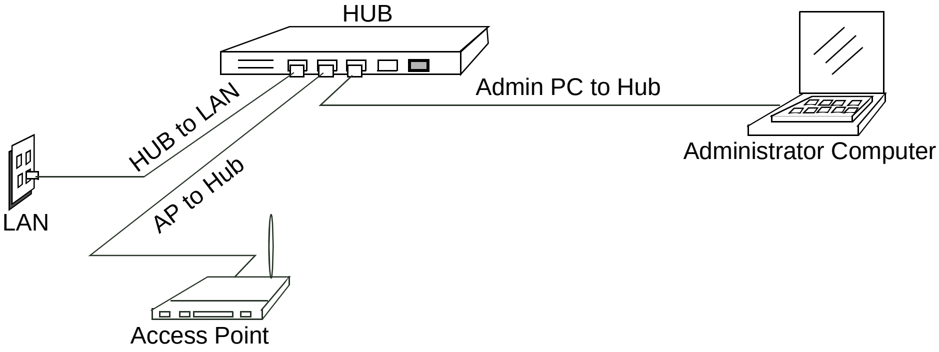


Figure 4.1 Ethernet Connections Using DHCP

ETHERNET CONNECTIONS WHEN USING STATIC IP FOR INITIAL CONFIGURATION

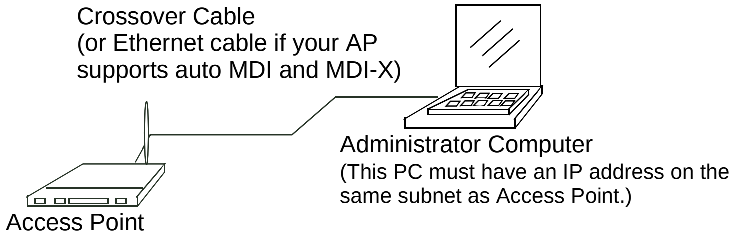

Crossover Cable
(or Ethernet cable if your AP
supports auto MDI and MDI-X)
Administrator Computer
(This PC must have an IP address on the
same subnet as Access Point.)
Access Point

Figure 4.2 Ethernet Connections Using Static IP

2. Connect the power adaptor to the power port on the back of the access point, and then plug the other end of the power cord into a power outlet (preferably, via a surge protector).

4.2.1 A Note About Setting Up Connections For A Guest Network

The 9160 G2 Wireless Gateway offers an out-of-the-box Guest Interface that allows you to configure an access point for controlled guest access to the network. The same access point can function as a bridge for two different wireless networks: a secure “Internal” LAN and a public “Guest” network. This can be done virtually, by defining two different Virtual LANs via the Administration UI.

For information on configuring Guest interface settings on the Administration UI, see Chapter 14: “Setting up Guest Access”.

4.2.1.1 Hardware Connections For A Guest VLAN

If you plan to configure a guest network using VLANs, do the following:

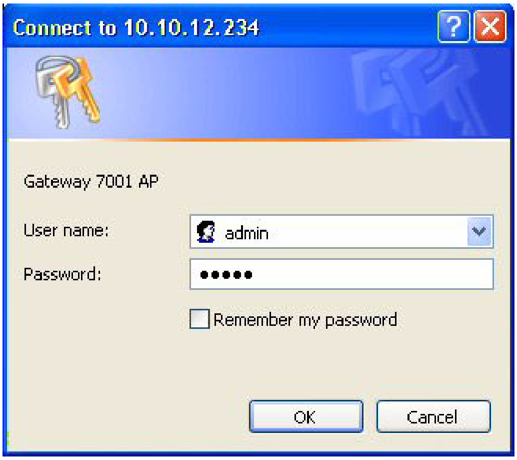
- Connect a network port on the access point to a VLAN-capable switch.
- Define VLANs on that switch.

4.3 Power On The Access Point

The 9160 G2 Wireless Gateway powers on and initializes when you plug it in.

4.4 Log On To The Administration Web Pages

When you go to the IP address of the 9160 G2 Wireless Gateway Administration Web pages, you are prompted for a user name and password.



Connect to 10.10.12.234

Gateway 7001 AP

User name: admin

Password: ●●●●●

□ Remember my password

The defaults for user name and password are as follows.

Field	Default Setting
User name	admin
Password	admin The user name is read-only. It cannot be modified.

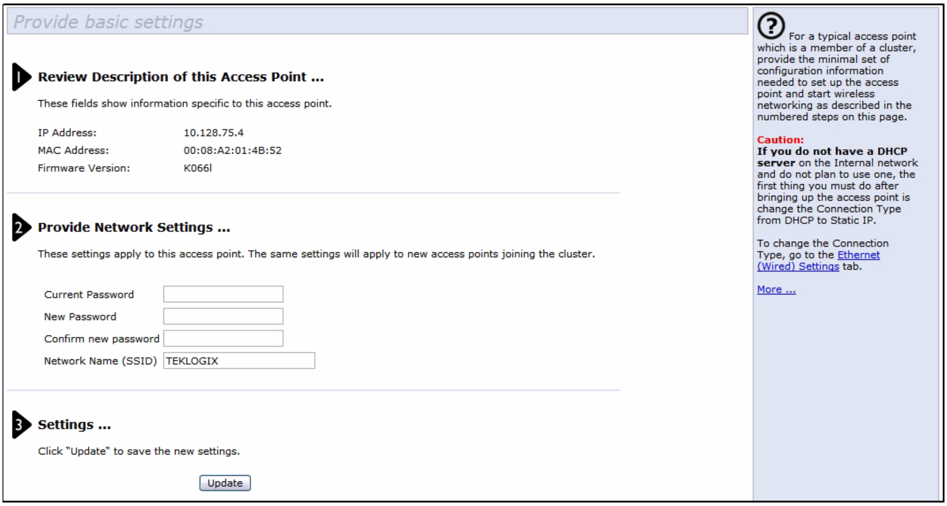
Table 4.3 Username And Password

Enter the user name and password and click **OK**.

4.4.1 Viewing Basic Settings For Access Points

When you first log in, the *Basic Settings* page for 9160 G2 Wireless Gateway administration is displayed. These are global settings for all access points that are members of the cluster and, if automatic configuration is specified, for any new access points that are added later.

Note: *Currently the 9160 G2 Wireless Gateway menus appear slightly different from those shown - the menu tabs are arranged vertically down the left side of the page, rather than across the top.*



Provide basic settings

1 **Review Description of this Access Point ...**

These fields show information specific to this access point.

IP Address: 10.128.75.4
MAC Address: 00:08:A2:01:4B:52
Firmware Version: K066l

2 **Provide Network Settings ...**

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password
New Password
Confirm new password
Network Name (SSID) TEKLOGIX

3 **Settings ...**

Click "Update" to save the new settings.

? For a typical access point which is a member of a cluster, provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

Caution:
If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

4.5 Configure 'Basic Settings' And Start The Wireless Network

Provide a minimal set of configuration information by defining the basic settings for your wireless network. These settings are all available on the *Basic Settings* page of the Administration Web interface, and are categorized into steps 1-3 on the Web page.

For a detailed description of these "Basic Settings" and how to properly configure them, please see Chapter 5: "Configuring Basic Settings". Summarized briefly here, the steps are:

1. Review Description of this Access Point.

   Provide IP addressing information. For more information, see "Review / Describe The Access Point" on page 48.

2. Provide Network Settings.

   Provide a new administrator password for clustered access points. For more information, see “Provide Network Settings” on page 49.

3. Settings.

   Click the **Update** button to activate the wireless network with these new settings. For more information, see “Update Basic Settings” on page 50.

4.5.1 Default Configuration

If you follow the steps above and accept all the defaults, the access point will have the default configuration described in “Default Settings For The 9160 G2 Wireless Gateway” on page 27.

4.6 What’s Next?

Next, make sure the access point is connected to the LAN, bring up some wireless clients, and connect the clients to the network. Once you have tested the basics of your wireless network, you can enable more security and fine-tune by modifying advanced configuration features on the access point.

4.6.1 Make Sure The Access Point Is Connected To The LAN

If you configured the access point and administrator PC by connecting both into a network hub, then your access point is already connected to the LAN. That’s it—you’re up and running! The next step is to test some wireless clients.

If you configured the access point using a direct wired connection via crossover cable from your computer to the access point, do the following:

1. Disconnect the crossover cable from the computer and the access point.
2. Connect a regular Ethernet cable from the access point to the ***LAN***.
3. Connect your computer to the LAN either via Ethernet cable or wireless client card.

4.6.2 Test LAN Connectivity With Wireless Clients

Test the 9160 G2 Wireless Gateway by trying to detect it and associate with it from some wireless client devices. (See “Wireless Client Computers” on page 31 in the ***PreLaunch Checklist*** for information on requirements for these clients.)

4.6.3 Secure And Fine-tune The Access Point Using Advanced Features

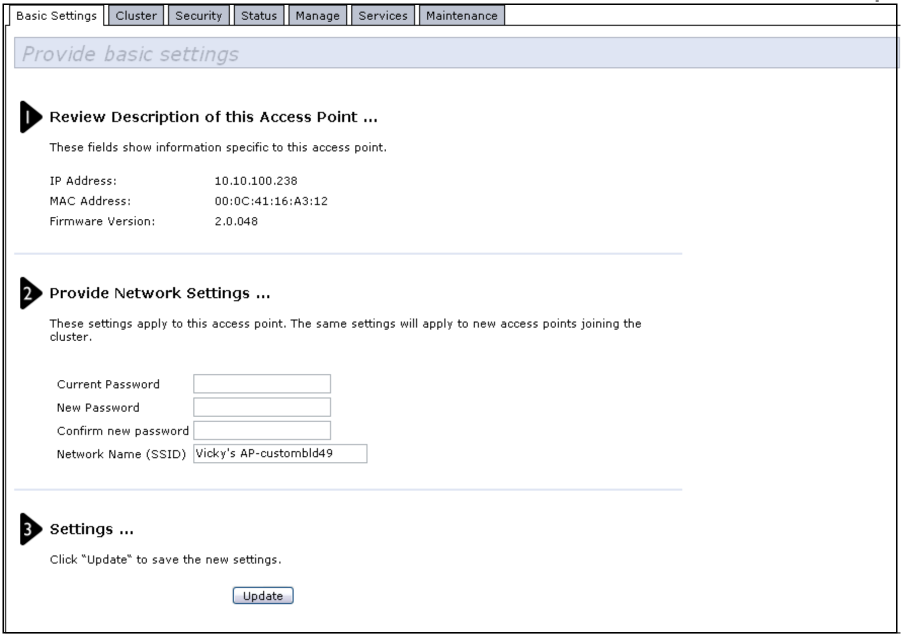
Once you have the wireless network up and running and have tested against the access point with some wireless clients, you can add in more layers of security, add users, configure a Guest interface, and fine-tune performance settings.

CONFIGURING BASIC SETTINGS 5

5.1 Navigating To Basic Settings

To configure initial settings, click *Basic Settings*.

If you type the IP address of the access point into your browser, the *Basic Settings* page is the default page that is displayed.



Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.10.100.238
MAC Address: 00:0C:41:16:A3:12
Firmware Version: 2.0.048

Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

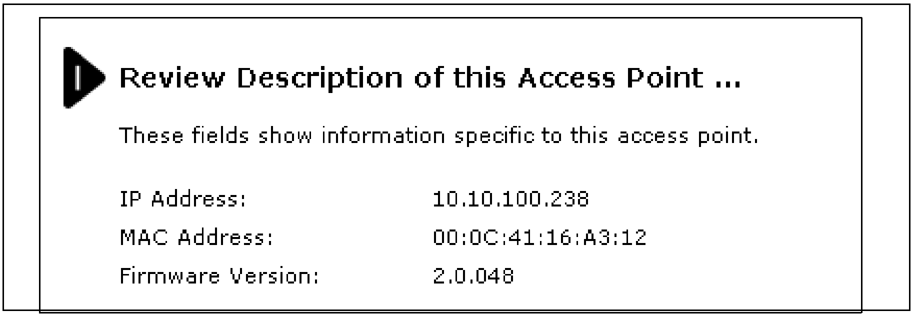
Current Password
New Password
Confirm new password
Network Name (SSID) Vicky's AP-custombld49

Settings ...

Click "Update" to save the new settings.

Fill in the fields on the Basic Settings screen as described in “Review / Describe The Access Point” on page 48.

5.2 Review / Describe The Access Point



Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.10.100.238

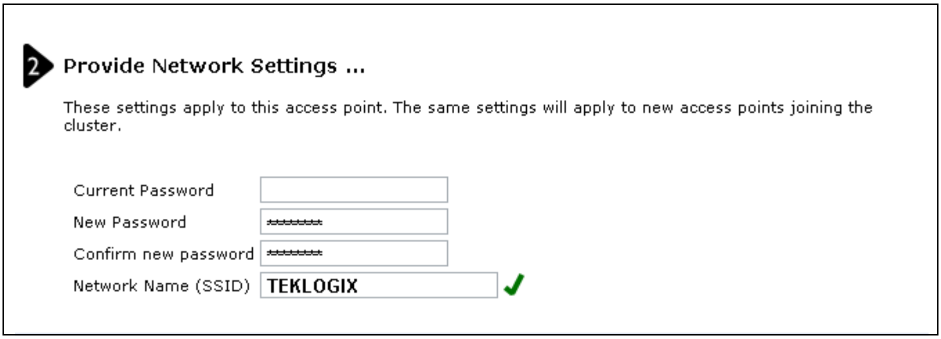
MAC Address: 00:0C:41:16:A3:12

Firmware Version: 2.0.048

Field	Description
IP Address	Shows IP address assigned to this access point. This field is not editable because the IP address is already assigned (either via DHCP, or statically through the Ethernet (wired) settings as described in “Configuring Guest Interface Ethernet (Wired) Settings” on page 138).
MAC Address	Shows the ***MAC*** address of the access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. The address shown here is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks. To see MAC addresses for Guest and Internal interfaces on the AP, see the *Status, Interfaces* tab.
Firmware Version	Version information about the firmware currently installed on the access point. As new versions of the 9160 G2 Wireless Gateway firmware become available, you can upgrade the firmware on your access points to take advantages of new features and enhancements. For instructions on how to upgrade the firmware, see “Upgrading The Firmware” on page 255.

Table 5.1 Basic Settings Screen Options

5.3 Provide Network Settings



2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

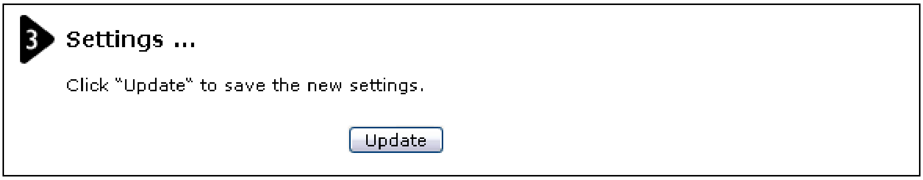
Current Password	
New Password	********
Confirm new password	********
Network Name (SSID)	TEKLOGIX ✓

Field	Description
Current Password	Enter the current administrator password. You must correctly enter the current password before you are able to change it.
New Password	Enter a new administrator password. The characters you enter will be displayed as " * " characters to prevent others from seeing your password as you type. The Administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces. ▶ As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.
Confirm New Password	Re-enter the new administrator password to confirm that you typed it as intended.
Network Name (SSID)	Enter a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this ***SSID***. The *Service Set Identifier* (***SSID***) is an alphanumeric string of up to 32 characters **Note:** *If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.*

Table 5.2 Administrator Password And Wireless Network

Note: *The 9160 G2 Wireless Gateway is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in sync, but there is no guarantee that all configuration changes specified by multiple users will be applied.*

5.4 Update Basic Settings



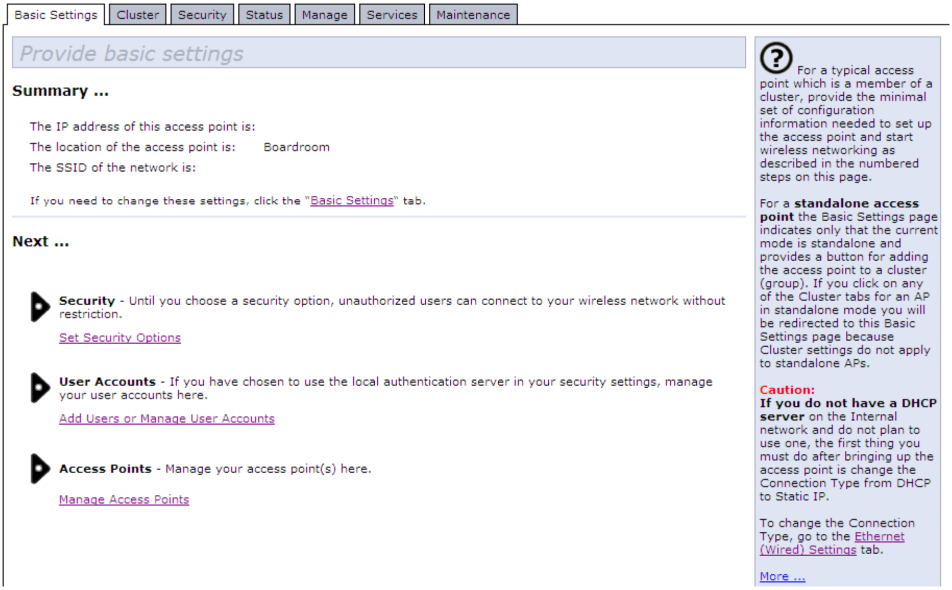
Settings ...

Click "Update" to save the new settings.

When you have reviewed the new configuration, click **Update** to apply the settings and deploy the access points as a wireless network.

5.5 Summary Of Settings

When you update the Basic Settings, a summary of the new settings is shown, along with information about next steps.



Provide basic settings

Summary ...

The IP address of this access point is:
The location of the access point is: Boardroom
The SSID of the network is:

If you need to change these settings, click the "Basic Settings" tab.

Next ...

Security - Until you choose a security option, unauthorized users can connect to your wireless network without restriction.
Set Security Options

User Accounts - If you have chosen to use the local authentication server in your security settings, manage your user accounts here.
Add Users or Manage User Accounts

Access Points - Manage your access point(s) here.
Manage Access Points

For a typical access point which is a member of a cluster, provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

For a **standalone access point** the Basic Settings page indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the Cluster tabs for an AP in standalone mode you will be redirected to this Basic Settings page because Cluster settings do not apply to standalone APs.

Caution:
If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

At initial startup, no security is in place on the access point. An important next step is to configure security, as described in Chapter 10: “Configuring Security”.

At this point if you click **Basic Settings** again, the summary of settings page is replaced by the standard Basic Settings configuration options.

5.6 Basic Settings For A Standalone Access Point

The *Basic Settings* tab for a standalone access point indicates only that the current mode is standalone. If you want to add the current access point to an existing cluster, navigate to the *Cluster* > *Access* Point tab.

For more information see “Starting Clustering” on page 61.

5.7 Your Network At A Glance: Understanding Indicator Icons

All the Cluster settings tabs on the Administration Web pages include visual indicator icons showing current network activity.

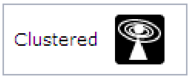
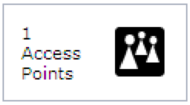
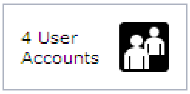
Icon	Description
 Clustered	When one or more APs on your network are available for service, the “Wireless Network Available” icon is shown. The clustering icon indicates whether the current access point is “Clustered” or “Not Clustered” (that is, standalone or when a state of change is in progress). For information about clustering, see “Understanding Clustering” on page 56.
 1 Access Points	The number of access points available for service on this network is indicated by the “Access Points” icon. For information about managing access points, see Chapter 6: “Managing Access Points & Clusters”.
 4 User Accounts	The number of client user accounts created and enabled on this network is indicated by the “User Accounts” icon. For information about setting up user accounts on the access point for use with the built-in authentication server, see Chapter 7: “Managing User Accounts”. See also “IEEE 802.1x” on page 107 and “WPA Enterprise” on page 112, which are the two security modes that offer the option of using the built-in authentication server.

Table 5.3 Indicator Icons

MANAGING ACCESS POINTS & CLUSTERS 6

6.1 Overview

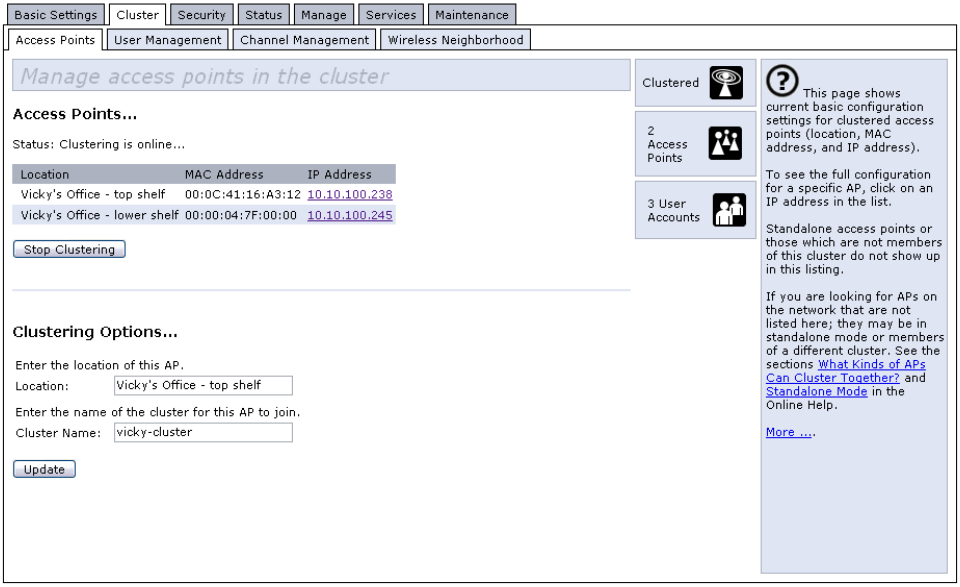
The 9160 G2 Wireless Gateway shows current basic configuration settings for clustered access points (location, IP address, MAC address, status, and availability) and provides a way of navigating to the full configuration for specific APs if they are cluster members.

Standalone access points or those which are not members of this cluster do not show up in this listing. To configure standalone access points, you must know the IP address of the access point and use it in a URL (*http://IPAddressOfAccessPoint*).

Note: *The 9160 G2 Wireless Gateway is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in sync but there is no guarantee that all configuration changes specified by multiple users will be applied.*

6.2 Navigating To Access Points Management

To view or edit information on access points in a cluster, click the **Cluster > Access Points** tab.



Manage access points in the cluster

Access Points...

Status: Clustering is online...

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

Clustering Options...

Enter the location of this AP.

Location: Vicky's Office - top shelf

Enter the name of the cluster for this AP to join.

Cluster Name: vicky-cluster

This page shows current basic configuration settings for clustered access points (location, MAC address, and IP address).

To see the full configuration for a specific AP, click on an IP address in the list.

Standalone access points or those which are not members of this cluster do not show up in this listing.

If you are looking for APs on the network that are not listed here; they may be in standalone mode or members of a different cluster. See the sections What Kinds of APs Can Cluster Together? and Standalone Mode in the Online Help.

More ....

6.3 Understanding Clustering

A key feature of the 9160 G2 Wireless Gateway is the ability to form a dynamic, configuration-aware group (called a *cluster*) with other 9160 G2 Wireless Gateways in a network in the same subnet. Access points can participate in a self-organizing cluster which makes it easier for you to deploy, administer, and secure your wireless network. The cluster provides a single point of administration and lets you view the deployment of access points as a single wireless network rather than a series of separate wireless devices.

6.3.1 What Is A Cluster?

A cluster is a group of access points which are coordinated as a single group via 9160 G2 Wireless Gateway administration. You can have multiple clusters on the same subnet if they have different cluster “names”.

6.3.2 How Many APs Can A Cluster Support?

Currently, there is no hard limit on the number of access points in a cluster. Validation testing has verified a dozen or more supported on the same subnet. You can include as many APs as needed in a cluster at any one time.

6.3.3 What Kinds Of APs Can Cluster Together?

A single 9160 G2 Wireless Gateway can form a cluster with itself (a “cluster of one”) and with other 9160 G2 Wireless Gateways. In order to be members of the same cluster, access points must be:

- Compatible devices as designated by the manufacturer (access points must have compatible design features).
- Of the same radio configuration (all one-radio APs or all two-radio APs).
- Of the same band configuration (all single-band APs or all dual-band APs).
- On the same ***LAN***.

Having a mix of APs on the network does not adversely affect 9160 G2 Wireless Gateway clustering in any way. However, it is helpful to understand the clustering behaviour for administration purposes:

- Access points joining the cluster must be named the same. For more information on setting the cluster name, see page 60.
- Access points of other brands will not join the cluster. These APs should be administered with their own associated Administration tools.

6.3.4 Which Settings Are Shared As Part Of The Cluster Configuration And Which Are Not?

Most configuration settings defined via the 9160 G2 Wireless Gateway Administration Web pages will be propagated to cluster members as a part of the *cluster configuration.*

6.3.4.1 Settings Shared In The Cluster Configuration

The cluster configuration includes:

- Network name (SSID).
- Administrator password.
- User accounts and authentication.
- Wireless interface settings.
- Guest Welcome screen settings.
- Network Time Protocol (NTP) settings.
- Radio settings.
  Only Mode, Channel, Fragmentation Threshold, RTS Threshold, and Rate Sets are synchronized across the cluster. Beacon Interval, DTIM Period, Maximum Stations, and Transmit Power do not cluster.

Note: *When Channel Planning is enabled, the radio Channel is not sync'd across the cluster. See "Stopping/Starting Automatic Channel Assignment" on page 76*

- Security settings.
- ***QoS*** queue parameters.
- MAC address filtering.

6.3.4.2 Settings Not Shared By The Cluster

The few exceptions (settings *not* shared among clustered access points) are the following, most of which by nature must be unique:

- IP addresses.
- MAC addresses.
- Location descriptions.
- Load Balancing settings.
- WDS bridges.
- Ethernet (Wired) Settings.
- Guest interface configuration.

Settings that are not shared must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the *Cluster > Access Points* page of the current AP.

6.3.5 Cluster Formation

A cluster is formed when the first AP is deployed with clustering enabled. The AP attempts to rendezvous with an existing cluster. If it is unable to locate any other APs on the subnet with the same cluster name, then it establishes a new cluster on its own.

6.3.6 Cluster Size And Membership

Currently, there is no hard limit on the number of APs in a cluster. Validation testing has verified a dozen or more supported on the same subnet. You can include as many APs as needed in a cluster at any one time.

Cluster membership is determined by:

- Cluster Name - APs with the same name will join the same cluster (see “Setting The Cluster Name” on page 60).
- Whether clustering is enabled - Only APs for which clustering is enabled will join a cluster (see “Starting Clustering” on page 61 and “Stopping Clustering” on page 61).

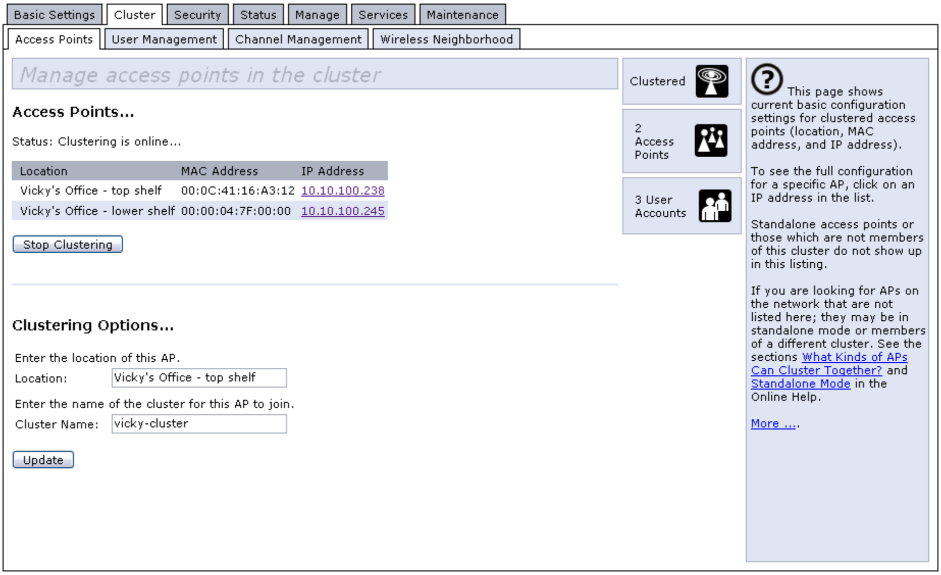
6.3.7 Intra-Cluster Security

For purposes of ease-of-use, the clustering component is designed to let new devices join a cluster without strong authentication. However, communications of all data between access points in a cluster is protected against casual eavesdropping using Secure Sockets Layer (SSL). The assumption is that the private wired network to which the devices are connected is secure. Both the cluster configuration file and the user database are transmitted among access points using SSL.

6.4 Understanding Access Point Settings

The Access Points tab provides information about all access points in the cluster. From this tab, you can view location descriptions, MAC addresses, IP addresses, enable (activate) or disable (deactivate) *clustered* access points, and remove access points from the cluster. You can also modify the location description for an access point. The IP address links provide a way to navigate to configuration settings and data on an access point.

Standalone access points (those which are not members of the cluster) are not shown on this page.



Manage access points in the cluster

Access Points...

Status: Clustering is online...

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

Clustering Options...

Enter the location of this AP.

Location: Vicky's Office - top shelf

Enter the name of the cluster for this AP to join.

Cluster Name: vicky-cluster

This page shows current basic configuration settings for clustered access points (location, MAC address, and IP address).

To see the full configuration for a specific AP, click on an IP address in the list.

Standalone access points or those which are not members of this cluster do not show up in this listing.

If you are looking for APs on the network that are not listed here; they may be in standalone mode or members of a different cluster. See the sections What Kinds of APs Can Cluster Together? and Standalone Mode in the Online Help.

More ....

Table 6.1 describes the access point settings and information display in detail.

Field	Description
Location	Description of where the access point is physically located.
MAC Address	Media Access Control (***MAC***) address of the access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point. The address shown here is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks. To see MAC addresses for Guest and Internal interfaces on the AP, see the *Status > interfaces* tab.
IP Address	Specifies the IP address for the access point. Each IP address is a link to the Administration Web pages for that access point. You can use the links to navigate to the Administration Web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.

Table 6.1 Access Point Settings

6.4.1 Modifying The Location Description

To make modifications to the location description:

1. Navigate to the *Cluster > Access Points* tab.
2. Under the *Clustering Options* section, type the new location of the AP in the *Location* field.
3. Click the **Update** button to apply the changes.

6.4.2 Setting The Cluster Name

To set the name of the cluster you want your AP to join, do the following:

1. Navigate to the Cluster > Access Points tab.
2. Under the *Clustering Options* section, type the new cluster name in the *Cluster Name* field.
3. Click the **Update** button to apply the changes.

Note: *If you want multiple APs to join a particular cluster, all these APs should have the same Cluster Name specified in the* Cluster Name *field. If the cluster name is different, the AP will not be able to join the cluster.*

6.5 Starting Clustering

To start clustering and add a particular access point to a cluster, do the following.

1. Go to the Administration Web pages for the standalone access point. (See “Navigating To An AP By Using Its IP Address In A URL” on page 62.)

   The Administration Web pages for the standalone access point are displayed.

2. Click the **Cluster > Access Points** tab for the standalone access point.
3. Click the **Start Clustering** button.
   The access point is now a cluster member. It appears in the list of clustered access points on the *Cluster > Access Points* tabbed page.

Note: *In some situations it is possible for the cluster to become out of sync. If after adding an access point to the cluster, the AP list does not reflect the added AP or shows an incomplete display; refer to the information on Cluster Recovery in Appendix D: “Troubleshooting” .*

6.6 Stopping Clustering

To stop clustering and remove a particular access point from a cluster, do the following.

1. Go to the Administration Web pages for the access point you want to remove from the cluster.
2. Click the **Cluster > Access Points** tab.
3. Click the **Stop Clustering** button to remove the access point from the Cluster.

The change will be reflected under *Status* for that access point; the access point will now show as *standalone* (instead of *cluster*).

Note: *In some situations it is possible for the cluster to become out of sync. If after removing an access point from the cluster, the AP list still reflects the deleted AP or shows an incomplete display, refresh your browser. If you still experience problems, refer to the information on Cluster Recovery in Appendix D: “Troubleshooting” .*

6.7 Navigating To Configuration Information For A Specific AP And Managing Standalone APs

In general, the 9160 G2 Wireless Gateway is designed for central management of *clustered* access points. For access points in a cluster, all access points in the cluster reflect the same configuration. In this case, it does not matter which access point you actually connect to for administration.

There may be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. Or you might want to configure and manage features on an access point that is running in *standalone* mode. In these cases, you can navigate to the Administration Web interface for individual access points by clicking the IP address links on the Access Point's tab.

All clustered access points are shown on the *Cluster > Access Points* page. To navigate to clustered access points, you can simply click on the IP address for a specific cluster member shown in the list.

6.7.1 Navigating To An AP By Using Its IP Address In A URL

You can also link to the Administration Web pages of a specific access point by entering the IP address for that access point as a URL directly into a Web browser address bar in the following form:

http://IPAddressOfAccessPoint

where *IPAddressOfAccessPoint* is the address of the particular access point you want to monitor or configure.

For standalone access points, this is the only way to navigate to their configuration information.

MANAGING USER ACCOUNTS 7

7.1 Overview

The 9160 G2 Wireless Gateway includes user management capabilities for controlling client access to access points.

User management and authentication must always be used in conjunction with the following two security modes, which require use of a ***RADIUS*** server for user authentication and management.

- IEEE 802.1x mode (see “IEEE 802.1x” on page 107 in Chapter 10: “Configuring Security”).
- WPA with RADIUS mode (see “WPA Enterprise” on page 112 in Chapter 10: “Configuring Security”).

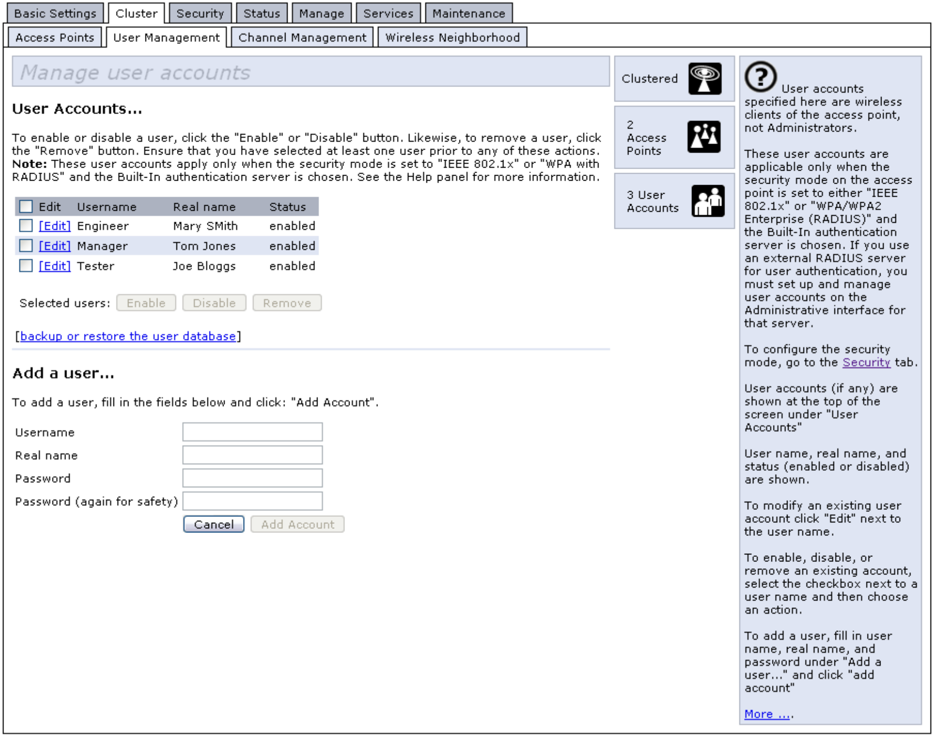
You have the option of using either the internal RADIUS server embedded in the 9160 G2 Wireless Gateway or an external RADIUS server that you provide. If you use the embedded RADIUS server, use the Administration Web page on the access point to set up and manage user accounts. If you are using an external RADIUS server, you will need to set up and manage user accounts on the Administrative interface for that server.

On the User Management page, you can create, edit, remove, and view client *user accounts*. Each user account consists of a user name and password. The set of users specified here represent approved *clients* that can log in and use one or more access points to access local, and possibly external, networks via your wireless network.

Note: *Users specified here are clients of the access point(s) who use the APs as a connectivity hub, not administrators of the wireless network. Only those with the administrator username and password and knowledge of the administration URL can log in as an administrator and view or modify configuration settings.*

7.2 Navigating To User Management For Clustered Access Points

To set up or modify user accounts, click the **Cluster > User Management** tab.



Manage user accounts

User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions. **Note:** These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

☐ Edit	Username	Real name	Status
☐ [Edit]	Engineer	Mary SMith	enabled
☐ [Edit]	Manager	Tom Jones	enabled
☐ [Edit]	Tester	Joe Bloggs	enabled

Selected users: Enable Disable Remove

[backup or restore the user database]

Add a user...

To add a user, fill in the fields below and click: "Add Account".

Username
Real name
Password
Password (again for safety)

Cancel Add Account

User accounts specified here are wireless clients of the access point, not Administrators.

These user accounts are applicable only when the security mode on the access point is set to either "IEEE 802.1x" or "WPA/WPA2 Enterprise (RADIUS)" and the Built-In authentication server is chosen. If you use an external RADIUS server for user authentication, you must set up and manage user accounts on the Administrative interface for that server.

To configure the security mode, go to the Security tab.

User accounts (if any) are shown at the top of the screen under "User Accounts"

User name, real name, and status (enabled or disabled) are shown.

To modify an existing user account click "Edit" next to the user name.

To enable, disable, or remove an existing account, select the checkbox next to a user name and then choose an action.

To add a user, fill in user name, real name, and password under "Add a user..." and click "add account"

More ....

7.3 Viewing User Accounts

User accounts are shown at the top of the screen under *User Accounts...* . The Username, Real name, and Status (enabled or disabled) of the user are shown. You make modifications to an existing user account by first selecting the checkbox next to a user name and then choosing an action. (See “Editing A User Account” on page 68.)

7.4 Adding A User

To create a new user, do the following:

1. Under *Add a User...*, provide information in the following fields.

Field	Description
Username	Provide a username. Usernames are alphanumeric strings of up to 237 characters. Do not use special characters or spaces.
Real name	For information purposes, provide the user's full name. There is a 256 character limit on real names.
Password	Specify a password for this user. Passwords are alphanumeric strings of up to 256 characters. Do not use special characters or spaces.

Table 7.1 New User Fields

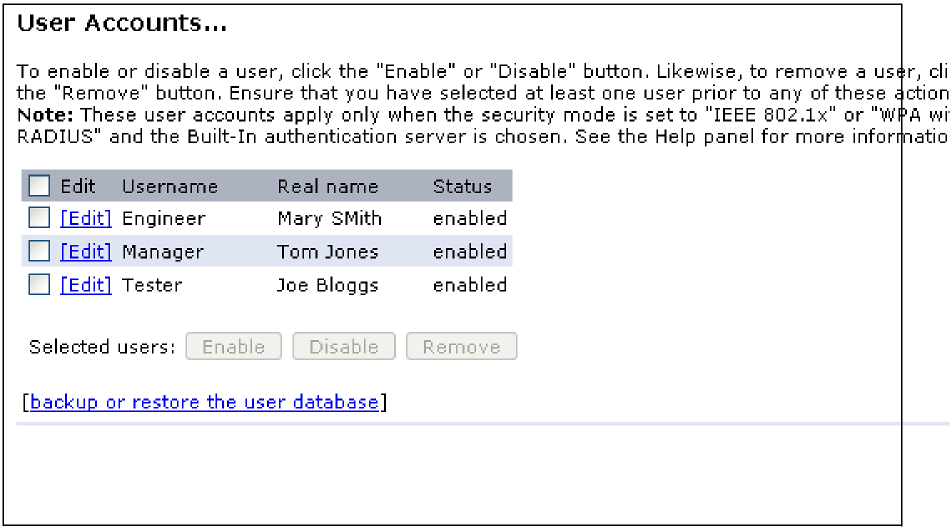
2. When you have filled in the fields, click **Add Account** to add the account.

   The new user is then displayed in *User Accounts...* . The user account is **enabled** by default when you first create it.

Note: *A limit of 100 user accounts per access point is imposed by the Administration user interface. Network usage may impose a more practical limit, depending upon the demand from each user.*

7.5 Editing A User Account

Once you have created a user account, it is displayed under *User Accounts...* at the top of the *User Management* Administration Web page. To make modifications to an existing user account, first click the checkbox next to the username so that the box is checked.



User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, cli the "Remove" button. Ensure that you have selected at least one user prior to any of these action **Note:** These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA wi RADIUS" and the Built-In authentication server is chosen. See the Help panel for more informatio

□	Edit	Username	Real name	Status
□	[Edit]	Engineer	Mary SMith	enabled
□	[Edit]	Manager	Tom Jones	enabled
□	[Edit]	Tester	Joe Bloggs	enabled

Then, choose an action such **Edit**, **Enable**, **Disable**, or **Remove**.

7.6 Enabling And Disabling User Accounts

A user account must be enabled for the user to log on as a client and use the access point.

You can **Enable** or **Disable** any user account. With this feature, you can maintain a set of user accounts and authorize or prevent users from accessing the network without having to remove or re-create accounts. This can come in handy in situations where users have an occasional need to access the network. For example, contractors who do work for your company on an intermittent but regular basis might need network access for 3 months at a time, then be off for 3 months, and back on for another assignment. You can enable and disable these user accounts as needed, and control access as appropriate.

7.6.1 Enabling A User Account

To enable a user account, click the checkbox next to the username and click **Enable**.

A user with an account that is *enabled* can log on to the wireless access points in your network as a client.

7.6.2 Disabling A User Account

To disable a user account, click the checkbox next to the username and click **Disable**.

A user with an account that is *disabled* cannot log on to the wireless access points in your network as a client. However, the user remains in the database and can be enabled later as needed.

7.7 Removing A User Account

To remove a user account, click the checkbox next to the username and click **Remove**.

If you think you might want to add this user back in at a later date, you might consider *disabling* the user rather than removing the account altogether.

7.8 Backing Up And Restoring A User Database

You can save a copy of the current set of user accounts to a backup configuration file. The backup file can be used at a later date to restore the user accounts on the AP to the previously saved configuration.

7.8.1 Backing Up The User Database

To create a backup copy of the user accounts for this access point:

1. Click the **[backup or restore the user database]** link.

   A *File Download or Open* dialog is displayed.

2. Choose the **Save** option on this first dialog.

   This brings up a file browser.

Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

You can keep the default file name (wirelessUsers.ubk) or rename the backup file, but be sure to save the file with a .ubk extension.

7.8.2 Restoring A User Database From A Backup File

To restore a user database from a backup file:

1. Select the backup configuration file you want to use, either by typing the full path and file name in the Restore field or click **Browse** and select the file.

   (Only those files that were created with the User Database Backup function and saved as .ubk backup configuration files are valid to use with Restore; for example, wirelessUsers.ubk.)

2. Click the **Restore** button.

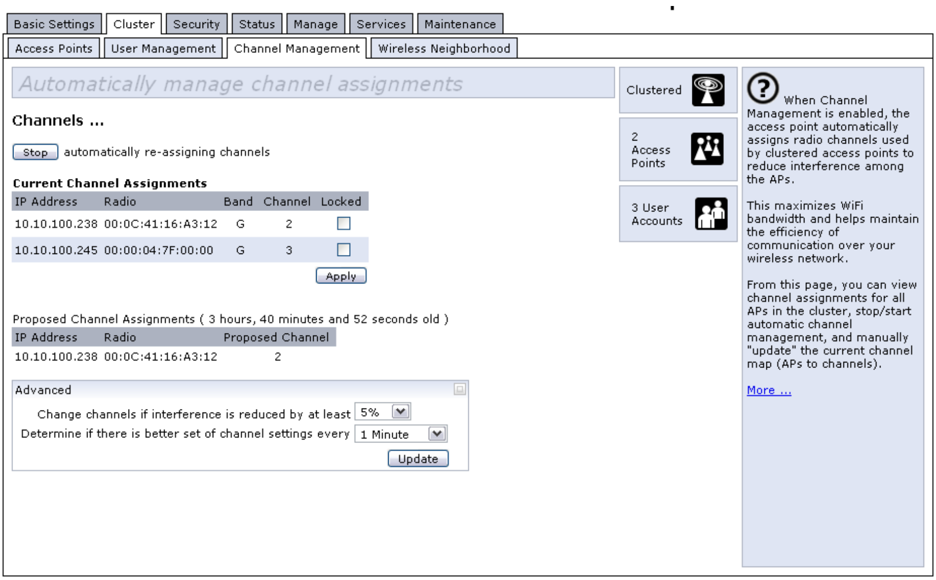
   When the backup restore process is complete, a message is shown to indicate that the user database has been successfully restored. (This process is not time-consuming; the restore should complete almost immediately.)

   Click the **Cluster > User Management** tab to see the restored user accounts.

CHANNEL MANAGEMENT 8

8.1 Navigating To Channel Management

To view session monitoring information, click the **Cluster > Channel Management** tab.



Automatically manage channel assignments

Channels ...

[Stop] automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Locked
10.10.100.238	00:0C:41:16:A3:12	G	2	□
10.10.100.245	00:00:04:7F:00:00	G	3	□

[Apply]

Proposed Channel Assignments (3 hours, 40 minutes and 52 seconds old)

IP Address	Radio	Proposed Channel
10.10.100.238	00:0C:41:16:A3:12	2

Advanced

Change channels if interference is reduced by at least: 5%

Determine if there is better set of channel settings every: 1 Minute

[Update]

Clustered

2 Access Points

3 User Accounts

When Channel Management is enabled, the access point automatically assigns radio channels used by clustered access points to reduce interference among the APs.

This maximizes WiFi bandwidth and helps maintain the efficiency of communication over your wireless network.

From this page, you can view channel assignments for all APs in the cluster, stop/start automatic channel management, and manually "update" the current channel map (APs to channels).

More ...

8.2 Understanding Channel Management

When *Channel Management* is enabled, the 9160 G2 Wireless Gateway automatically assigns radio channels used by clustered access points to reduce mutual interference (or interference with other access points outside of its cluster). This maximizes
Wi-Fi bandwidth and helps maintain the efficiency of communication over your wireless network.

(You must start channel management to get automatic channel assignments; it is disabled by default on a new AP. See “Stopping/Starting Automatic Channel Assignment” on page 76.)

8.2.1 How It Works In A Nutshell

At a specified interval (the default is **1 hour**) or on demand (click **Update**), the Channel Manager maps APs to channel use and measures interference levels in the cluster. If significant channel interference is detected, the Channel Manager automatically re-assigns some or all of the APs to new channels per an efficiency algorithm (or *automated channel plan*).

8.2.2 For The Curious: More About Overlapping Channels

The radio frequency (RF) broadcast ***Channel*** defines the portion of the radio spectrum that the radio on the access point uses for transmitting and receiving. The range of available channels for an access point is determined by the ***IEEE 802.11*** mode (also referred to as band) of the access point.

IEEE ***802.11b***/***802.11g*** modes (802.11 b/g) support use of channels 1 through 11 inclusive, while IEEE ***802.11a*** mode supports a larger set of non-consecutive channels (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165).

Interference can occur when multiple access points within range of each other are broadcasting on the same or *overlapping* channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic are competing for bandwidth.

The Channel Manager detects which bands (b/g or a) clustered APs are on, and uses a predetermined collection of channels that will not mutually interfere. For the “b/g” radio band, the classical set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap. A similar set of non-interfering channels is used for the “a” radio band, which includes all channels for that mode since they are not overlapping.

8.2.3 Example: A Network Before And After Channel Management

Without automated channel management, channel assignments to clustered APs might be made on *consecutive channels*, which would overlap and cause interference. For example, AP1 could be assigned to channel 6, AP2 to channel 6, and AP3 to channel 5 as shown in Figure 8.1 on page 75.

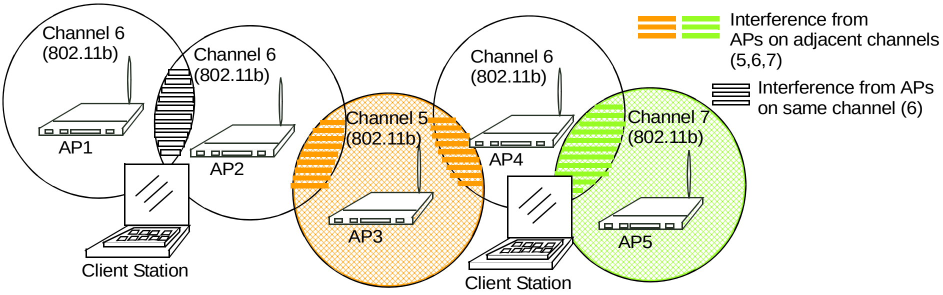


Figure 8.1 Without Automatic Channel Management

With automated channel management, APs in the cluster are automatically re-assigned to non-interfering channels as shown in Figure 8.2.

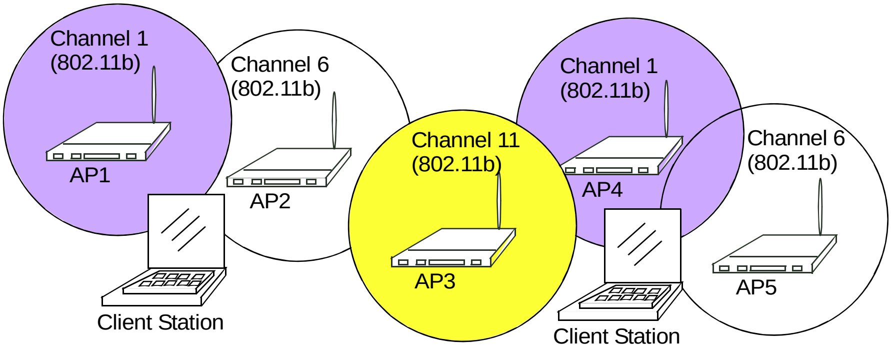


Figure 8.2 With Channel Management Enabled

8.3 Configuring And Viewing Channel Management Settings

The Channel Management page shows previous, current, and planned channel assignments for clustered access points. By default, automatic channel assignment is disabled. You can start channel management to optimize channel usage across the cluster on a scheduled interval.

From this page, you can view channel assignments for all APs in the cluster, stop/start automatic channel management, and manually “update” the current channel map (APs to channels). On a manual update, the Channel Manager will assess channel usage and, if necessary, re-assign APs to new channels to reduce interference based on the current Advanced Settings.

By using the Advanced settings you can modify the interference reduction potential that triggers channel re-assignment, change the schedule for automatic updates, and re-configure the channel set used for assignments.

The following sections describe how to configure and use channel management on your network:

- “Stopping/Starting Automatic Channel Assignment” on page 76.
- “Viewing Current Channel Assignments And Setting Locks” on page 77.
- “Update Current Channel Settings (Manual)” on page 77.
- “Viewing Last Proposed Set Of Changes” on page 78.
- “Configuring Advanced Settings (Customizing And Scheduling Channel Plans)” on page 78.
- “Update Advanced Settings” on page 80.

8.3.1 Stopping/Starting Automatic Channel Assignment

By default, automatic channel assignment is disabled (off).

- Click **Start** to resume automatic channel assignment. When automatic channel assignment is enabled, the Channel Manager periodically maps radio channels used by clustered access points and, if necessary, re-assigns channels on clustered APs to reduce interference (with cluster members or other APs outside the cluster).

Note: *Channel Management overrides the default cluster behaviour, which is to synchronize radio channels of all APs across a cluster. When Channel Management is enabled, the radio Channel is not sync'd across the cluster to other APs. See the note under Radio Settings in "Settings Shared In The Cluster Configuration" on page 57.*

- Click **Stop** to stop automatic channel assignment. (No channel usage maps or channel re-assignments will be made. Only manual updates will affect the channel assignment.)

8.3.2 Viewing Current Channel Assignments And Setting Locks

The *Current Channel Settings* shows a list of all access points in the cluster by IP Address. The display shows the band on which each AP is broadcasting, the current channel used by each AP, and an option to "lock" an AP on its current radio channel so that it cannot be re-assigned to another. Details about Current Channel Settings are provided below.

Field	Description
IP Address	Specifies the ***IP Address*** for the access point.
Radio	Indicates the ***MAC*** address of the access point.
Band	Indicates the band (b/g or a) on which the access point is broadcasting.
Channel	Indicates the radio ***Channel*** on which this access point is currently broadcasting.
Locked	Click **Locked** if you want to this access point to remain on the current channel. When the "Locked" checkbox is checked (enabled) for an access point, automated channel management plans will not re-assign the AP to a different channel as a part of the optimization strategy. Instead, APs with locked channels will be factored in as requirements for the plan. If you click **Update**, you will see that locked APs show the same channel for "Current Channel" and "Proposed Channel". Locked APs will keep their current channels.

Table 8.3 Current Channel Settings

8.3.2.1 Update Current Channel Settings (Manual)

You can run a manual channel management update at any time by clicking **Update** under the *Current Channel Settings* display.

8.3.3 Viewing Last Proposed Set Of Changes

The *Last Proposed Set of Channel Changes* shows the last channel plan. The plan lists all access points in the cluster by IP Address, and shows the current and proposed channels for each AP. Locked channels will not be re-assigned and the optimization of channel distribution among APs will take into account the fact that locked APs must remain on their current channels. APs that are not “Locked” may be assigned to different channels than they were previously using, depending on the results of the plan.

Field	Description
IP Address	Specifies the ***IP Address*** for the access point.
Current	Indicates the radio channel on which this access point is currently broadcasting.
Proposed	Indicates the radio channel to which this access point would be re-assigned if the Channel Plan is executed.

Table 8.4 AP’s Channel Plan

8.3.4 Configuring Advanced Settings (Customizing And Scheduling Channel Plans)

If you use *Channel Management* as provided (without updating *Advanced Settings*), channels are automatically fine-tuned once every hour if interference can be reduced by 25 percent or more. Channels will be re-assigned even if the network is busy. The appropriate channel sets will be used (‘b/g’ for APs using IEEE 802.11b/g and ‘a’ for APs using IEEE 802.11a).

These defaults are designed to satisfy most scenarios where you would need to implement channel management.

You can use *Advanced Settings* to modify the interference reduction potential that triggers channel re-assignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments.

Field	Description
Advanced	Click the “Advanced” toggle to show / hide display settings that modify timing and details of the channel planning algorithm. By default, these settings are **hidden**.
Change channels if interference is reduced by at least__	Specify the minimum percentage of interference reduction a proposed plan must achieve in order to be applied. The default is **25 percent.** Use the drop-down menu to choose percentages ranging from 25% to 75%. This setting lets you set a gating factor for channel re-assignment so that the network is not continually disrupted for minimal gains in efficiency. For example, if channel interference must be reduced by 75%, and the proposed channel assignments will only reduce interference by 30%, then channels will not be re-assigned. However; if you re-set the minimal channel interference benefit to 25% and click **Update**, the proposed channel plan will be implemented and channels re-assigned as needed.
Determine if there is better set of channel settings every__	Use the drop-down menu to specify the schedule for automated updates. A range of intervals is provided, from “1 Minute” to “6 Months”. The default is “**1 Hour**” (channel usage re-assessed and the resulting channel plan applied every hour).
Use these channels when applying channel assignments	Choose a set of non-interfering channels on a particular band (“b/g” or “a”). The choices are: • b/g channels 1-6-11 • b/g channels 1-4-8-11 • a IEEE ***802.11b***/***802.11g*** modes (802.11 b/g) support use of channels 1 through 11. For the “b/g” radio band, the classic set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap. IEEE ***802.11a*** mode supports a larger set of non-consecutive channels (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165). All “a” band channels are non-interfering.
Apply channel modifications even when the network is busy	Click to **enable** or **disable** this setting. A checkmark indicates it is enabled and channel modifications will be applied even when the network is busy. If this is not checked, channel modifications will not be applied on a busy network. This setting (along with the interference reduction setting) is designed to help weigh the cost/benefit impact on network performance of re-assigning channels against the inherent disruption it can cause to clients during a busy time.

Table 8.5 Advanced Settings

8.3.4.1 Update Advanced Settings

Click **Update** under *Advanced Settings* to apply these settings.

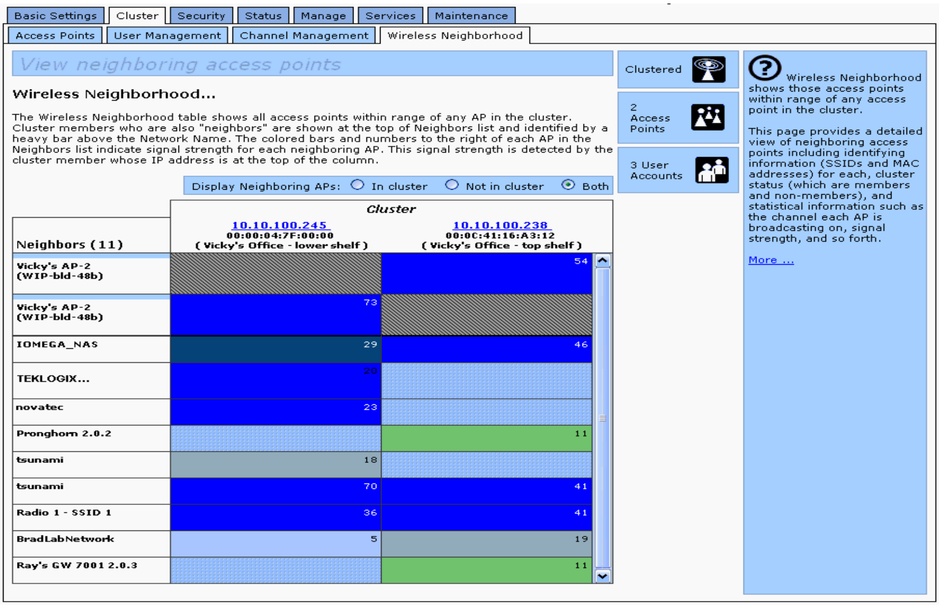
Advanced Settings will take effect when they are applied, and influence how automatic channel management is performed. (The new interference reduction minimum, scheduled tuning interval, channel set, and network busy settings will be taken into account for automated and manual updates.)

WIRELESS NEIGHBORHOOD 9

The *Wireless Neighborhood* screen shows those access points within range of any access point in the cluster. This page provides a detailed view of neighboring access points, including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each AP is broadcasting on, signal strength, and so forth.

9.1 Navigating To Wireless Neighborhood

To view the *Wireless Neighborhood*, click the **Cluster > Wireless Neighborhood** tab.



Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ○ In cluster ○ Not in cluster ● Both

	Cluster	
Neighbors (11)	10.10.100.245 00:00:04:7F:00:00 (Vicky's Office - lower shelf)	10.10.100.238 00:0C:41:16:A3:12 (Vicky's Office - top shelf)
Vicky's AP-2 (WIP-bld-48b)	▨	54
Vicky's AP-2 (WIP-bld-48b)	73	▨
IOMEGA_NAS	29	46
TEKLOGIX...	20	
novatec	23	
Pronghorn 2.0.2		11
tsunami	18	
tsunami	70	41
Radio 1 - SSID 1	36	41
BradLabNetwork	5	19
Ray's GW 7001 2.0.3		11

Wireless Neighborhood shows those access points within range of any access point in the cluster.

This page provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each AP is broadcasting on, signal strength, and so forth.

Figure 9.1 Neighbor APs Both In Cluster And Not In Cluster

9.2 Understanding Wireless Neighborhood Information

The *Wireless Neighborhood* view shows all access points within range of every member of the cluster, shows which access points are within range of which cluster members, and distinguishes between cluster members and non-members.

For each neighbor access point, the Wireless Neighborhood view shows identifying information (***SSID*** or Network Name, ***IP Address***, ***MAC*** address) along with radio statistics (signal strength, channel, beacon interval). You can click on an AP to get additional statistics about the APs in radio range of the currently selected AP.

The Wireless Neighborhood view can help you:

- Detect and locate unexpected (or *rogue*) access points in a wireless domain so that you can take action to limit associated risks.
- Verify coverage expectations. By assessing which APs are visible at what signal strength from other APs, you can verify that the deployment meets your planning goals.
- Detect faults. Unexpected changes in the coverage pattern are evident at a glance in the colour-coded table.

9.3 Viewing Wireless Neighborhood

Details about Wireless Neighborhood information shown is described below.

Field	Description
Display Neighboring APs	Click one of the following radio buttons to change the view: • *In cluster* - Shows only neighbor APs that are members of the cluster. • *Not in cluster* - Shows only neighbor APs that are not cluster members. • *Both* - Shows all neighbor APs (cluster members and non-members).
Cluster	The “Cluster” list at the top of the table shows IP addresses for all access points in the cluster. (This is the same list of cluster members shown on the *Cluster* > *Access Points* tab described in “Navigating To Access Points Management” on page 55.) If there is only one AP in the cluster, only a single IP address column will be displayed here; indicating that the AP is “clustered with itself”. You can click on an IP address to view more details on a particular AP as shown in Figure 9.3 on page 86.

Table 9.2 Wireless Neighborhood Statistics

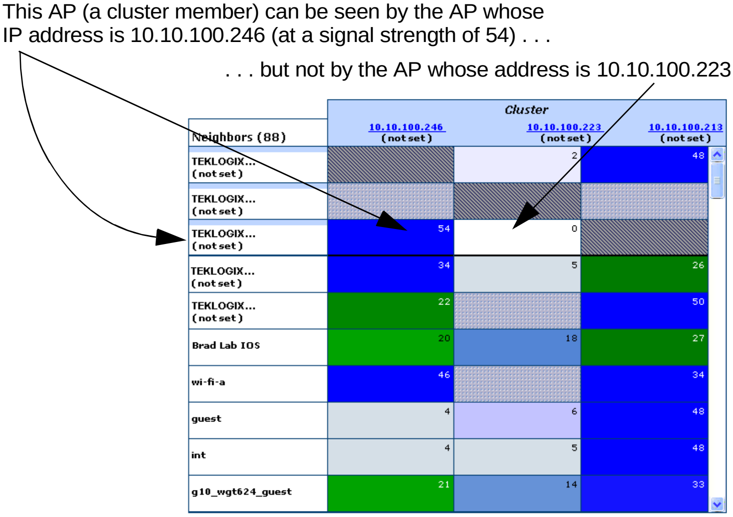
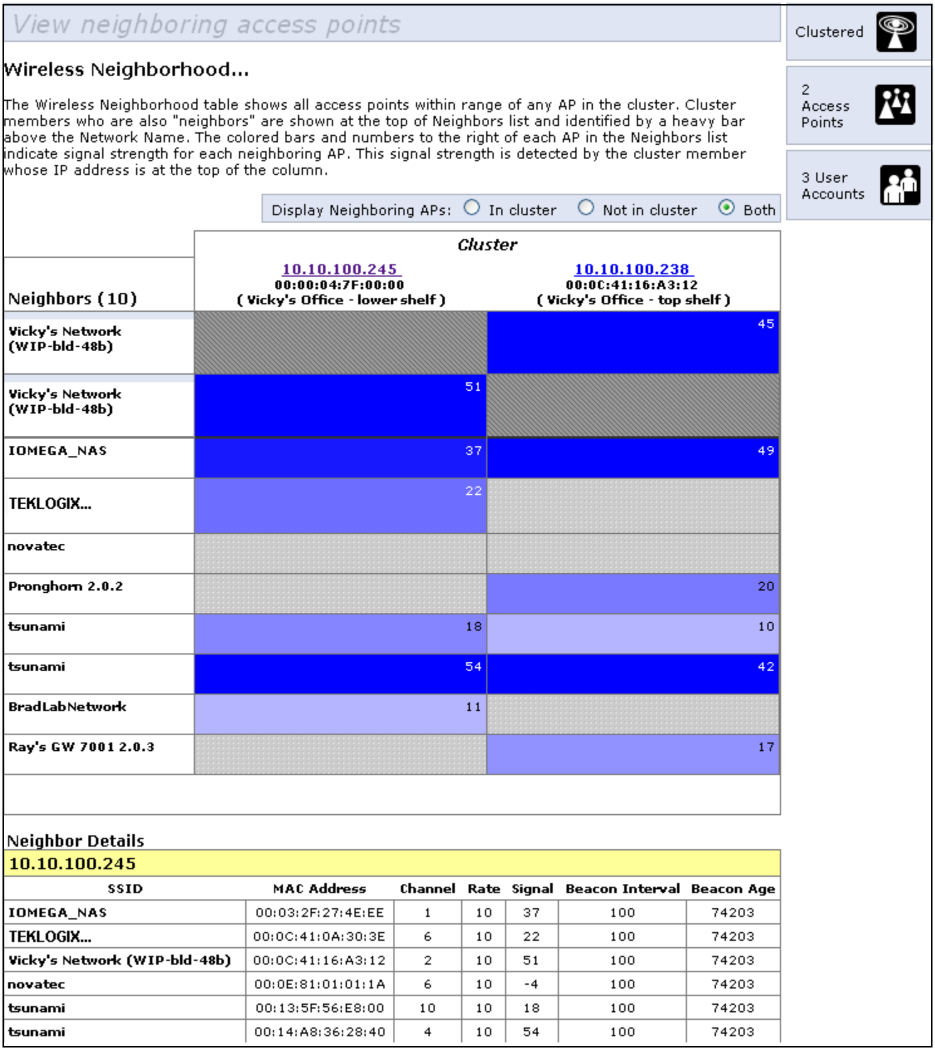
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><i>Neighbors</i></td><td>
Access points which are neighbors of one or more of the clustered APs are listed in the left column by SSID (Network Name). An access point which is detected as a neighbor of a cluster member can also be a cluster member itself. Neighbors who are also cluster members are always shown at the top of the list with a heavy bar above and include a location indicator.
The coloured bars to the right of each AP in the Neighbors list shows the signal strength for each of the neighbor APs as detected by the cluster member whose IP address is shown at the top of the column:

This AP (a cluster member) can be seen by the AP whose IP address is 10.10.100.246 (at a signal strength of 54) . . .
. . . but not by the AP whose address is 10.10.100.223
<table>
<tr><th></th><th colspan="3">Cluster</th></tr>
<tr><th>Neighbors (88)</th><th>10.10.100.246
(not set)</th><th>10.10.100.223
(not set)</th><th>10.10.100.213
(not set)</th></tr>
<tr><td>TEKLOGIX...
(not set)</td><td>▨</td><td>2</td><td>48</td></tr>
<tr><td>TEKLOGIX...
(not set)</td><td>░</td><td>▨</td><td>░</td></tr>
<tr><td>TEKLOGIX...
(not set)</td><td>54</td><td>0</td><td>▨</td></tr>
<tr><td>TEKLOGIX...
(not set)</td><td>34</td><td>5</td><td>26</td></tr>
<tr><td>TEKLOGIX...
(not set)</td><td>22</td><td>░</td><td>50</td></tr>
<tr><td>Brad Lab IOS</td><td>20</td><td>18</td><td>27</td></tr>
<tr><td>wi-fi-a</td><td>46</td><td>░</td><td>34</td></tr>
<tr><td>guest</td><td>4</td><td>6</td><td>48</td></tr>
<tr><td>int</td><td>4</td><td>5</td><td>48</td></tr>
<tr><td>g10_wgt624_guest</td><td>21</td><td>14</td><td>33</td></tr>
</table>
<ul>
<li><b>Dark Blue Bar</b> - A dark blue bar and a high signal strength number (for example 50) indicates good signal strength detected from the Neighbor seen by the AP whose IP address is listed above that column.</li>
<li><b>Lighter Blue Bar -</b> A lighter blue bar and a lower signal strength number (for example 20 or lower) indicates medium or weak signal strength from the Neighbor seen by the AP whose IP address is listed above that column.</li>
<li><b>White Bar</b> - A white bar and the number 0 indicates that a neighboring AP that was detected by one of the cluster members cannot be detected by the AP whose IP address is listed above that column.</li>
<li><b>Light Gray Bar -</b> A light gray bar and no signal strength number indicates a Neighbor that is detected by other cluster members but not by the AP whose IP address is listed above that column.</li>
<li><b>Dark Gray Bar</b> - A dark gray bar and no signal strength number indicates this <i>is</i> the AP whose IP address is listed above that column (since it is not applicable to show how well the AP can detect itself).</li>
</ul>
</td></tr>
</table>

Table 9.2 Wireless Neighborhood Statistics

9.4 Viewing Details For A Cluster Member

To view details on a cluster member AP, click on the **IP address** of a cluster member at the top of the page.



View neighboring access points

Clustered

2 Access Points

3 User Accounts

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ○ In cluster ○ Not in cluster ● Both

	Cluster	
Neighbors (10)	10.10.100.245 00:00:04:7F:00:00 (Vicky's Office - lower shelf)	10.10.100.238 00:0C:41:16:A3:12 (Vicky's Office - top shelf)
Vicky's Network (WIP-bld-48b)	▨	45
Vicky's Network (WIP-bld-48b)	51	▨
IOMEGA_NAS	37	49
TEKLOGIX...	22	
novatec		
Pronghorn 2.0.2		20
tsunami	18	10
tsunami	54	42
BradLabNetwork	11	
Ray's GW 7001 2.0.3		17

Neighbor Details

10.10.100.245

SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
IOMEGA_NAS	00:03:2F:27:4E:EE	1	10	37	100	74203
TEKLOGIX...	00:0C:41:0A:30:3E	6	10	22	100	74203
Vicky's Network (WIP-bld-48b)	00:0C:41:16:A3:12	2	10	51	100	74203
novatec	00:0E:81:01:01:1A	6	10	-4	100	74203
tsunami	00:13:5F:56:E8:00	10	10	18	100	74203
tsunami	00:14:A8:36:28:40	4	10	54	100	74203

Figure 9.3 Details For A Cluster Member AP

The following table explains the details shown about the selected AP.

Field	Description
SSID	The *Service Set Identifier* (***SSID***) for the access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. The SSID is set in Basic Settings (Chapter 5: “Configuring Basic Settings”) or in *Advanced* > *Wireless Settings* (Chapter 13: “Setting the Wireless Interface”.) A Guest network and an Internal network running on the same access point must always have two different network names.
MAC Address	Shows the ***MAC*** address of the neighboring access point. A ***MAC*** address is a hardware address that uniquely identifies each node of a network.
Channel	Shows the channel on which the access point is currently broadcasting. The ***Channel*** defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The channel is set in *Advanced* > *Radio*. (See Chapter 16: “Configuring 802.11 Radio Settings”.)
Rate	Shows the rate (in megabits per second) at which this access point is currently transmitting. The current rate will always be one of the rates shown in *Supported Rates*.
Signal	Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).
Beacon Interval	Shows the ***Beacon*** interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on *Advanced* > *Radio*. (See Chapter 16: “Configuring 802.11 Radio Settings”.)
Beacon Age	Shows the date and time of the most recent beacon was transmitted from the access point.

Table 9.4 Access Point Statistics

CONFIGURING SECURITY 10

The following sections describe how to configure Security settings on the 9160 G2 Wireless Gateway.

10.1 Understanding Security Issues On Wireless Networks

Wireless mediums are inherently less secure than wired mediums. For example, an Ethernet ***NIC*** transmits its packets over a physical medium such as coaxial cable or twisted pair. A wireless NIC broadcasts radio signals over the air allowing a wireless LAN to be easily tapped without physical access or sophisticated equipment. A hacker equipped with a laptop, a wireless NIC, and a bit of knowledge can easily attempt to compromise your wireless network. One does not even need to be within normal range of the access point. By using a sophisticated antenna on the client, a hacker may be able to connect to the network from many miles away.

The 9160 G2 Wireless Gateway provides a number of authentication and encryption schemes to ensure that your wireless infrastructure is accessed only by the intended users. The details of each security mode are described in the sections below.

See also the related topic, Appendix C: “Security Settings On Wireless Clients And RADIUS Server Setup”.

10.1.1 How Do I Know Which Security Mode To Use?

In general, we recommend that on your Internal network you use the most robust security mode that is feasible in your environment. When configuring security on the access point, you first must choose the security mode, then in some modes an authentication algorithm, and whether to allow clients not using the specified security mode to associate.

Wi-Fi Protected Access (***WPA***) with *Remote Authentication Dial-In User Service* (***RADIUS***) using the CCMP (AES) encryption algorithm provides the best data protection available and is clearly the best choice if all client stations are equipped with WPA supplicants. However, backward compatibility or interoperability issues with clients or even with other access points may require that you configure WPA with RADIUS with a different encryption algorithm or choose one of the other security modes.

That said, however, security may not be as much of a priority on some types of networks. If you are simply providing internet and printer access, as on a guest network, setting the security mode to *None (Plain-text)* may be the appropriate choice. To prevent clients from accidentally discovering and connecting to your network, you can disable the broadcast SSID so that your network name is not advertised. If the network is sufficiently isolated from access to sensitive information, this may offer enough protection in some situations. This level of protection is the only one offered for guest networks, and also may be the right convenience trade-off for other scenarios where the priority is making it as easy as possible for clients to connect. (See "Does Prohibiting The Broadcast SSID Enhance Security?" on page 98)

Following is a brief discussion of what factors make one mode more secure than another, a description of each mode offered, and when to use each mode.

10.1.2 Comparison Of Security Modes For Key Management, Authentication And Encryption Algorithms

Three major factors that determine the effectiveness of a security protocol are:

- How the protocol manages keys.
- Presence or absence of integrated user authentication in the protocol.
- Encryption algorithm or formula the protocol uses to encode/decode the data.

Following is a list of the security modes available on the 9160 G2 Wireless Gateway, along with a description of the key management, authentication, and encryption algorithms used in each mode. We include some suggestions as to when one mode might be more appropriate than another.

- "When To Use Unencrypted (No Security)" on page 93.
- "When To Use Static WEP" on page 93.
- "When To Use IEEE 802.1x" on page 94.
- "When To Use WPA Personal" on page 95.
- "When To Use WPA Enterprise" on page 96.

10.1.2.1 When To Use Unencrypted (No Security)

Setting the security mode to *None (Plain-text)* by definition provides no security. In this mode, the data is not encrypted but rather sent as "plain-text" across the network. No key management, data encryption or user authentication is used.

Recommendations

Unencrypted mode, i.e. None (Plain-text), is not recommended for regular use on the Internal network because it is not secure. This is the only mode in which you can run the Guest network, which is by definition an unsecure LAN, always virtually or physically separated from any sensitive information on the Internal LAN.

Therefore, only set the security mode to *None (Plain-text)* on the Guest network, and on the Internal network for initial setup, testing, or problem solving only.

See Also

For information on how to configure unencrypted security mode, see "None (Plain-text)" on page 100.

10.1.2.2 When To Use Static WEP

Static *Wired Equivalent Privacy* (***WEP***) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Key Management	Encryption Algorithm	User Authentication
*Static **WEP** uses a fixed key that is provided by the administrator. WEP keys are indexed in different slots (up to four on the 9160 G2 Wireless Gateway).* *The client stations must have the same key indexed in the same slot to access data on the access point.*	An ***RC4*** stream cipher is used to encrypt the frame body and *cyclic redundancy checking* (CRC) of each 802.11 frame.	If you set the Authentication Algorithm to "Shared Key", this protocol provides a rudimentary form of user authentication. However, if the Authentication Algorithm is set to "Open System", no authentication is performed. If the algorithm is set to "Both", only WEP clients are authenticated.

Table 10.1 Static WEP Security Mode

Recommendations

Static WEP was designed to provide security equivalent of sending unencrypted data through an Ethernet connection, however it has major flaws and it does not provide even this intended level of security.

Therefore, **Static WEP is not recommended** as a secure mode. The only time to use Static WEP is when interoperability issues make it the only option available to you and you are not concerned with the potential of exposing the data on your network.

See Also

For information on how to configure Static WEP security mode, see “Static WEP” on page 102.

10.1.2.3 When To Use IEEE 802.1x

IEEE ***802.1x*** is the standard for passing the Extensible Authentication Protocol (***EAP***) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than Static WEP.

Key Management	Encryption Algorithm	User Authentication
IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. *There are different* ***Unicast*** *keys for each station.*	An ***RC4*** stream cipher is used to encrypt the frame body and *cyclic redundancy checking* (CRC) of each 802.11 frame.	IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server. You have a choice of using the 9160 G2 Wireless Gateway embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

Table 10.2 IEEE 801.1x Security Mode

Recommendations

IEEE 802.1x mode is a better choice than Static WEP because keys are dynamically generated and changed periodically. However, the encryption algorithm used is the same as that of Static WEP and is therefore not as reliable as the more advanced encryption methods such as ***TKIP*** and ***CCMP*** (***AES***) used in *Wi-Fi Protected Access* (***WPA***) or ***WPA2***.

Additionally, compatibility issues may be cumbersome because of the variety of authentication methods supported and the lack of a standard implementation method.

Therefore, IEEE 802.1x mode is not as secure a solution as *Wi-Fi Protected Access* (***WPA***) or ***WPA2***. If you cannot use ***WPA*** because some of your client stations do not have WPA, then a better solution than using IEEE 802.1x mode is to **use WPA Enterprise** mode.

See Also

For information on how to configure IEEE 802.1x security mode, see "IEEE 802.1x" on page 107.

10.1.2.4 When To Use WPA Personal

Wi-Fi Protected Access Personal *Pre-Shared Key* (***PSK***) is an implementation of the Wi-Fi Alliance IEEE ***802.11h*** standard, which includes *Advanced Encryption Algorithm* (AES), *Counter mode/CBC-MAC Protocol* (CCMP), and *Temporal Key Integrity Protocol* (***TKIP***) mechanisms. This mode offers the same encryption algorithms as WPA 2 with RADIUS but without the ability to integrate a RADIUS server for user authentication.

This security mode is backwards-compatible for wireless clients that support only the original ***WPA***.

Key Management	Encryption Algorithms	User Authentication
WPA Personal provides dynamically-generated keys that are periodically refreshed. *There are different **Unicast** keys for each station.*	• Temporal Key Integrity Protocol (***TKIP***). • Counter mode/CBC-MAC Protocol (***CCMP***) Advanced Encryption Standard (***AES***).	The use of a Pre-Shared (***PSK***) key provides user authentication similar to that of shared keys in ***WEP***.

Table 10.3 WPA Personal Security Mode

Recommendations

WPA Personal is not recommended for use with the 9160 G2 Wireless Gateway when WPA Enterprise is an option.

We recommend that you use WPA Enterprise mode instead, unless you have interoperability issues that prevent you from using this mode.

For example, some devices on your network may not support WPA or WPA2 with ***EAP*** talking to a ***RADIUS*** server. Embedded printer servers or other small client devices with very limited space for implementation may not support RADIUS. For such cases, we recommend that you use WPA Personal.

See Also

For information on how to configure this security mode, see “WPA Personal” on page 109.

10.1.2.5 When To Use WPA Enterprise

Wi-Fi Protected Access Enterprise with *Remote Authentication Dial-In User Service* (***RADIUS***) is an implementation of the Wi-Fi Alliance IEEE ***802.11h*** standard, which includes *Advanced Encryption Standard* (***AES***), *Counter mode/CBC-MAC Protocol* (***CCMP***), and *Temporal Key Integrity Protocol* (***TKIP***) mechanisms. This mode requires the use of a RADIUS server to authenticate users. WPA Enterprise provides the best security available for wireless networks.

This security mode also provides backwards-compatibility for wireless clients that support only the original ***WPA***.

Key Management	Encryption Algorithms	User Authentication
WPA Enterprise mode provides dynamically-generated keys that are periodically refreshed. *There are different* ***Unicast*** *keys for each station.*	• Temporal Key Integrity Protocol (***TKIP***). • Counter mode/CBC-MAC Protocol (***CCMP***) Advanced Encryption Standard (***AES***).	Remote Authentication Dial-In User Service (***RADIUS***) You have a choice of using the 9160 G2 Wireless Gateway embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

Table 10.4 WPA Enterprise Security Mode

Recommendations

WPA Enterprise mode is the **recommended mode**. The ***CCMP*** (***AES***) and ***TKIP*** encryption algorithms used with WPA modes are far superior to the ***RC4*** algorithm used for Static ***WEP*** or IEEE 802.1x modes. Therefore, CCMP (AES) or TKIP should be used whenever possible. All WPA modes allow you to use these encryption schemes, so WPA security modes are recommended above the others when using WPA is an option. Additionally, this mode incorporates a RADIUS server for user authentication which gives it an edge over WPA Personal mode.

Use the following guidelines for choosing options within the WPA Enterprise mode security mode:

1. The best security you can have to date on a wireless network is WPA Enterprise mode using CCMP (AES) encryption algorithm. AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks. If all clients or other APs on the network are WPA/CCMP compatible, use this encryption algorithm. (If all clients are WPA2 compatible, choose to support only WPA2 clients.)

2. The second best choice is WPA Enterprise with the encryption algorithm set to both TKIP and CCMP. This lets WPA client stations without CCMP associate, uses TKIP for encrypting ***Multicast*** and ***Broadcast*** frames, and allows clients to select whether to use CCMP or TKIP for ***Unicast*** (AP-to-single-station) frames. This WPA configuration allows more interoperability, at the expense of some security. Client stations that support CCMP can use it for their ***Unicast*** frames. If you encounter AP-to-station interoperability problems with the "Both" encryption algorithm setting, then you will need to select TKIP instead. (See next option.)

3. The third best choice is WPA Enterprise with the encryption algorithm set to ***TKIP***. Some clients have interoperability issues with CCMP and TKIP enabled at same time. If you encounter this problem, then choose TKIP as the encryption algorithm. This is the standard WPA mode, and most interoperable mode with client Wireless software security features. TKIP is the only encryption algorithm that is being tested in ***Wi-Fi WPA*** certification.

See Also

For information on how to configure this security mode, see "WPA Enterprise" on page 112.

10.1.3 Does Prohibiting The Broadcast SSID Enhance Security?

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.

Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor unencrypted traffic.

This offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.

(See also "Guest Network" on page 101.)

10.1.4 How Does Station Isolation Protect The Network?

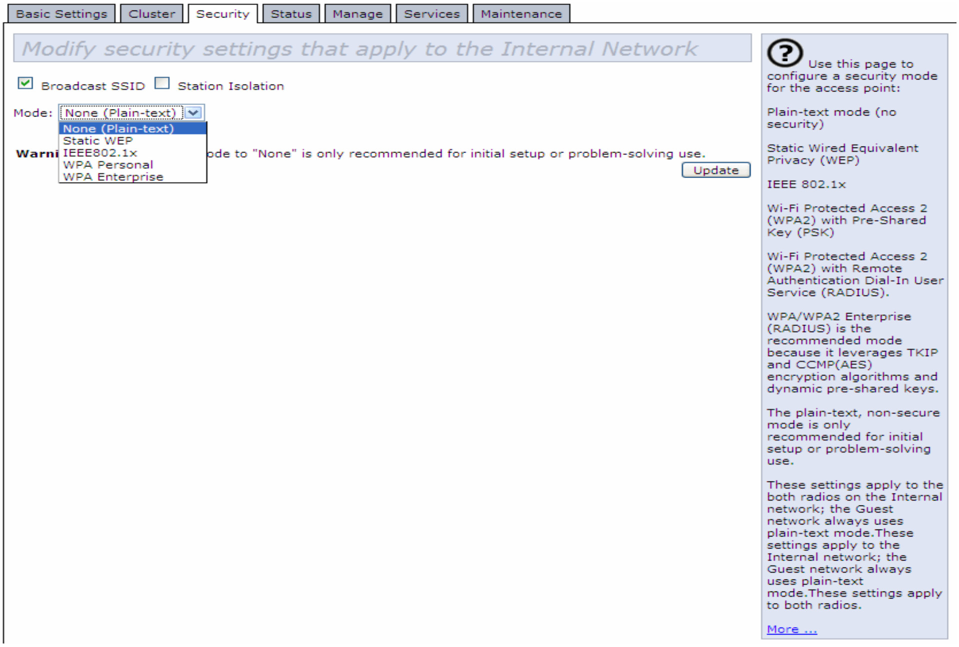
When *Station Isolation* is enabled, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients.

The traffic blocking extends to wireless clients connected to the network via ***WDS*** links; these clients cannot communicate with each other when Station Isolation is on.

See Chapter 20: "Wireless Distribution System" for more information about WDS.

10.2 Configuring Security Settings

To set the security mode, navigate to the *Security* tab, and update the fields as described below.



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: None (Plain-text)

None (Plain-text)
Static WEP
IEEE802.1x
WPA Personal
WPA Enterprise

Warni ode to "None" is only recommended for initial setup or problem-solving use.

Use this page to configure a security mode for the access point:

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS).

WPA/WPA2 Enterprise (RADIUS) is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the both radios on the Internal network; the Guest network always uses plain-text mode.These settings apply to the Internal network; the Guest network always uses plain-text mode.These settings apply to both radios.

The following configuration information explains how to configure security modes on the access point. Keep in mind that each wireless client that wants to exchange data with the access point must be configured with the same security mode and encryption key settings consistent with access point security.

On a two-radio AP, these Security Settings apply to both radios.

Note: *Security modes other than Plain-text apply only to configuration of the "Internal" network. On the "Guest" network, you can use only Plain-text mode. (For more information about guest networks, see Chapter 14: "Setting up Guest Access".)*

10.2.1 Broadcast SSID, Station Isolation, And Security Mode

To configure security on the access point, select a security mode and fill in the related fields as described in Table 10.5.

Note: *You can also allow or prohibit the Broadcast SSID and enable/disable Station Isolation as extra precautions as mentioned below.)*

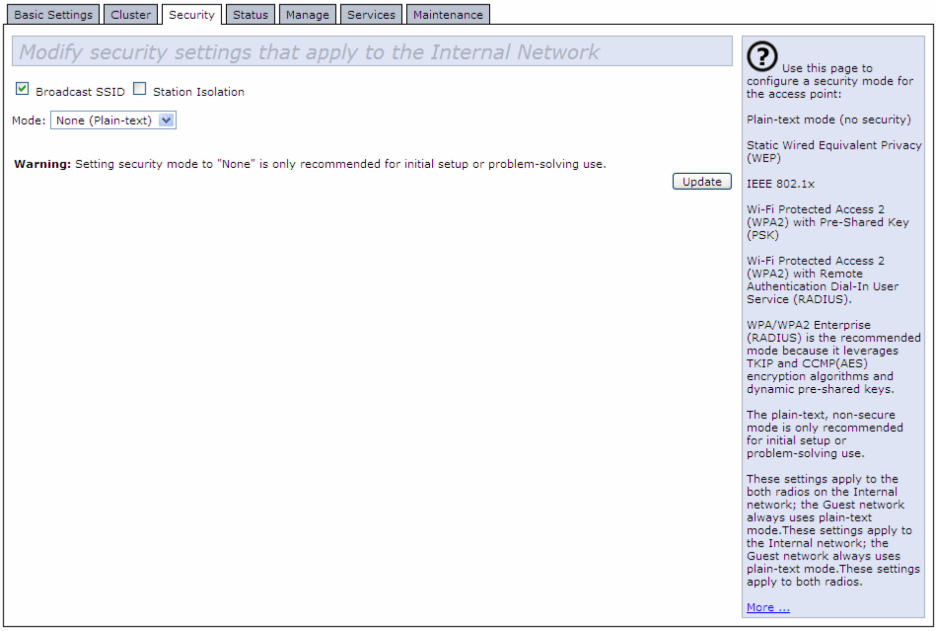
Field	Description
Broadcast SSID	To enable the Broadcast SSID, select the checkbox directly beside it. By default, the access point broadcasts (allows) the *Service Set Identifier* (***SSID***) in its beacon frames. You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.
Station Isolation	To enable station isolation, select the checkbox directly beside it. • When Station Isolation is **disabled**, wireless clients can communicate with one another normally by sending traffic through the access point. • When Station Isolation is **enabled**, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. The traffic blocking extends to wireless clients connected to the network via ***WDS*** links; these clients cannot communicate with each other when Station Isolation is on. See Chapter 20: "Wireless Distribution System" for more information about WDS.
Security Mode	Select the *Security Mode*. Select one of the following: • "None (Plain-text)" on page 100. • "Static WEP" on page 102. • "IEEE 802.1x" on page 107. • "WPA Personal" on page 109. • "WPA Enterprise" on page 112. For a Guest network, the only security mode that can be applied is "None (Plain-text)". (For more information, see Chapter 14: "Setting up Guest Access".) Security modes other than "None (Plain-text)" apply only to configuration of the "Internal" network.

Table 10.5 Security Settings

10.2.2 None (Plain-text)

None (or plain-text security) means any data transferred to and from the 9160 G2 Wireless Gateway is not encrypted.

If you select **None (Plain-text)** as your security mode, no further options are configurable on the AP. This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: None (Plain-text)

Warning: Setting security mode to "None" is only recommended for initial setup or problem-solving use.

Use this page to configure a security mode for the access point:

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS).

WPA/WPA2 Enterprise (RADIUS) is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the both radios on the Internal network; the Guest network always uses plain-text mode.These settings apply to the Internal network; the Guest network always uses plain-text mode.These settings apply to both radios.

10.2.3 Guest Network

Setting security to “None (Plain-text)” is the only mode in which you can run the Guest network, which is by definition an easily accessible, unsecure ***LAN*** always virtually or physically separated from any sensitive information on the Internal LAN. For example, the guest network might simply provide internet and printer access for day visitors.

The absence of security on the Guest AP is designed to make it as easy as possible for guests to get a connection without having to program any security settings in their clients.

For a minimum level of protection on a guest network, you can choose to suppress (prohibit) the broadcast of the SSID (network name) to discourage client stations from automatically discovering your access point. (See also “Does Prohibiting The Broadcast SSID Enhance Security?” on page 98).

For more about the Guest network, see Chapter 14: “Setting up Guest Access”.

10.2.4 Static WEP

Wired Equivalent Privacy (***WEP***) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

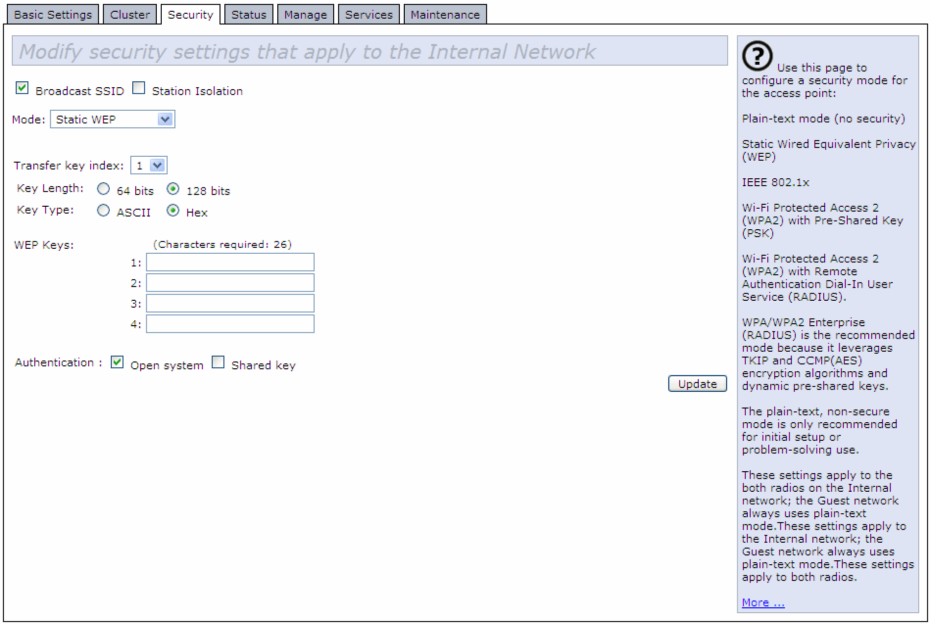
You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Static WEP is not the most secure mode available, but it offers more protection than setting security to “None (Plain-text)”, as it does prevent an outsider from easily sniffing out unencrypted wireless traffic. (For more secure modes, see the sections on “IEEE 802.1x” on page 107, “WPA Personal” on page 109.), or “WPA Enterprise” on page 112.

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a “stream” cipher called RC4.) The access point uses a key to transmit data to the client stations. Each client station must use that same key to decrypt data it receives from the access point.

Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you selected “Static WEP” Security Mode, provide the information on the access point settings, as shown in the following figure and described in Table 10.6.



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: Static WEP

Transfer key index: 1

Key Length: ○ 64 bits ● 128 bits

Key Type: ○ ASCII ● Hex

WEP Keys: (Characters required: 26)

1:
2:
3:
4:

Authentication : ☑ Open system ☐ Shared key

Use this page to configure a security mode for the access point:

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS).

WPA/WPA2 Enterprise (RADIUS) is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the both radios on the Internal network; the Guest network always uses plain-text mode.These settings apply to the Internal network; the Guest network always uses plain-text mode.These settings apply to both radios.

Field	Description
Transfer Key Index	Select a key index from the drop-down menu. Key indexes 1 through 4 are available. The default is 1. The Transfer Key Index indicates which WEP key the access point will use to encrypt the data it transmits.
Key Length	Specify the length of the key by clicking one of the radio buttons: • 64 bits • 128 bits
Key Type	Select the key type by clicking one of the radio buttons: • ASCII • Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.

Table 10.6 Static WEP Security Settings

Field	Description
WEP Keys	You can specify up to four WEP keys. In each text box, enter a string of characters for each key. If you selected "ASCII", enter any combination of integers and letters `0-9`, `a-z`, and `A-Z`. If you selected "HEX", enter hexadecimal digits (any combination of `0-9` and `a-f` or `A-F`). Use the same number of characters for each key as specified in the "Characters Required" field. These are the RC4 WEP keys shared with the stations using the access point. Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the AP. (See "Rules To Remember For Static WEP" on page 104.)
Authentication Algorithm	The authentication algorithm defines the method used to determine whether a client station is allowed to associate with an access point when static WEP is the security mode. Specify the authentication algorithm you want to use by choosing one of the following from the drop-down menu: • Open System. • Shared Key. • Both. **Open System** authentication allows any client station to associate with the access point whether that client station has the correct WEP key or not. This is algorithm is also used in plaintext, IEEE 802.1x, and WPA modes. When the authentication algorithm is set to "Open System", any client can associate with the access point. Note that just because a client station is allowed to *associate* does not ensure it can exchange traffic with an access point. A station must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point. **Shared Key** authentication requires the client station to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to "Shared Key", a station with an incorrect WEP key will not be able to associate with the access point. **Both** is the default. When the authentication algorithm is set to "Both": • Client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the access point. • Client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the access point even if they do not have the correct WEP key.

Table 10.6 Static WEP Security Settings

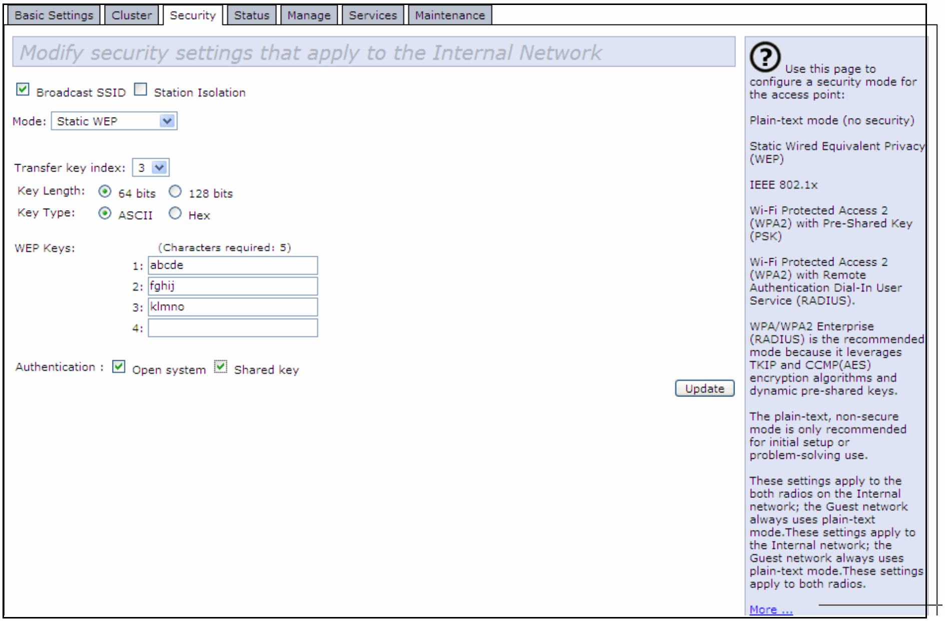
10.2.4.1 Rules To Remember For Static WEP

- All client stations must have the Wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the AP in order to de-code AP-to-station data transmissions.

- The AP must have all keys used by clients for station-to-AP transmit so that it can de-code the station transmissions.
- The same key must occupy the same slot on all nodes (AP and clients). For example if the AP defines abc123 key as WEP key 3, then the client stations must define that same string as WEP key 3.
- On some wireless client software (like Funk Odyssey), you can configure multiple WEP keys and define a client station "transfer key index", and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring APs cannot decode each other's transmissions.

10.2.4.2 Example Of Using Static WEP

For a simple example, suppose you configure three WEP keys on the access point. In our example, the Transfer Key Index for the AP is set to **3**. This means that the WEP key in slot "3" is the key the access point will use to encrypt the data it sends.



Modify security settings that apply to the Internal Network

☑ Broadcast SSID □ Station Isolation

Mode: Static WEP

Transfer key index: 3

Key Length: ● 64 bits ○ 128 bits

Key Type: ● ASCII ○ Hex

WEP Keys: (Characters required: 5)

1: abcde
2: fghij
3: klmno
4:

Authentication : ☑ Open system ☑ Shared key

? Use this page to configure a security mode for the access point:

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS).

WPA/WPA2 Enterprise (RADIUS) is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

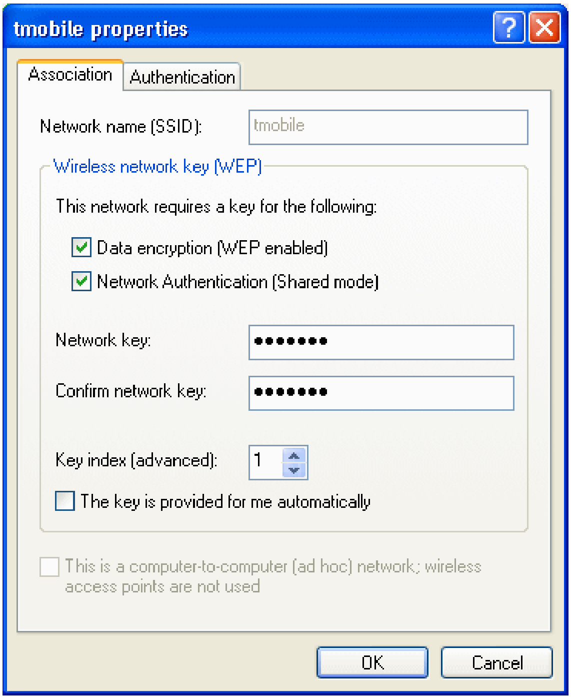
These settings apply to the both radios on the Internal network; the Guest network always uses plain-text mode.These settings apply to the Internal network; the Guest network always uses plain-text mode.These settings apply to both radios.

More ...

Figure 10.7 Setting The AP Transfer Key On The Access Point

You must then set all client stations to use WEP and provide each client with one of the slot/key combinations you defined on the AP.

For this example, we'll set WEP key 1 on a Windows client.



Network name (SSID): tmobile

Wireless network key (WEP)

This network requires a key for the following:

☑ Data encryption (WEP enabled)

☑ Network Authentication (Shared mode)

Network key: •••••••

Confirm network key: •••••••

Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Figure 10.8 Providing A Wireless Client With A WEP Key

If you have a second client station, that station also needs to have one of the WEP keys defined on the AP. You could give it the same WEP key you gave to the first station. Or for a more secure solution, you could give the second station a different WEP key (key 2, for example) so that the two stations cannot decrypt each other's transmissions.

10.2.4.3 Static WEP With Transfer Key Indexes On Client Stations

Some Wireless client software (like Funk Odyssey) lets you configure multiple WEP keys and set a transfer index on the client station, then you can specify different keys to be used for station-to-AP transmissions. (The standard Windows wireless client software does not allow you to do this.)

To build on our example, using Funk Odyssey client software you could give each of the clients WEP key 3 so that they can decode the AP transmissions with that key and also give client 1 WEP key 1 and set this as its transfer key. You could then give client 2 WEP key 2 and set this as its transfer key index.

Figure 10.9 illustrates the dynamics of the AP and two client stations using multiple WEP keys and a transfer key index.

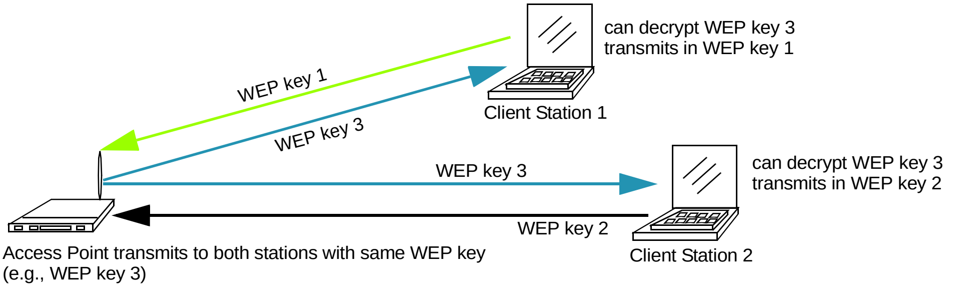


Figure 10.9 Example Of Using Multiple WEP Keys And Transfer Key Index On Client Stations

10.2.5 IEEE 802.1x

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (***EAP***) messages sent over an ***IEEE 802.11*** wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

This mode requires the use of a ***RADIUS*** server to authenticate users. If the option for the internal RADIUS server is enabled, configure user accounts on the AP via the *Cluster > User Management* tab. Otherwise configure user accounts on the external RADIUS server.

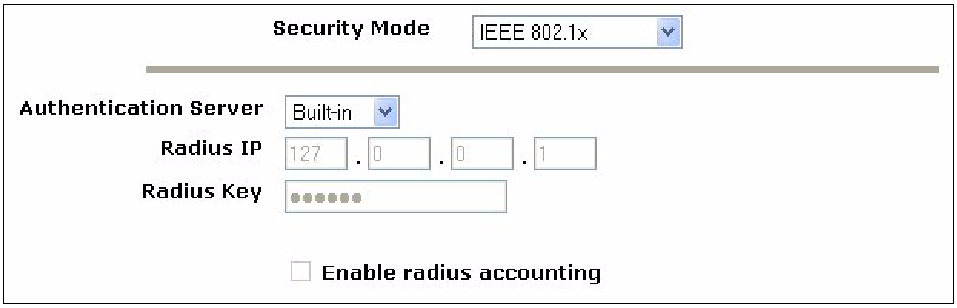
The access point requires a RADIUS server capable of ***EAP***, such as the Microsoft Internet Authentication Server or the 9160 G2 Wireless Gateway internal authentication server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and ***MSCHAP V2***.

When configuring IEEE 802.1x mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The

9160 G2 Wireless Gateway embedded RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

If you use your own RADIUS server, you have the option of using any of a variety of authentication methods that the IEEE 802.1x mode supports, including certificates, Kerberos, and public key authentication. Keep in mind, however, that the client stations must be configured to use the same authentication method being used by the access point.

If you selected “IEEE 802.1x” Security Mode, provide the following:



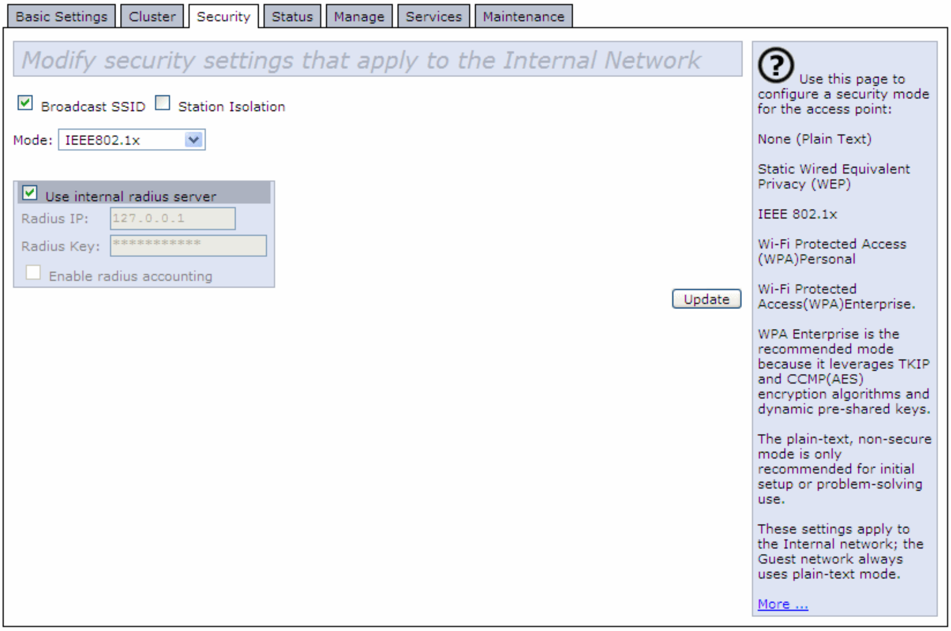
Security Mode: IEEE 802.1x

Authentication Server: Built-in

Radius IP: 127 . 0 . 0 . 1

Radius Key: ●●●●●●

□ Enable radius accounting



Modify security settings that apply to the Internal Network

☑ Broadcast SSID □ Station Isolation

Mode: IEEE802.1x

☑ Use internal radius server

Radius IP: 127.0.0.1

Radius Key: ***********

□ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

Field	Description
Use internal radius server	Select one of the following from the drop-down menu: • To use the authentication server provided with the 9160 G2 Wireless Gateway, ensure the checkbox beside the **Use internal radius server field** is selected. If this option is selected, you do not have to provide the Radius IP and Radius Key; they are automatically provided. If the option for the internal RADIUS server is enabled, configure user accounts on the AP via the *Cluster > User Management* tab. For more information, see Chapter 7: "Managing User Accounts". • To use an external authentication server, ensue the checkbox beside the **Use internal radius server field** is deselected. If you deselect this checkbox, you must supply a Radius IP and Radius Key of the server you want to use. ***Note:*** *The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the 9160 G2 Wireless Gateway, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The 9160 G2 Wireless Gateway is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)*
Radius IP	Enter the Radius IP in the text box. The *Radius IP* is the IP address of the ***RADIUS*** server. (The 9160 G2 Wireless Gateway internal authentication server is `127.0.0.1`.) For information on setting up user accounts, see Chapter 7: "Managing User Accounts".
Radius Key	Enter the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you enter will be displayed as " * " characters to prevent others from seeing the RADIUS key as you type. (The 9160 G2 Wireless Gateway internal authentication server key is secret.) This value is never sent over the network.
Enable radius accounting	Click the checkbox beside "Enable radius accounting" if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.

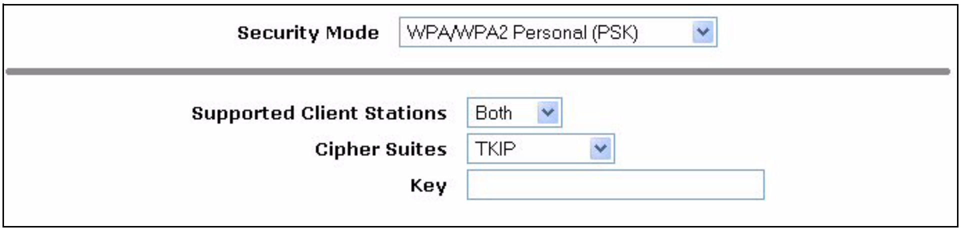
Table 10.10 IEEE 802.1x Security Settings

10.2.6 WPA Personal

Wi-Fi Protected Access Personal is a Wi-Fi Alliance IEEE ***802.11i*** standard, which includes *Counter mode/CBC-MAC Protocol-Advanced Encryption Algorithm* (***CCMP-AES***), and *Temporal Key Integrity Protocol* (***TKIP***) mechanisms.

The Personal version of WPA employs a pre-shared key (instead of using IEEE ***802.1x*** and ***EAP*** as is used in the Enterprise WPA security mode). The PSK is used for an initial check of credentials only. This security mode is backwards-compatible for wireless clients that support the original ***WPA***.

If you selected "WPA Personal" *Security Mode*, complete the settings as described in Table 10.11 on page 111.

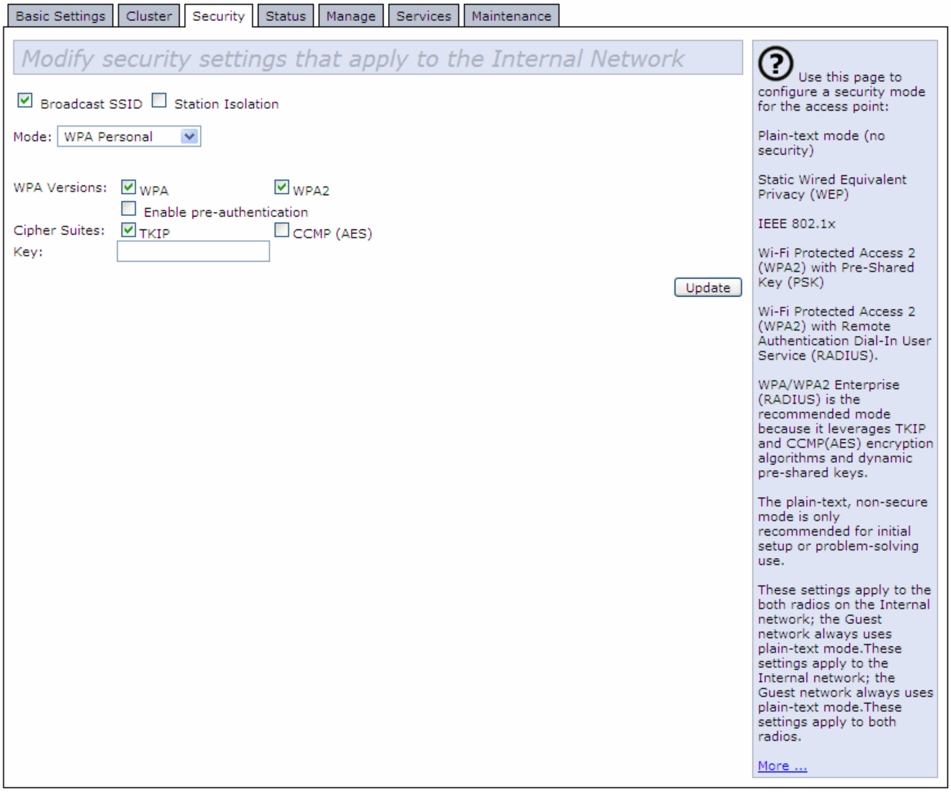


Security Mode WPA/WPA2 Personal (PSK)

Supported Client Stations Both

Cipher Suites TKIP

Key



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: WPA Personal

WPA Versions: ☑ WPA ☑ WPA2

☐ Enable pre-authentication

Cipher Suites: ☑ TKIP ☐ CCMP (AES)

Key:

Use this page to configure a security mode for the access point:

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS).

WPA/WPA2 Enterprise (RADIUS) is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the both radios on the Internal network; the Guest network always uses plain-text mode.These settings apply to the Internal network; the Guest network always uses plain-text mode.These settings apply to both radios.

Field	Description
WPA Versions	Select the types of client stations you want to support: • WPA • WPA2 • Both **WPA.** If all client stations on the network support the original ***WPA*** but none support the newer ***WPA2***, then select WPA. **WPA2.** If all client stations on the network support ***WPA2***, we suggest using WPA2 which provides the best security per the ***IEEE 802.11i*** standard. **Both.** If you have a mix of clients, some of which support ***WPA2*** and others which support only the original ***WPA***, select “Both”. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
Cipher Suites	Select the cipher suite you want to use: • TKIP • CCMP (AES) • Both **Temporal Key Integrity Protocol** (***TKIP***) is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit “temporal key” shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. **Counter mode/CBC-MAC Protocol** (***CCMP***) is an encryption method for IEEE ***802.11i*** that uses the **Advanced Encryption Algorithm** (***AES***). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. If you select both TKIP and CCMP(AES), Pairwise cipher is AES and Groupwise cipher is TKIP. Pairwise cipher is used for unicast traffic and Groupwise cipher is used for multicast/broadcast traffic. Both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the AP: • A valid TKIP key • A valid CCMP (AES) key Clients not configured to use a ***WPA*** Personal will not be able to associate with AP.

Table 10.11 WPA Personal Security Settings

Field	Description
Key	The *Pre-shared Key* is the shared secret key for ***WPA*** Personal. Enter a string of at least 8 characters to a maximum of 63 characters.

Table 10.11 WPA Personal Security Settings

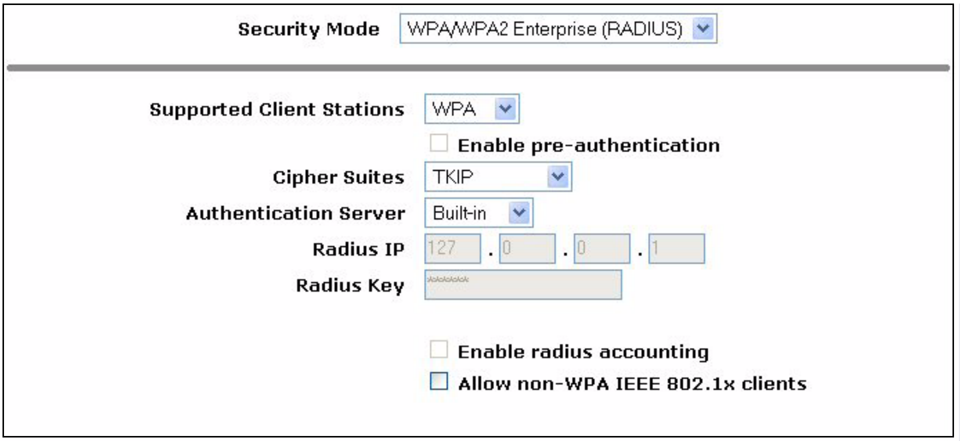
10.2.7 WPA Enterprise

Wi-Fi Protected Access Enterprise with *Remote Authentication Dial-In User Service* (***RADIUS***) is an implementation of the Wi-Fi Alliance IEEE ***802.11h*** standard, which includes *Advanced Encryption Standard* (***AES***), *Counter mode/CBC-MAC Protocol* (***CCMP***), and *Temporal Key Integrity Protocol* (***TKIP***) mechanisms. The Enterprise mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts via the *Cluster, User Management* tab.

This security mode is backwards-compatible with wireless clients that support the original ***WPA***.

When configuring WPA Enterprise mode, you have a choice of whether to use the built-in RADIUS server or an external RADIUS server that you provide. The 9160 G2 Wireless Gateway built-in RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

If you selected “WPA Enterprise” *Security Mode*, complete the settings as described in Table 10.12 on page 113.



Security Mode: WPA/WPA2 Enterprise (RADIUS)

Supported Client Stations: WPA

□ Enable pre-authentication

Cipher Suites: TKIP

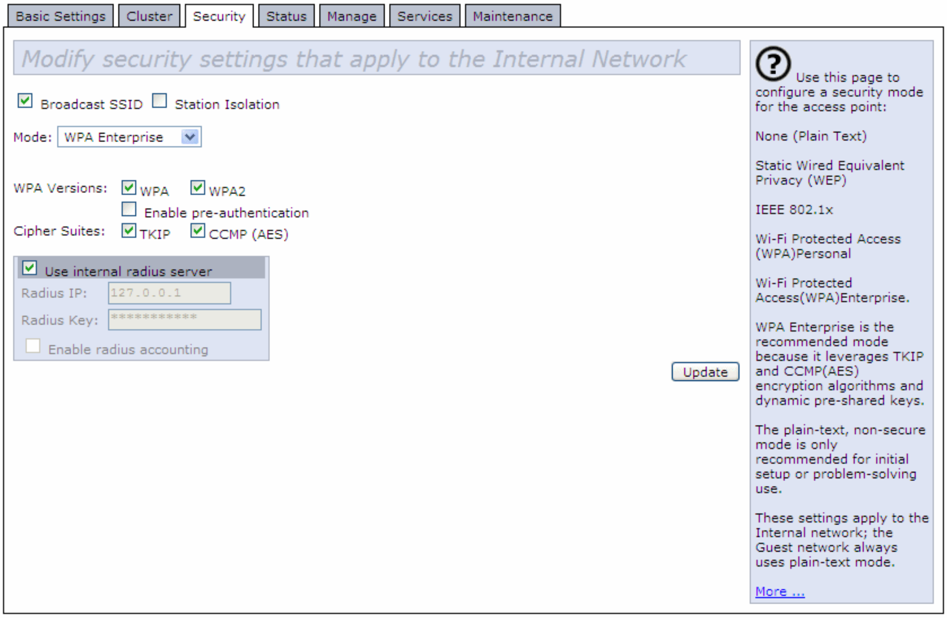
Authentication Server: Built-in

Radius IP: 127 . 0 . 0 . 1

Radius Key: ******

□ Enable radius accounting

□ Allow non-WPA IEEE 802.1x clients



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☑ WPA ☑ WPA2
☐ Enable pre-authentication

Cipher Suites: ☑ TKIP ☑ CCMP (AES)

☑ Use internal radius server

Radius IP: 127.0.0.1

Radius Key: ***********

☐ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

Field	Description
WPA Versions	Select the types of client stations you want to support: • WPA • WPA2 • Both **WPA.** If all client stations on the network support the original ***WPA*** but none support the newer ***WPA2***, then select WPA. **WPA2.** If all client stations on the network support ***WPA2***, we suggest using WPA2 which provides the best security per the ***IEEE 802.11i*** standard. **Both.** If you have a mix of clients, some of which support ***WPA2*** and others which support only the original ***WPA***, select both WPA and WPA2. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.

Table 10.12 WPA Enterprise Security Settings

Field	Description
Enable pre-authentication	If for WPA Versions you select only WPA2 or both WPA and WPA2, you can enable pre-authentication for WPA2 clients. Click **Enable** pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. This option does not apply if you selected “WPA” for WPA Versions because the original WPA does not support this feature.
Cipher Suites	Select the cipher you want to use: • ***TKIP*** • ***CCMP*** (***AES***) • Both **Temporal Key Integrity Protocol** (***TKIP***) is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit “temporal key” shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. **Counter mode/CBC-MAC Protocol** (***CCMP***) is an encryption method for IEEE ***802.11i*** that uses the **Advanced Encryption Algorithm** (***AES***). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. When both TKIP and CCMP are selected, both TKIP and AES clients can associate with the access point. Client stations configured to use WPA with RADIUS must have one of the following to be able to associate with the AP: • A valid TKIP RADIUS IP address and valid shared Key. • A valid CCMP (AES) IP address and valid shared Key. Clients not configured to use WPA with RADIUS will not be able to associate with AP. By default both TKIP and CCMP are selected. When both TKIP and CCMP are selected, client stations configured to use WPA with RADIUS must have one of the following: • A valid TKIP RADIUS IP address and RADIUS Key. • A valid CCMP (AES) IP address and RADIUS Key.

Table 10.12 WPA Enterprise Security Settings

Field	Description
Use internal radius server	You can choose whether to use the built-in authentication server provided with the 9160 G2 Wireless Gateway, or you can use an external radius server. • To use the authentication server provided with the 9160 G2 Wireless Gateway, ensure the checkbox beside the Use internal radius server field is selected. If this option is selected, you do not have to provide the Radius IP and Radius Key; they are automatically provided. If the option for the internal RADIUS server is enabled, configure user accounts on the AP via the *Cluster* > *User Management* tab. For more information, see Chapter 7: “Managing User Accounts”. • To use an external authentication server, ensue the checkbox beside the **Use internal radius server field** is deselected. If you deselect this checkbox you must supply a Radius IP and Radius Key of the server you want to use. ***Note:*** *The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the 9160 G2 Wireless Gateway, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The 9160 G2 Wireless Gateway is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)*
Radius IP	Enter the Radius IP in the text box. The *Radius IP* is the IP address of the ***RADIUS*** server. (The 9160 G2 Wireless Gateway internal authentication server is `127.0.0.1`.) For information on setting up user accounts, see Chapter 7: “Managing User Accounts”.
Radius Key	Enter the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you enter will be displayed as “ * ” characters to prevent others from seeing the RADIUS key as you type. (The 9160 G2 Wireless Gateway internal authentication server key is *`secret`*.) This value is never sent over the network.
Enable RADIUS Accounting	Click **Enable RADIUS Accounting** if you want to enforce authentication for ***WPA*** client stations with user names and passwords for each station. See also Chapter 7: “Managing User Accounts”.

Table 10.12 WPA Enterprise Security Settings

10.3 Updating Settings

To update Security settings:

1. Navigate to the *Security* tab page.
2. Configure the security settings as required.
3. Click the **Update** button to apply the changes.

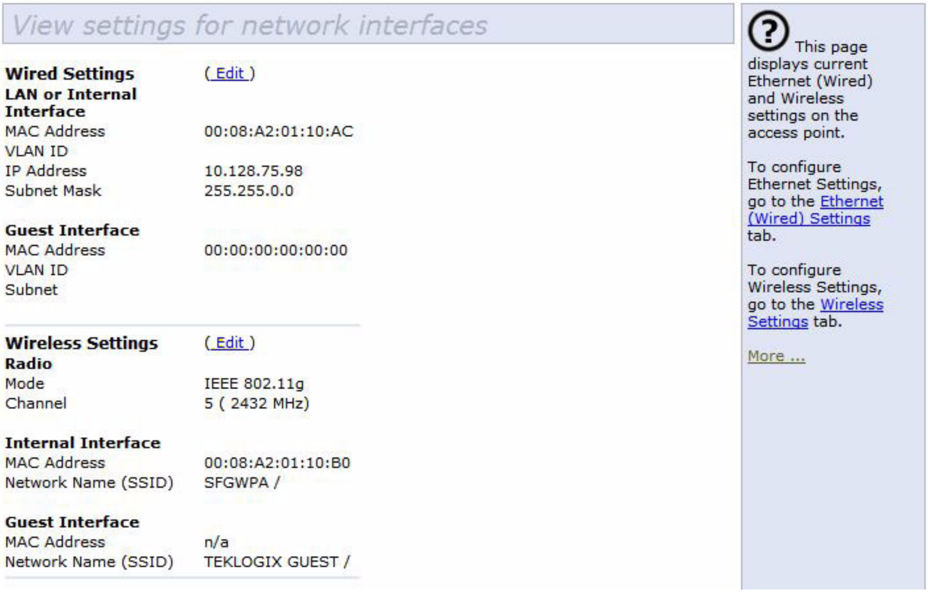
MAINTENANCE AND MONITORING 11

Important: ***The maintenance and monitoring tasks described here all pertain to viewing and modifying settings on specific access points; not on a cluster configuration that is automatically shared by multiple access points. Therefore, it is important to ensure that you are accessing the Administration Web pages for the particular access point you want to configure. For information on this, see "Navigating To Configuration Information For A Specific AP And Managing Standalone APs" on page 62.***

11.1 Interfaces

To monitor wired LAN and wireless LAN (***WLAN***) settings, navigate to *Status > Interfaces* on the access point you want to monitor.

Note: *On a two-radio access point, current wireless settings for both Radio One and Radio Two are shown. On a one-radio access point, settings are shown for one radio. The* Interfaces *page for a two-radio AP is shown in the following figure.*



View settings for network interfaces

Wired Settings	(Edit)
LAN or Internal Interface	
MAC Address	00:08:A2:01:10:AC
VLAN ID	
IP Address	10.128.75.98
Subnet Mask	255.255.0.0
Guest Interface	
MAC Address	00:00:00:00:00:00
VLAN ID	
Subnet	
Wireless Settings	(Edit)
Radio	
Mode	IEEE 802.11g
Channel	5 (2432 MHz)
Internal Interface	
MAC Address	00:08:A2:01:10:B0
Network Name (SSID)	SFGWPA /
Guest Interface	
MAC Address	n/a
Network Name (SSID)	TEKLOGIX GUEST /

? This page displays current Ethernet (Wired) and Wireless settings on the access point.

To configure Ethernet Settings, go to the Ethernet (Wired) Settings tab.

To configure Wireless Settings, go to the Wireless Settings tab.

More ...

This page displays the current settings of the 9160 G2 Wireless Gateway. It displays the *Ethernet (Wired) Settings* and the *Wireless Settings*.

11.1.1 Ethernet (Wired) Settings

The *Internal* interface includes the Ethernet ***MAC** Address*, ***IP Address***, ***Subnet Mask***, and Associated Network Wireless Name (***SSID***).

The *Guest* interface includes the *MAC Address*, ***VLAN** ID*, and Associated Network Wireless Name (***SSID***).

If you want to change any of these settings, click the **Edit** link.

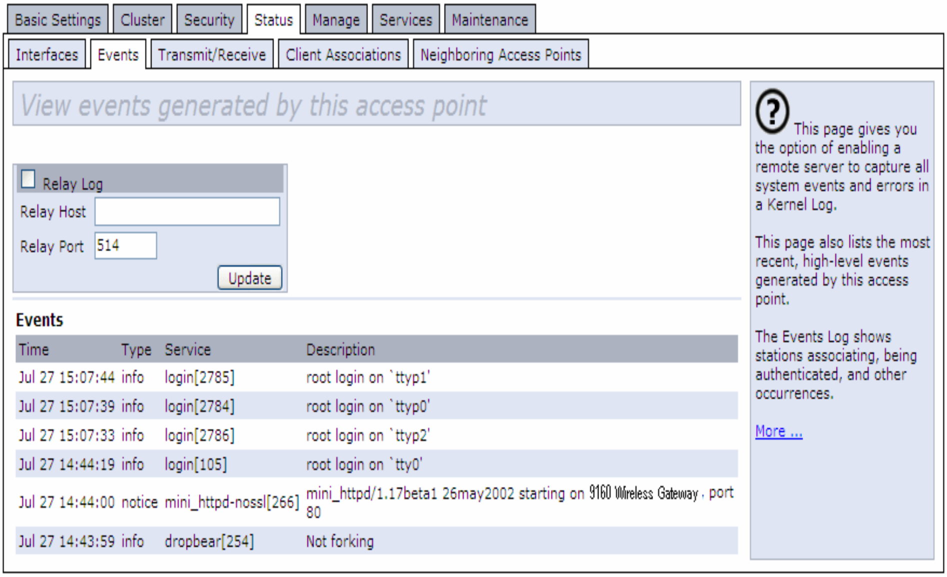
11.1.2 Wireless Settings

The *Radio* interface includes the radio *Mode*, and ***Channel***. Also shown here are ***MAC** addresses* (read-only) and Network Names for the internal and guest interfaces. (See Chapter 13: “Setting the Wireless Interface” and Chapter 16: “Configuring 802.11 Radio Settings” for more information.)

If you want to change any of these settings, click the **Edit** link.

11.2 Event Logs

To view system events and kernel log for a particular access point, navigate to *Status*, *Events* on the Administration Web pages for the access point you want to monitor.



View events generated by this access point

□ Relay Log

Relay Host

Relay Port 514

Events

Time	Type	Service	Description
Jul 27 15:07:44	info	login[2785]	root login on `ttyp1'
Jul 27 15:07:39	info	login[2784]	root login on `ttyp0'
Jul 27 15:07:33	info	login[2786]	root login on `ttyp2'
Jul 27 14:44:19	info	login[105]	root login on `tty0'
Jul 27 14:44:00	notice	mini_httpd-nossl[266]	mini_httpd/1.17beta1 26may2002 starting on 9160 Wireless Gateway , port 80
Jul 27 14:43:59	info	dropbear[254]	Not forking

This page gives you the option of enabling a remote server to capture all system events and errors in a Kernel Log.

This page also lists the most recent, high-level events generated by this access point.

The Events Log shows stations associating, being authenticated, and other occurrences.

This page lists the most recent events generated by this access point (see “Events Log” on page 124).

This page also gives you the option of enabling a remote “log relay host” to capture all system events and errors in a Kernel Log. (This requires setting up a remote relay host first. See “Log Relay Host For Kernel Messages” on page 121).

Note: *The 9160 G2 Wireless Gateway acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as Greenwich Mean Time). You need to convert the reported time to your local time.*

For information on setting the network time protocol, see Chapter 23: “Network Time Protocol Server”.

11.2.1 Log Relay Host For Kernel Messages

- “Understanding Remote Logging” on page 121.
- “Setting Up The Log Relay Host” on page 122.
- “Enabling Or Disabling The Log Relay Host On The Status, Events Page” on page 123.

11.2.1.1 Understanding Remote Logging

The Kernel Log is a comprehensive list of system events (shown in the System Log) and kernel messages, such as error conditions like dropping frames.

You cannot view Kernel Log messages directly from the Administration Web UI for an access point. You must first set up a remote server running a syslog process and acting as a syslog “log relay host” on your network. Then, you can configure the 9160 G2 Wireless Gateway to send its syslog messages to the remote server.

Using a remote server to collect access point syslog messages affords you several benefits. You can:

- Aggregate syslog messages from multiple access points.
- Store a longer history of messages than kept on a single access point.
- Trigger scripted management operations and alerts.

11.2.1.2 Setting Up The Log Relay Host

To use Kernel Log relaying, you must configure a remote server to receive the syslog messages. This procedure will vary depending on the type of machine you use as the remote log host. The following is an example of how to configure a remote Linux server using the syslog daemon.

Example Of Using Linux syslogd

The following steps activate the syslog daemon on a Linux server. Make sure you have root user identity for these tasks.

1. Log on as `root` to the machine you want to use as your syslog relay host.

   The following operations require `root` user permissions. If you are not already logged on as root, type `su` at the command line prompt to become `root` ("super user").

2. Edit `/etc/init.d/sysklogd` and add " `-r` " to the variable `SYSLOGD` near the top of the file. The line you edit will look like this:

   ```
   SYSLOGD= "-r"
   ```

   Consult the man pages to get more information on syslogd command options. (Type man `syslogd` at the command line.)

3. If you want to send all the messages to a file, edit `/etc/syslog.conf`.

   For example you can add this line to send all messages to a log file called "`AP_syslog`":

   ```
   * . *       -/tmp/AP_syslog
   ```

   Consult the man pages to get more information on syslog.conf command options. (Type man `syslog.conf` at the command line.)

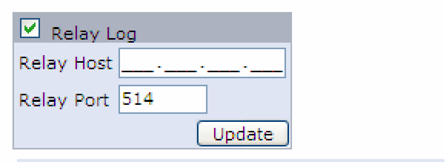
4. Restart the syslog server by typing the following at the command line prompt:

   ```
   /etc/init.d/sysklogd restart
   ```

Note: *The syslog process will default to use port **514**. We recommend keeping this default port. However; If you choose to reconfigure the log port, make sure that the port number you assign to syslog is not being used by another process.*

11.2.1.3 Enabling Or Disabling The Log Relay Host On The Status, Events Page

To enable and configure Log Relaying on the *Status* > *Events* page, set the *Log Relay* options as described below and then click **Update**.


☑ Relay Log
Relay Host ___.___.___.___
Relay Port 514

Field	Description
Relay Log	Choose to either enable or disable use of the Log Relay Host: If you select the **Relay Log** checkbox, the Log Relay Host is enabled and the *Relay Host* and *Relay Port* fields are editable.
Relay Host	Specify the ***IP Address*** or ***DNS*** name of the Relay Host. ***Note:*** *If you are using Devicescape Wireless Operations Center, the Repository Server should receive the syslog messages from all access points. In this case, use the IP address of the Operations Center Repository Server as the Relay Host.*
Relay Port	Specify the Port number for the syslog process on the Relay Host. The default port is **514**.

Table 11.1 Log Relay Host Settings

Update Settings

To apply your changes, click **Update**.

If you *enabled* the Log Relay Host, clicking **Update** will activate remote logging. The access point will send its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

If you *disabled* the Log Relay Host, clicking **Update** will disable remote logging.

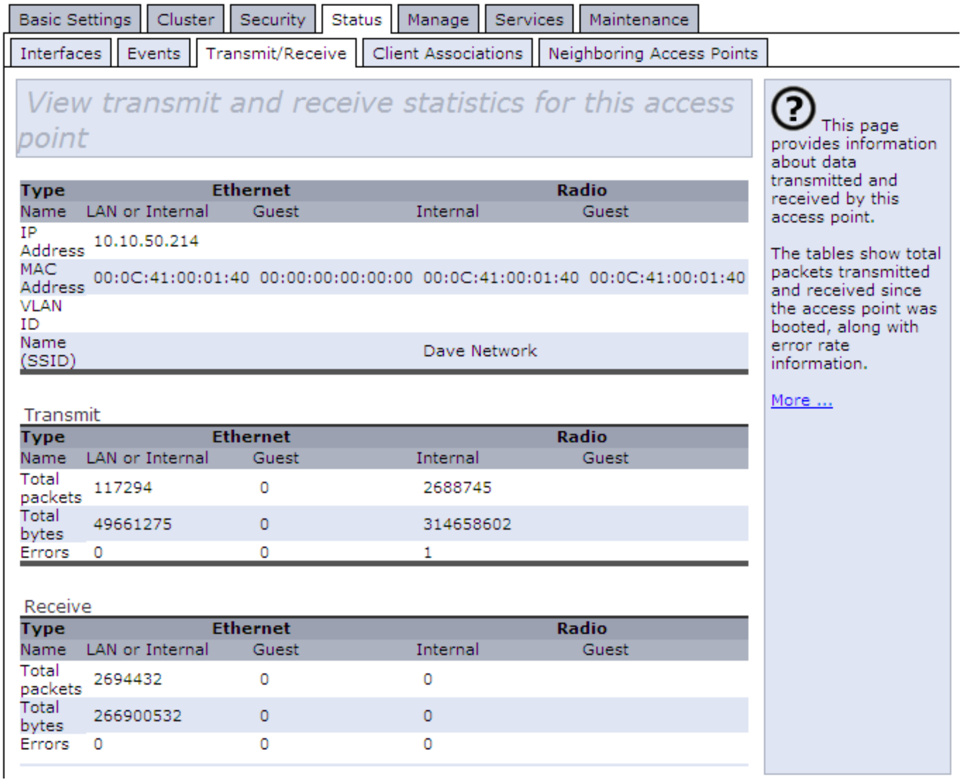
11.2.2 Events Log

The Events Log shows system events on the access point such as stations associating, being authenticated, and other occurrences. The real-time Events Log is always shown on the *Status*, *Events* Administration Web UI page for the access point you are monitoring.

11.3 Transmit/Receive Statistics

To view transmit/receive statistics for a particular access point, navigate to *Status > Transmit/Receive* on the Administration Web pages for the access point you want to monitor.

Note: *The following figure shows the* Transmit/Receive *page for a two-radio AP. The Administration Web page for the one-radio AP will look slightly different.*



View transmit and receive statistics for this access point

Type	Ethernet		Radio	
Name	LAN or Internal	Guest	Internal	Guest
IP Address	10.10.50.214			
MAC Address	00:0C:41:00:01:40	00:00:00:00:00:00	00:0C:41:00:01:40	00:0C:41:00:01:40
VLAN ID				
Name (SSID)			Dave Network	

Transmit

Type	Ethernet		Radio	
Name	LAN or Internal	Guest	Internal	Guest
Total packets	117294	0	2688745	
Total bytes	49661275	0	314658602	
Errors	0	0	1	

Receive

Type	Ethernet		Radio	
Name	LAN or Internal	Guest	Internal	Guest
Total packets	2694432	0	0	
Total bytes	266900532	0	0	
Errors	0	0	0	

This page provides information about data transmitted and received by this access point.

The tables show total packets transmitted and received since the access point was booted, along with error rate information.

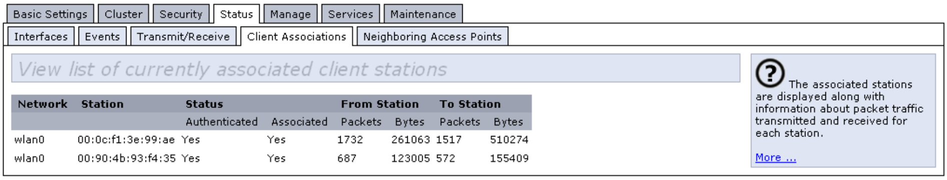
This page provides some basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in Table 11.2 on page 125. All transmit and receive statistics shown are totals since the access point was last started. If the AP is rebooted, these figures indicate transmit/receive totals since the re-boot.

Field	Description
IP Address	***IP Address*** for the access point.
MAC Address	Media Access Control (***MAC***) address for the specified interface. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. The 9160 G2 Wireless Gateway has a unique MAC address for each interface. A two-radio access point has a different MAC address for each interface on each of its two radios.
VLAN ID	Virtual ***LAN*** (***VLAN***) ID. A VLAN is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. VLANs can be used to establish internal and guest networks on the same access point.
Name (SSID)	Wireless network name. Also known as the ***SSID***, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the Basic Settings tab. (See “Provide Network Settings” on page 49.)
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this access point.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this access point.
Errors	Indicates total errors related to sending and receiving data on this access point.

Table 11.2 Transmit/Receive Statistics

11.4 Associated Wireless Clients

To view the client stations associated with a particular access point, navigate to *Status* > *Client Associations* on the Administration Web pages for the access point you want to monitor.



View list of currently associated client stations

Network	Station	Status		From Station		To Station	
		Authenticated	Associated	Packets	Bytes	Packets	Bytes
wlan0	00:0c:f1:3e:99:ae	Yes	Yes	1732	261063	1517	510274
wlan0	00:90:4b:93:f4:35	Yes	Yes	687	123005	572	155409

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

More ...

The associated stations are displayed, along with information about packet traffic transmitted and received for each station.

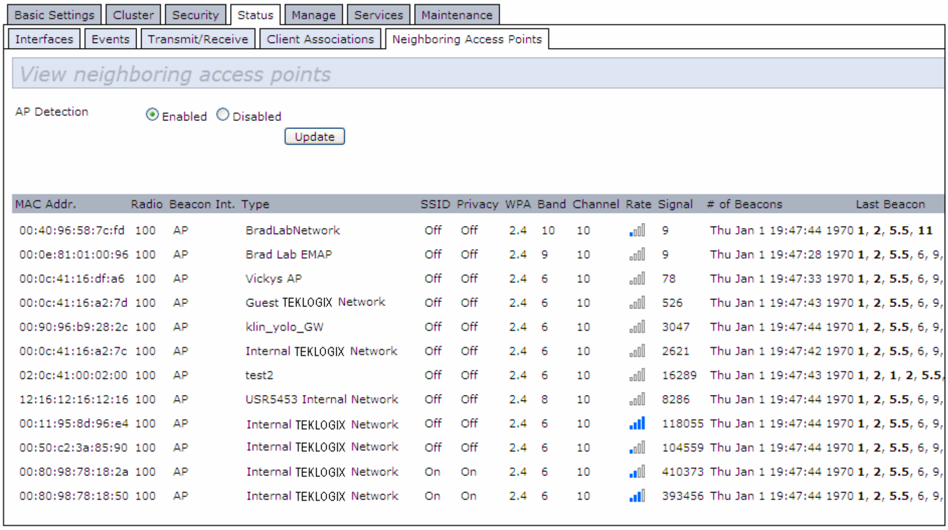
11.4.1 Link Integrity Monitoring

The 9160 G2 Wireless Gateway provides *link integrity monitoring* to continually verify its connection to each associated client (even when there is no data exchange occurring). To do this, the AP sends data packets to clients every few seconds when no other traffic is passing. This allows the access point to detect when a client goes out of range, even during periods when no normal traffic is exchanged.The client connection drops off the list of associated clients within 300 seconds of a client disappearing, even if they do not disassociate (but went out of range).

11.5 Neighboring Access Points

The status page for “neighboring access points” provides real-time statistics for all access points within range of the access point on which you are viewing the Administration Web pages.

To view information about other access points on the wireless network, navigate to *Status* > *Neighboring Access Points*.



View neighboring access points

AP Detection ● Enabled ○ Disabled

MAC Addr.	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	# of Beacons	Last Beacon
00:40:96:58:7c:fd	100	AP	BradLabNetwork	Off	Off	2.4	10	10	▂▄▆█	9	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, **11**
00:0e:81:01:00:96	100	AP	Brad Lab EMAP	Off	Off	2.4	9	10	▂▄▆█	9	Thu Jan 1 19:47:28 1970	**1**, **2**, **5.5**, 6, 9,
00:0c:41:16:df:a6	100	AP	Vickys AP	Off	Off	2.4	6	10	▂▄▆█	78	Thu Jan 1 19:47:33 1970	**1**, **2**, **5.5**, 6, 9,
00:0c:41:16:a2:7d	100	AP	Guest TEKLOGIX Network	Off	Off	2.4	6	10	▂▄▆█	526	Thu Jan 1 19:47:43 1970	**1**, **2**, **5.5**, 6, 9,
00:90:96:b9:28:2c	100	AP	klin_yolo_GW	Off	Off	2.4	6	10	▂▄▆█	3047	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, 6, 9,
00:0c:41:16:a2:7c	100	AP	Internal TEKLOGIX Network	Off	Off	2.4	6	10	▂▄▆█	2621	Thu Jan 1 19:47:42 1970	**1**, **2**, **5.5**, 6, 9,
02:0c:41:00:02:00	100	AP	test2	Off	Off	2.4	6	10	▂▄▆█	16289	Thu Jan 1 19:47:43 1970	**1**, **2**, **1**, **2**, **5.5**,
12:16:12:16:12:16	100	AP	USR5453 Internal Network	Off	Off	2.4	8	10	▂▄▆█	8286	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, 6, 9,
00:11:95:8d:96:e4	100	AP	Internal TEKLOGIX Network	Off	Off	2.4	6	10	▂▄▆█	118055	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, 6, 9,
00:50:c2:3a:85:90	100	AP	Internal TEKLOGIX Network	Off	Off	2.4	6	10	▂▄▆█	104559	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, 6, 9,
00:80:98:78:18:2a	100	AP	Internal TEKLOGIX Network	On	On	2.4	6	10	▂▄▆█	410373	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, 6, 9,
00:80:98:78:18:50	100	AP	Internal TEKLOGIX Network	On	On	2.4	6	10	▂▄▆█	393456	Thu Jan 1 19:47:44 1970	**1**, **2**, **5.5**, 6, 9,

Information provided on neighboring access points is described in Table 11.3.

Field	Description
MAC Address	Shows the ***MAC*** address of the neighboring access point. A ***MAC*** address is a hardware address that uniquely identifies each node of a network.
Radio	**Two-Radio APs** If the access point that is “doing the detecting” of neighboring APs is a two-radio access point, the Radio field is included. The Radio field indicates which radio the neighboring AP was detected on: • wlan0 (Radio One) • wlan1 (Radio Two) **One-Radio APs** This field is not included on the *Neighboring Access Points* pages of one-radio access points.

Table 11.3 Neighboring Access Point Statistics

Field	Description
Beacon Interval	Shows the ***Beacon*** interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every **100** milliseconds (or 10 per second). The Beacon Interval is set on the *Manage* > *Radio* tab page. (See Chapter 16: “Configuring 802.11 Radio Settings”.)
Type	Indicates the type of device: • **AP** indicates the neighboring device is an access point that supports the IEEE 802.11 ***Wireless Networking Framework*** in ***Infrastructure Mode***. • **Ad hoc** indicates a neighboring station running in ***Ad hoc Mode***. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional access point. Ad-hoc mode is an IEEE 802.11 ***Wireless Networking Framework*** also referred to as “*peer-to-peer*” mode or an *Independent Basic Service Set* (***IBSS***).
SSID	The *Service Set Identifier* (***SSID***) for the access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the “Network Name”. The SSID is set in Basic Settings. (See Chapter 5: “Configuring Basic Settings”) or in *Manage* > *Wireless Settings* (see Chapter 13: “Setting the Wireless Interface”.) A Guest network and an Internal network running on the same access point must always have two different network names.
Privacy	Indicates whether there is any security on the neighboring device. • **Off** indicates that the Security mode on the neighboring device is set to “None” mode (no security). • **On** indicates that the neighboring device has some security in place. Security is configured on the AP from the *Security* tab page. For more information on security settings, see Chapter 10: “Configuring Security”.
WPA	Indicates whether ***WPA*** security is **On** or **Off**” or this access point.

Table 11.3 Neighboring Access Point Statistics

Field	Description
Band	This indicates the IEEE 802.11 mode being used on this access point. (For example, ***IEEE 802.11a***, IEEE ***802.11b***, IEEE ***802.11g***.) The number shown indicates the mode according to the following map: • **2.4** indicates IEEE 802.11b mode or IEEE 802.11g mode. • **5** indicates IEEE 802.11a mode.
Channel	Shows the channel on which the access point is currently broadcasting. The ***Channel*** defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The channel is set in *Radio Settings*. (See Chapter 16: “Configuring 802.11 Radio Settings”.)
Rate	Shows the rate (in megabits per second) at which this access point is currently transmitting. The current rate will always be one of the supported rates shown in *Rates*.
Signal	Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).
# of Beacons	Shows the total number of beacons transmitted by this access point since it was last booted.
Last Beacon	Shows the date and time that the most recent beacon was transmitted from the access point.
Rates	Shows supported and basic (advertised) rate sets for the neighboring access point. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on *Radio Settings*. (See Chapter 16: “Configuring 802.11 Radio Settings”.) The rates shown for an access point will always be the rates currently specified for that AP in its *Radio Settings*.

Table 11.3 Neighboring Access Point Statistics

THE ETHERNET (WIRED) INTERFACE 12

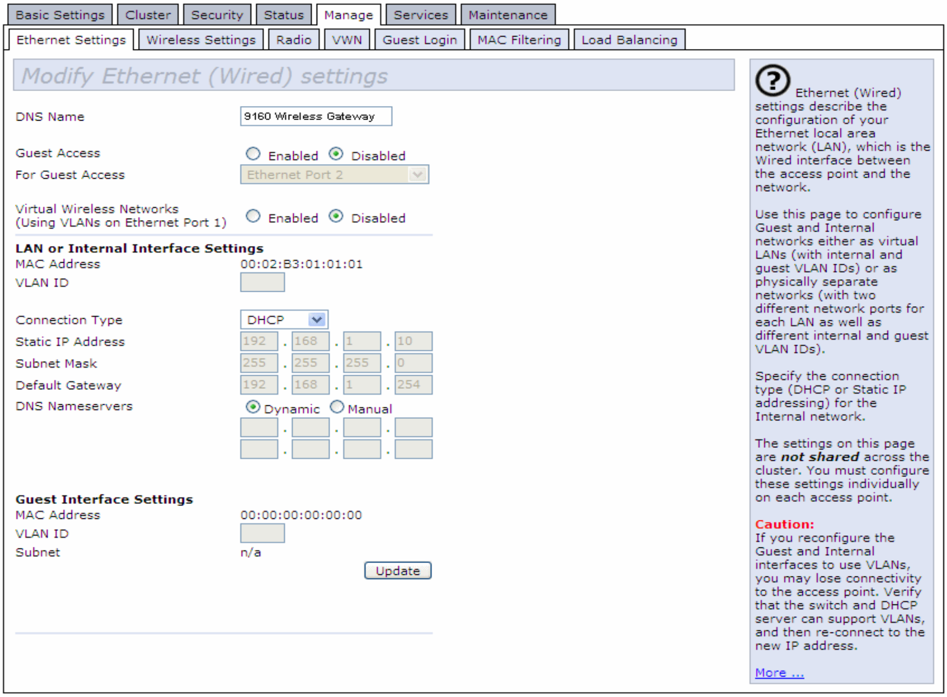
Ethernet (Wired) Settings describe the configuration of your ***Ethernet*** local area network (***LAN***).

Note: *The Ethernet Settings are not shared across the cluster. These settings must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its **IP Address** link on the* Cluster > Access Points *page of the current AP. For more information about which settings are shared by the cluster and which are not, see “Which Settings Are Shared As Part Of The Cluster Configuration And Which Are Not?” on page 57.*

The following sections describe how to configure “Wired” address and related settings on the 9160 G2 Wireless Gateway:

12.1 Navigating To Ethernet (Wired) Settings

To set the wired address for an access point, navigate to the *Manage > Ethernet Settings* tab, and update the fields as described below.



Modify Ethernet (Wired) settings

DNS Name: 9160 Wireless Gateway

Guest Access: ○ Enabled ● Disabled
For Guest Access: Ethernet Port 2

Virtual Wireless Networks (Using VLANs on Ethernet Port 1): ○ Enabled ● Disabled

LAN or Internal Interface Settings
MAC Address: 00:02:B3:01:01:01
VLAN ID:

Connection Type: DHCP
Static IP Address: 192 . 168 . 1 . 10
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 192 . 168 . 1 . 254
DNS Nameservers: ● Dynamic ○ Manual

Guest Interface Settings
MAC Address: 00:00:00:00:00:00
VLAN ID:
Subnet: n/a

Ethernet (Wired) settings describe the configuration of your Ethernet local area network (LAN), which is the Wired interface between the access point and the network.

Use this page to configure Guest and Internal networks either as virtual LANs (with internal and guest VLAN IDs) or as physically separate networks (with two different network ports for each LAN as well as different internal and guest VLAN IDs).

Specify the connection type (DHCP or Static IP addressing) for the Internal network.

The settings on this page are ***not shared*** across the cluster. You must configure these settings individually on each access point.

Caution:
If you reconfigure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. Verify that the switch and DHCP server can support VLANs, and then re-connect to the new IP address.

12.1.1 Setting The DNS Name

Field	Description
DNS Name	Enter the DNS name for the access point in the text box. This is the host name. It may be provided by your ISP or network administrator, or you can provide your own. The rules for system names are: • This name can be up to 20 characters long. • Only letters, numbers and dashes are allowed. • The name must start with a letter and end with either a letter or a number.

Table 12.1 Setting DNS Name

12.1.2 Enabling Or Disabling Guest Access

You can provide controlled guest access over an isolated network and a secure internal ***LAN*** on the same 9160 G2 Wireless Gateway.

12.1.2.1 Configuring An Internal LAN And A Guest Network

A *Local Area Network* (***LAN***) is a communications network covering a limited area, for example, one floor of a building. A LAN connects multiple computers and other network devices like storage and printers.

Ethernet is the most common technology implementing a LAN. ***Wi-Fi*** (***IEEE***) is another very popular LAN technology.

The 9160 G2 Wireless Gateway allows you to configure two different LANs on the same access point: one for a secure *internal* LAN and another for a public *guest* network with no security and little or no access to internal resources. To configure these networks, you need to provide both Wireless and Ethernet (Wired) settings.

Information on how to configure the Ethernet (Wired) settings is provided in the sections below.

(For information on how to configure the Wireless settings, see Chapter 13: “Setting the Wireless Interface”. For an overview of how to set up the Guest interface, see Chapter 14: “Setting up Guest Access”.)

12.1.2.2 Enabling Or Disabling Guest Access

The 9160 G2 Wireless Gateway ships with the Guest Access feature **disabled** by default. If you want to provide guest access on your AP, enable Guest access on the *Ethernet (Wired) Settings* tab.

Field	Description
Guest Access	By default, the 9160 G2 Wireless Gateway ships with Guest Access **disabled**. • To enable Guest Access, click **Enabled**. • To disable Guest Access, click **Disabled**.

Table 12.2 Enabling/Disabling Guest Access

12.1.2.3 Specifying A Virtual Guest Network

If you enable Guest Access, you must create both an “Internal” and “Guest Network” on this access point *virtually*, by connecting the LAN port on the access point to a tagged port on a ***VLAN*** capable switch, and then defining two different Virtual LANs on this Administration page. (For more information, see Chapter 14: “Setting up Guest Access”.) Create the virtually separate internal and guest LANs as described in Table 12.3.

Field	Description
Guest Access	• Select **Enabled** to enable Guest Access. (If you choose this option, you must select VLANs on the next setting, *For Guest access use,* and then provide details on VLAN for the Guest Network on the rest of the page.) • Select **Disabled** to disable Guest Access.
For Guest Access	Specify a *virtually* separate guest network on this access point: • Since the access point is using only one physical connection to your internal LAN, choose **VLAN on Ethernet Port 1** from the drop-down menu. This will enable the “VLAN” settings where you must provide a VLAN ID. See “Configuring Guest Interface Ethernet (Wired) Settings” on page 138. ***Important: If you reconfigure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring the VLAN on the*** Manage > Ethernet Settings ***page, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, reconnect via the Administration Web pages to the new IP address.*** ***(If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)***

Table 12.3 Specifying A Virtual Guest Network

12.1.3 Enabling / Disabling Virtual Wireless Networks On The AP

If you want to configure the Internal network as a VLAN (whether or not you have a Guest network configured), you can enable “Virtual Wireless Networks” on the access point.

You must enable this feature if you want to configure additional virtual networks on VLANs on the *Advanced* > *Virtual Wireless Networks* tab as described in “Configuring VLANs” on page 157.

Field	Description
Virtual Wireless Networks (Using VLANs on Ethernet Port 1)	• Select **Enabled** to enable VLANs for the Internal network and for additional networks. (If you choose this option, you can run the Internal network on a VLAN whether or not you have Guest Access configured and you can set up additional networks on VLANs using the *Advanced > Virtual Wireless Networks* tab as described in “Configuring VLANs” on page 157.) • Select **Disabled** to disable the VLAN for the Internal network, and for any additional virtual networks on this access point.

12.1.4 Configuring LAN Or Internal Interface Ethernet Settings

To configure Ethernet (wired) settings for the Internal LAN, fill in the fields as described in Table 12.4.

Field	Description
MAC Address	Shows the ***MAC*** address for the Internal interface for the Ethernet port on this access point. This is a read-only field that you cannot change.
VLAN ID	If you choose to configure Internal and Guest networks by “VLANs”, this field will be **enabled**. Provide a number between 1 and 4094 for the Internal VLAN. This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support ***VLAN*** IEEE ***802.1p*** frames. The access point must be able to reach the DHCP server. Check with the Administrator regarding the VLAN and DHCP configurations.

Table 12.4 Ethernet Settings For Internal LAN

Field	Description
Connection Type	You can select **DHCP** or **Static IP**. The *Dynamic Host Configuration Protocol* (***DHCP***) is a protocol specifying how a centralized server can provide network configuration information to devices on the network. A DHCP server "offers" a "lease" to the client system. The information supplied includes the IP addresses and netmask, plus the address of its DNS servers and gateway. *Static IP* indicates that all network settings are provided manually. You must provide the IP address for the 9160 G2 Wireless Gateway, its subnet mask, the IP address of the default gateway, and the IP address of at least one DNS nameserver. If you select **DHCP**, the 9160 G2 Wireless Gateway will acquire its IP Address, subnet mask, and DNS and gateway information from the DHCP Servers. Otherwise, if you select **Static IP**, fill in the items described in *Static IP Settings*. ***Important: If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the AP is change the Connection Type from DHCP to Static IP. When you change the Connection Type to Static IP, you can either assign a new Static IP Address to the AP or continue using the default address. We recommend assigning a new address so that if later you bring up another 9160 G2 Wireless Gateway on the same network, the IP addresses for the two APs will be unique.*** If you need to recover the default Static IP address, you can do so by resetting the AP to the factory defaults as described in "Resetting Factory Default Configuration" on page 253.
Static IP Address	If you chose **Static IP** as the Connection Type, these fields will be enabled. Enter the Static IP Address in the text boxes.
Subnet Mask	Enter the **Subnet Mask** in the text boxes. You must obtain this information from your ISP or network administrator.

Table 12.4 Ethernet Settings For Internal LAN

Field	Description
Default Gateway	Enter the **Default Gateway** in the text boxes.
DNS Nameservers	The *Domain Name Service* (***DNS***) is a system that resolves the descriptive name (*domainname*) of a network resource (for example, *www.psionteklogix.com*) to its numeric IP address (for example, `66.93.138.219`). A DNS server is called a *Nameserver*. There are usually two Nameservers; a Primary Nameserver and a Secondary Nameserver. You can choose *Dynamic* or *Manual* mode. • If you choose **Dynamic**, the IP addresses for the DNS servers will be assigned automatically via DHCP. (This option is only available if you specified DHCP for the Connection Type.) • If you choose **Manual**, you should assign static IP addresses manually.

Table 12.4 Ethernet Settings For Internal LAN

12.1.5 Configuring Guest Interface Ethernet (Wired) Settings

To configure Ethernet (Wired) Settings for the “Guest” interface, fill in the fields as described below.

Field	Description
MAC Address	Shows the ***MAC*** address for the Guest interface for the Ethernet port on this access point. This is a read-only field that you cannot change.
VLAN ID	If you choose to configure Internal and Guest networks by “VLANs”, this field will be **enabled**. Provide a number between 1 and 4094 for the Guest VLAN.
Subnet	Shows the subnetwork address for the Guest interface. For example, `192.168.1.0`.

Table 12.5 Configuring Guest Interface Ethernet Settings

12.1.6 Updating Settings

To update Ethernet settings:

1. Navigate to the *Ethernet Settings* page.
2. Configure the ethernet settings as required.
3. Click the **Update** button to apply the changes.

SETTING THE WIRELESS INTERFACE 13

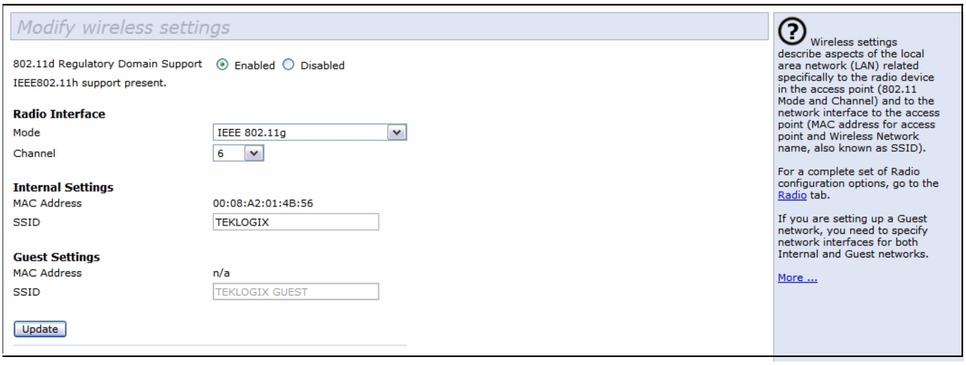
Wireless Settings describes aspects of the local area network (***LAN***) related specifically to the radio device in the access point (***802.11*** Mode and ***Channel***) and to the network interface to the access point (***MAC*** address for access point and Wireless Network name, also known as ***SSID***).

The following sections describe how to configure the "Wireless" address and related settings on the 9160 G2 Wireless Gateway.

13.1 Navigating To Wireless Settings

To set the wireless address for an access point, navigate to the *Manage > 802.11 Basic Settings* tab which will open the *Wireless Settings* page, and update the fields as described below.

Note: *The following figure shows the Wireless Settings page for a two-radio AP. The Administration Web page for the single-radio AP will look slightly different.*



Modify wireless settings

802.11d Regulatory Domain Support ● Enabled ○ Disabled

IEEE802.11h support present.

Radio Interface

Mode: IEEE 802.11g

Channel: 6

Internal Settings

MAC Address: 00:08:A2:01:4B:56

SSID: TEKLOGIX

Guest Settings

MAC Address: n/a

SSID: TEKLOGIX GUEST

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and Wireless Network name, also known as SSID).

For a complete set of Radio configuration options, go to the Radio tab.

If you are setting up a Guest network, you need to specify network interfaces for both Internal and Guest networks.

13.2 Configuring 802.11d Regulatory Domain Support

You can enable or disable IEEE ***802.11d*** Regulatory Domain Support to broadcast the access point country code information as described below.

Field	Description
802.11d Regulatory Domain Support	Enabling support for IEEE 802.11d on the access point causes the AP to broadcast which country it is operating in as a part of its beacons: • To enable 802.11d regulatory domain support, click **Enabled**. • To disable 802.11d regulatory domain support, click **Disabled**.For the two-radio AP, two MAC addresses are shown: one for each Radio on the Internal interface. ***Note:*** *The IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without re-configuration. IEEE 802.11d allows client stations to operate in any country without re-configuration. The Devicescape Reference AP must be configured by the Manufacturer via the command line interface (CLI) country codes for operation in a particular country.*

13.3 802.11h Regulatory Domain Control

Field	Description
IEEE 802.11h	The Administration UI will show whether IEEE 802.11h regulatory domain control is in effect on the AP. IEEE 802.11h cannot be disabled by an end user Administrator. The following details are provided for informational purposes only. IEEE 802.11h is a standard that provides two services required to satisfy certain regulatory domains for the 5GHz band. These two services are Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). • TPC requires that Radio Local Area Networks (RLANs) operating in the 5 GHz band use transmitter power control. This involves adhering to a regulatory maximum transmit output power and a mitigation requirement for each permitted channel. The result of which is the reduced interference with satellite services. • DFS requires that RLANs operating in the 5 GHz band implement a mechanism to avoid co-channel operation with radar systems and ensure uniform utilization of any available channels. ***Note:*** *802.11h is automatically enabled if the AP is configured to work in any country that requires 802.11h as a minimum standard. This standard is currently only required by those countries which fall into the European Telecommunications Standard Institute (ETSI) category. 802.11h is also enabled for Japan.*

There are a number of key points for the AP Developer that should be remembered in relation to the IEEE ***802.11h*** standard:

- 802.11h only works for the 802.11a band. It is not required for 802.11b, nor 802.11g.
- If you are operating in an 802.11h enabled domain, then the channel selection of the BSS will always be "Auto". Even if another channel has been has been configured, this will be ignored and auto-channel selection will occur.
- When 802.11h is enabled, the initial bootup time will increase by a minimum of sixty seconds. This is the minimum time required to scan the selected channel for radar interference.
- Setting up WDS links may be difficult when 802.11h is operational. This is because the operating channels of the two APs on the WDS link may keep changing depending on channel usage and radar interference. WDS will only work if both the APs operate on the same channel. For more information on WDS, see Chapter 20: "Wireless Distribution System".

13.4 Configuring The Radio Interface

The radio interface allows you to set the radio ***Channel*** and ***802.11*** mode as described below.

Note: *On a two-radio AP, you must configure these radio interface settings for both Radio Interface One and Radio Interface Two.*

Field	Description
MAC Addresses (Shown on two-radio AP only)	Indicates the Media Access Control () addresses for the interface. On the two-radio AP only, the ***MAC*** addresses for Radio Interface One (Internal/Guest) and Radio Interface Two (Internal/Guest) are shown. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.

Table 13.1 Radio Interface Settings

Field	Description
Mode	The *Mode* defines the *Physical Layer* (***PHY***) standard being used by the radio. The 9160 G2 Wireless Gateway is available as a single or dual-band access point with one or two radios. The configuration options for Mode differ depending on which product you have. **Single-Band AP:** For the Single-Band AP, select one of these modes: • IEEE ***802.11b*** • IEEE ***802.11g*** **Dual-Band AP:** For the dual-band AP, select one of these modes: a mode for each Radio Interface. • IEEE ***802.11b*** • IEEE ***802.11g*** • ***IEEE 802.11a*** **One or Two-Radio AP:** If you have a two-radio AP, select an IEEE 802.11 mode for each of the two radio interfaces. (For a one-radio AP there is only one radio interface.)
Channel	Select the *Channel*. The range of channels and the default is determined by the *Mode* of the radio interface. The ***Channel*** defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R). The default is **Auto**, which picks the least busy channel at startup time.

Table 13.1 Radio Interface Settings

13.5 Configuring "Internal" Wireless LAN Settings

The Internal Settings describe the ***MAC*** Address (read-only) and Network Name (also known as the ***SSID***) for the internal *Wireless LAN* (WLAN) as described in Table 13.2.

Field	Description
MAC Address	Shows the ***MAC*** address(es) for Internal interface for this access point. This is a read-only field that you cannot change. Although this access is point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple *Basic Service Set Identifiers* (***BSSID***s) for a single access point. The MAC address(es) shown for the "Internal" access point is the BSSID(s) for the "Internal" interface. For the two-radio AP, two MAC addresses are shown: one for each Radio on the Internal interface.
Wireless Network Name (SSID)	Enter the **SSID** for the internal WLAN. The *Service Set Identifier* (***SSID***) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Table 13.2 Wireless LAN Settings

13.6 Configuring "Guest" Network Wireless Settings

The Guest Settings describe the ***MAC*** Address (read-only) and wireless network name (***SSID***) for the *Guest Network* as described in Table 13.3. Configuring an access point with two different network names (SSIDs) allows you to leverage the Guest interface feature on the 9160 G2 Wireless Gateway. For more information, see Chapter 14: "Setting up Guest Access".

Field	Description
MAC Address	Shows the ***MAC*** address for the Guest interface for this access point. This is a read-only field that you cannot change. Although this access is point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple *Basic Service Set Identifiers* (***BSSID***) for a single access point. The MAC address(es) shown for the "Guest" access point is the BSSID(s) for the "Guest" interface. For the two-radio AP, two MAC addresses are shown: one for each Radio on the Guest interface.
Wireless Network Name (SSID)	Enter the **SSID** for the *guest network*. The *Service Set Identifier* (***SSID***) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID. For the guest network, provide an SSID that is different from the internal SSID and easily identifiable as the "guest" network.

Table 13.3 Guest Network Wireless Settings

13.7 Updating Settings

To update wireless settings:

1. Navigate to the *802.11 Basic Settings* page.
2. Configure the wireless settings as required.
3. Click the **Update** button to apply the changes.

SETTING UP GUEST ACCESS 14

Out-of-the-box *Guest Interface* features allow you to configure the 9160 G2 Wireless Gateway for controlled guest access to an isolated network. You can configure the same access point to broadcast and function as two different wireless networks: a secure "Internal" LAN and a public "Guest" network. Guest clients can access the guest network without a username or password. When guests log in, they see a guest *Welcome* screen (also known as a "captive portal").

14.1 Understanding The Guest Interface

You can define unique parameters for *guest* connectivity and isolate guest clients from other more sensitive areas of the network.

Important: ***No security is provided on the guest network; only plain-text security mode is allowed.***

Simultaneously, you can configure a secure *internal* network (using the same access point as your guest interface) that provides full access to protected information behind a firewall and requires secure login or certificates for access.

You can configure an 9160 G2 Wireless Gateway for the Guest interface by using a single network with VLANs by setting up the guest interface configuration options on the Administration Web pages for the 9160 G2 Wireless Gateway. (For details on how to set up this type of guest interface, see "Configuring A Guest Network On A Virtual LAN" on page 150.

Notes: *This method leverages multiple* ***BSSID*** *and Virtual LAN (****VLAN****) technologies that are built-in to the 9160 G2 Wireless Gateway. The Internal and Guest networks are implemented as multiple BSSIDs on the same access point, each with different network names (****SSID****s) on the Wireless interface and different VLAN IDs on the Wired interface.*

On a two-radio access point, the Guest Management and Login settings apply to both Radio One and Radio Two.

14.2 Configuring The Guest Interface

To configure the Guest interface on the 9160 G2 Wireless Gateway, perform these steps:

1. Configure the access point to represent two *virtually* separate networks as described in the section below, “Configuring A Guest Network On A Virtual LAN”.

2. Set up the guest *Welcome* screen for the guest captive portal as described in the section, “Configuring The Welcome Screen (Captive Portal)” on page 152.

Note: *Guest Interface settings are not shared among access points across the cluster. These settings must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its* **IP Address** *link on the* Cluster, Access Points *page of the current AP. For more information about which settings are shared by the cluster and which are not, see “Which Settings Are Shared As Part Of The Cluster Configuration And Which Are Not?” on page 57.*

14.2.1 Configuring A Guest Network On A Virtual LAN

Notes: *If you want to configure the Guest and Internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs.*

As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

Guest Welcome Screen settings are shared among access points across the cluster. When you update these settings for one access point, the configuration will be shared with the other access points in the cluster. For more information about which settings are shared by the cluster and which are not, see “Which Settings Are Shared As Part Of The Cluster Configuration And Which Are Not?” on page 57.

To configure Internal and Guest networks on Virtual LANs, do the following:

1. Use only one wired connection from the network port on the access point to the LAN. (Make sure this port is configured to handle VLAN tagged packets.)

2. Configure Ethernet (wired) Settings for Internal and Guest networks on VLANs as described in the sections in Chapter 12: "The Ethernet (Wired) Interface".

   (Start by enabling Guest Access and choosing "For Internal and Guest access, use two: **VLANs**" as described in "Specifying A Virtual Guest Network" on page 135.)

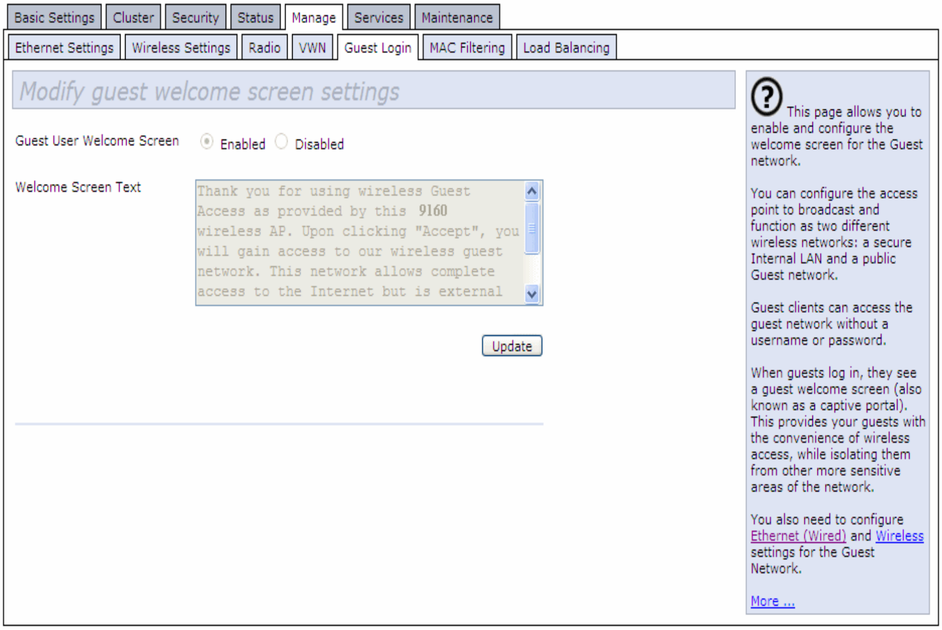
3. Provide the radio interface settings and network names (SSIDs) for both Internal and Guest networks as described in Chapter 13: "Setting the Wireless Interface".

4. Configure the guest splash screen as described in "Configuring The Welcome Screen (Captive Portal)" on page 152.

14.2.2 Configuring The Welcome Screen (Captive Portal)

You can set up or modify the Welcome screen guest clients see when they open a Web browser or try to browse the Web. To set up the captive portal, do the following:

1. Navigate to the *Manage* > *Guest Login* tab.



Modify guest welcome screen settings

Guest User Welcome Screen ● Enabled ○ Disabled

Welcome Screen Text

```
Thank you for using wireless Guest
Access as provided by this  9160
wireless AP. Upon clicking "Accept", you
will gain access to our wireless guest
network. This network allows complete
access to the Internet but is external
```

This page allows you to enable and configure the welcome screen for the Guest network.

You can configure the access point to broadcast and function as two different wireless networks: a secure Internal LAN and a public Guest network.

Guest clients can access the guest network without a username or password.

When guests log in, they see a guest welcome screen (also known as a captive portal). This provides your guests with the convenience of wireless access, while isolating them from other more sensitive areas of the network.

You also need to configure Ethernet (Wired) and Wireless settings for the Guest Network.

More ...

2. Choose **Enabled** to activate the Welcome screen.
3. In the *Welcome Screen Text* field, type the text message you would like guest clients to see on the captive portal.
4. Click **Update** to apply the changes.

14.3 Using The Guest Network As A Client

Once the guest network is configured, a client can access the guest network as follows:

1. A guest client enters an area of coverage and scans for wireless networks.
2. The guest network advertises itself via a Guest SSID or some similar name, depending on how the guest SSID is specified in the Administration Web pages for the Guest interface.

3. The guest client chooses Guest SSID.
4. The guest client starts a Web browser and receives a Guest Welcome screen.
5. The Guest Welcome Screen provides a button for the client to click to continue.
6. The guest client is now enabled to use the “guest” network.

14.4 Deployment Example

In Figure 14.1, the dotted lines indicate dedicated guest connections.
All access points and all connections (including guests) are administered from the same 9160 G2 Wireless Gateway Administration Web pages.

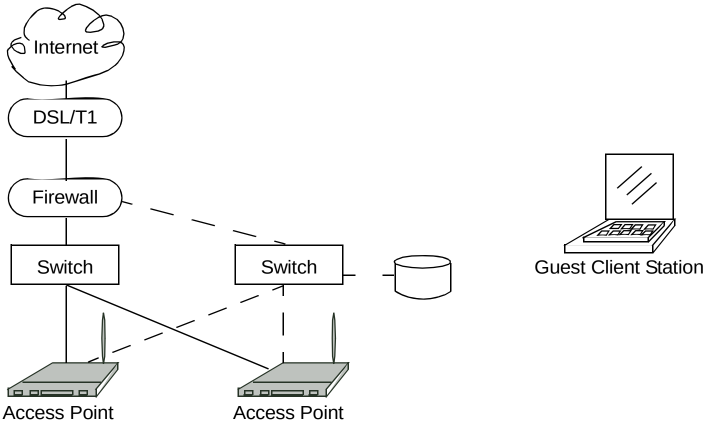


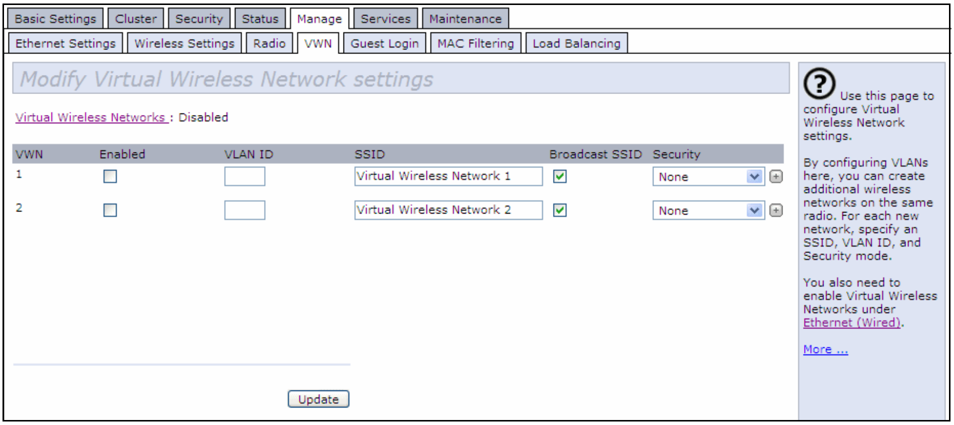
Figure 14.1 Dedicated Guest Connections

CONFIGURING VLANS 15

The following sections describe how to configure multiple wireless networks on Virtual LANs (***VLAN***s).

15.1 Navigating To Virtual Wireless Network Settings

To set up multiple networks on VLANs, navigate to the *Manage > Virtual Wireless Networks* tab, and update the fields as described below.



Modify Virtual Wireless Network settings

Virtual Wireless Networks : Disabled

VWN	Enabled	VLAN ID	SSID	Broadcast SSID	Security
1	□		Virtual Wireless Network 1	☑	None
2	□		Virtual Wireless Network 2	☑	None

Use this page to configure Virtual Wireless Network settings.

By configuring VLANs here, you can create additional wireless networks on the same radio. For each new network, specify an SSID, VLAN ID, and Security mode.

You also need to enable Virtual Wireless Networks under Ethernet (Wired).

15.2 Configuring VLANs

Note: *To configure additional networks on VLANs, you must first enable Virtual Wireless Networks on the Ethernet* Settings *page. See “Enabling / Disabling Virtual Wireless Networks On The AP” on page 136.*

Important: ***If you configure VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring VLANs, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, re-connect via the Administration Web pages to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)***

Field	Description
Virtual Wireless Network	You can configure up to 6 VWNs.
Enabled	You can enable or disable a configured network. • To enable the specified network, **check** the *Enabled* checkbox beside the appropriate VWN. • To disable the specified network, **uncheck** the *Enabled* checkbox beside the appropriate VWN. If you disable the specified network, you will lose the VLAN ID you entered.
VLAN ID	Provide a number between 1 and 4094 for the Internal VLAN. This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server. Check with the Administrator regarding the VLAN and DHCP configurations.
SSID	Enter a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this SSID. The Service Set Identifier (SSID) is an alphanumeric string of up to 32 characters. ***Note:*** *If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.*
Broadcast SSID	Select the *Broadcast SSID* setting by selecting the **Broadcast SSID** checkbox. By default, the access point broadcasts (allows) the *Service Set Identifier* (SSID) in its beacon frames. You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP's broadcast SSID is suppressed, the network name will not be displayed in the *List of Available Networks* on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect. ***Note:*** *The Broadcast SSID you set here is specifically for this Virtual Network (**One** or **Two**). Other networks continue to use the security modes already configured:* • Your original Internal network (configured on the Ethernet *Settings page*) uses the Broadcast SSID set on *Security*. • If a Guest network is configured, the Broadcast SSID is always allowed.

Table 15.1 Virtual Wireless Network Settings

Field	Description
Security Mode	Select the *Security Mode* for this VLAN. Select one of the following: • ***None (Plain-text)*** • ***Static WEP*** • ***WPA Personal*** **Note:** *The Security mode you set here is specifically for this Virtual Network. Other networks continue to use the security modes already configured:* • Your original Internal network (configured on the Ethernet *Settings page*) uses the Security mode set on *Security*. • If a Guest network is configured, always set the security mode to “None”.

Table 15.1 Virtual Wireless Network Settings

15.3 Updating Settings

To update VLAN settings:

1. Navigate to the *VLAN* tab page.
2. Configure the VLAN settings as required.
3. Click the **Update** button to apply the changes.

CONFIGURING 802.11 RADIO SETTINGS 16

The following sections describe how to configure 802.11 Radio Settings on the 9160 G2 Wireless Gateway:

16.1 Understanding Radio Settings

Radio settings directly control the behaviour of the radio device in the access point, and its interaction with the physical medium; that is, how/what type of electromagnetic waves the AP emits. You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between AP beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

The 9160 G2 Wireless Gateway comes configured as a dual-band access point with one radio.

The access point is capable of broadcasting in the following modes:

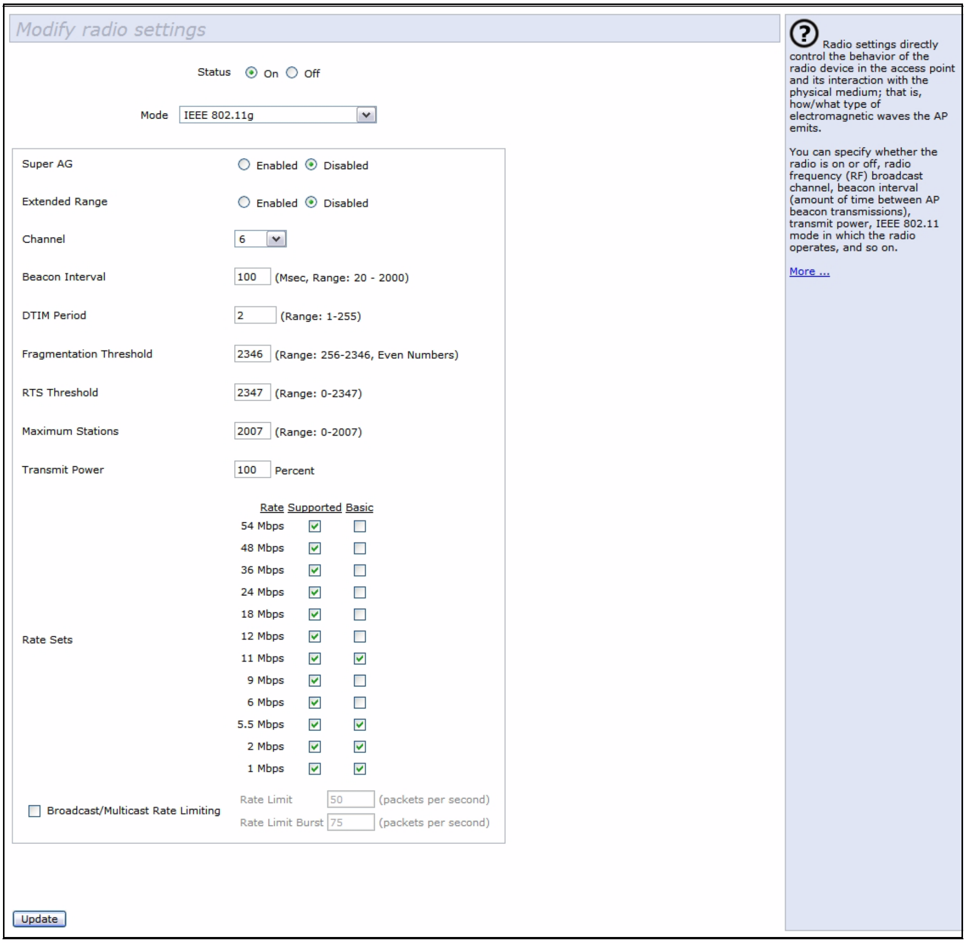
- IEEE ***802.11b*** mode.
- IEEE ***802.11g*** mode.
- IEEE ***802.11a*** mode.
- Atheros Turbo 5 GHz.
- Atheros Dynamic Turbo 5 GHz.
- Atheros Turbo 2.4 GHz.
- Atheros Dynamic Turbo 2.4 GHz.
- Extended Range.

Important: ***Psion Teklogix terminals do not support Atheros Turbo modes and to prevent unnecessary radio overhead the use of Turbo mode is not recommended.***

The IEEE mode, along with other radio settings, are configured as described in “Navigating To Radio Settings” on page 164 and “Configuring Radio Settings” on page 165.

16.2 Navigating To Radio Settings

To specify radio settings, navigate to *Manage > 802.11 Advanced Settings* tab, which will open the *Radio Settings* page, and update the fields as described in Table 16.1 on page 165.



Modify radio settings

Status ● On ○ Off

Mode IEEE 802.11g

Super AG ○ Enabled ● Disabled

Extended Range ○ Enabled ● Disabled

Channel 6

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, Even Numbers)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 2007 (Range: 0-2007)

Transmit Power 100 Percent

Rate Sets

Rate	Supported	Basic
54 Mbps	☑	□
48 Mbps	☑	□
36 Mbps	☑	□
24 Mbps	☑	□
18 Mbps	☑	□
12 Mbps	☑	□
11 Mbps	☑	☑
9 Mbps	☑	□
6 Mbps	☑	□
5.5 Mbps	☑	☑
2 Mbps	☑	☑
1 Mbps	☑	☑

□ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

Radio settings directly control the behavior of the radio device in the access point and its interaction with the physical medium; that is, how/what type of electromagnetic waves the AP emits.

You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between AP beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

16.3 Configuring Radio Settings

Field	Description
Radio	The 9160 G2 Wireless Gateway is available as a one-radio or two-radio access point. **One-Radio AP:** If you have a one-radio version of the 9160 G2 Wireless Gateway, this field is not included on the Radio tab. **Two-Radio AP:** If you have a two-radio version of the 9160 G2 Wireless Gateway, specify **Radio One** or **Radio Two**. On a two-radio AP, the rest of the settings on this tab apply to the radio selected in this field. Be sure to configure settings for both radios.
Status (On/Off)	Specify whether you want the radio on or off by clicking **On** or **Off**.
Mode	The *Mode* defines the *Physical Layer* (***PHY***) standard being used by the radio. The 9160 G2 Wireless Gateway is available as a single or dual-band access point. **Single-Band AP:** For the Single-Band access point, select one of these modes: • ***IEEE 802.11b*** • IEEE ***802.11g*** **Dual-Band AP:** For the Dual-Band access point, select one of these modes. • ***IEEE 802.11b*** • IEEE ***802.11g*** • ***IEEE 802.11a*** **Note:** *If you have a two-radio AP, different modes may available depending on whether Radio One or Radio Two is selected in the Radio field above.* *When you select the radio Mode, the appropriate set of Basic and Supported Rates for that Mode is automatically selected. (See description of* Rate Sets *further down in this table, on page 168.)*
Super AG	Enabling Super AG provides better performance by increasing radio throughput for a radio mode (IEEE 802.11b, g, a, and so on). Keep in mind that, with Super AG enabled, the access point transmissions will consume more bandwidth. • To enable Super AG click **Enabled**. • To disable Super AG click **Disabled**.

Table 16.1 Radio Settings

Field	Description
Extended Range	Atheros Extended Range (XR) is a proprietary method for implementing low rate traffic over longer distances. It is transparent to XR enabled clients and access points and is designed to be interoperable with the 802.11 standard in 802.11g and 802.11a modes. There is no support for Atheros XR in 802.11b, Atheros Turbo 5 GHz, or Atheros Dynamic Turbo 5 GHz. Enabling Atheros XR will extend the range over which your client and access point can operate. • To enable Extended Range, click **Enabled**. • To disable Extended Range, click **Disabled**. This option will not be available if you selected the hardware mode IEEE 802.11b, Atheros Turbo 5 GHz, or Atheros Dynamic Turbo 5 GHz. Atheros XR is not supported by these hardware modes.
Channel	The ***Channel*** defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. For most Modes, the default is **Auto**. Auto is the recommended mode because it automatically detects the best channel choices based on signal strength, traffic loads, and so on. However, you can also select a channel between one and eleven, inclusively.
Beacon Interval	***Beacon*** frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every **100** milliseconds (or 10 per second). The *Beacon Interval* value is set in milliseconds. Enter a value from **20** to **2000**.
DTIM Period	The *Delivery Traffic Information Map* (***DTIM***) message is an element included in some ***Beacon*** frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up. The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup. Specify a DTIM period within the given range (**1 - 255**). The measurement is in beacons. For example, if you set this to **1**, clients will check for buffered data on the AP at every beacon. If you set this to **2**, clients will check on every other beacon. If you set this to **10**, clients will check on every 10th beacon.

Table 16.1 Radio Settings

Field	Description
Fragmentation Threshold	Specify a number between **256** and **2,346** to set the frame size threshold in bytes. The *fragmentation threshold* is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value (**2,346** bytes) effectively disables fragmentation. Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help *improve* network performance and reliability if properly configured. Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems; for example, with microwave ovens. By default, fragmentation is **off**. We recommend not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.
RTS Threshold	Specify an ***RTS Threshold*** value between **0** and **2347**. The RTS threshold specifies the packet size of a request to send (***RTS***) transmission. This helps control traffic flow through the access point, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
Maximum Stations	Specify the maximum number of stations allowed to access this AP at any one time. You can enter a value between **0** and **2007**.

Table 16.1 Radio Settings

Field	Description
Transmit Power	Provide a percentage value to set the transmit power for this access point. The default is to have the access point transmit using **100 percent** of its power. ▶ Recommendations: • For most cases, we recommend keeping the default and having the transmit power set to **100 percent**. This is more cost-efficient as it gives the access point a maximum broadcast range, and reduces the number of APs needed. • To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This will help reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
Rate Sets	Check the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise. Rates are expressed in megabits per second. • *Supported Rate Sets* indicate rates that the access point supports. You can check multiple rates (click a checkbox to select or de-select a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP. • *Basic Rate Sets* indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets. To support both “b” and “g” clients, change the radio Mode to I**EEE 802.11g**. The Web UI will automatically select the default Rate Sets that allow both “b” and “g” clients to connect. To support only “g” clients, change the radio Mode to I**EEE 802.11g**. The Web UI will automatically select the default Rate Sets. Now add **24**, **12**, and **6** as Basic Rates. This will prevent “b” clients from connecting since they do not support these rates, but will allow “g” clients to connect since they are required by the standard to support these rates. For more information, see description of *Mode* further up in this table, on page 165.

Table 16.1 Radio Settings

Field	Description
Enable Broadcast/Multicast Rate Limiting	Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. Some protocols use multicast and broadcast packets for traffic that the majority of nodes on a network are uninterested in. For example, ARP requests for other machines, DHCP or BOOTP messages. For some protocols, if you set a rate limit control you limit the number of redundant packets transmitted across the network. Typically, any filtered traffic will be retransmitted at a later time and will not cause difficulties. • To enable Multicast and Broadcast Rate Limiting, click **Enabled**. • To disable Multicast and Broadcast Rate Limiting, click **Disabled**. By default the *Multicast/Broadcast Rate Limiting* option is disabled. Until you enable Multicast/Broadcast Rate Limiting, the following fields will be disabled.
Broadcast/ Multicast Rate Limit	Enter the rate limit you want to set for multicast and broadcast traffic. The limit should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform and be transmitted to the appropriate destination. The default and maximum rate limit setting is 50 packets per second.
Broadcast/ Multicast Rate Limit Burst	Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit. The default and maximum rate limit burst setting is 75 packets per second.

Table 16.1 Radio Settings

16.4 Updating Settings

To update Radio settings:

1. Navigate to the *802.11 Advanced Settings* tab page.
2. Configure the radio settings as required.
3. Click the **Update** button to apply the changes.

Note: *If you are using the two-radio version of the 9160 G2 Wireless Gateway, keep in mind that both Radio One and Radio Two are configured on this tab. The displayed settings apply to either Radio One or Radio Two, depending on which radio you choose in the* Radio *field (first field on tab). When you have configured settings for one of the radios, click* ***Update*** *and then select and configure the other radio. Be sure to click* ***Update*** *to apply the second set of configuration settings for the other radio.*

MAC ADDRESS FILTERING 17

A *Media Access Control* (***MAC***) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

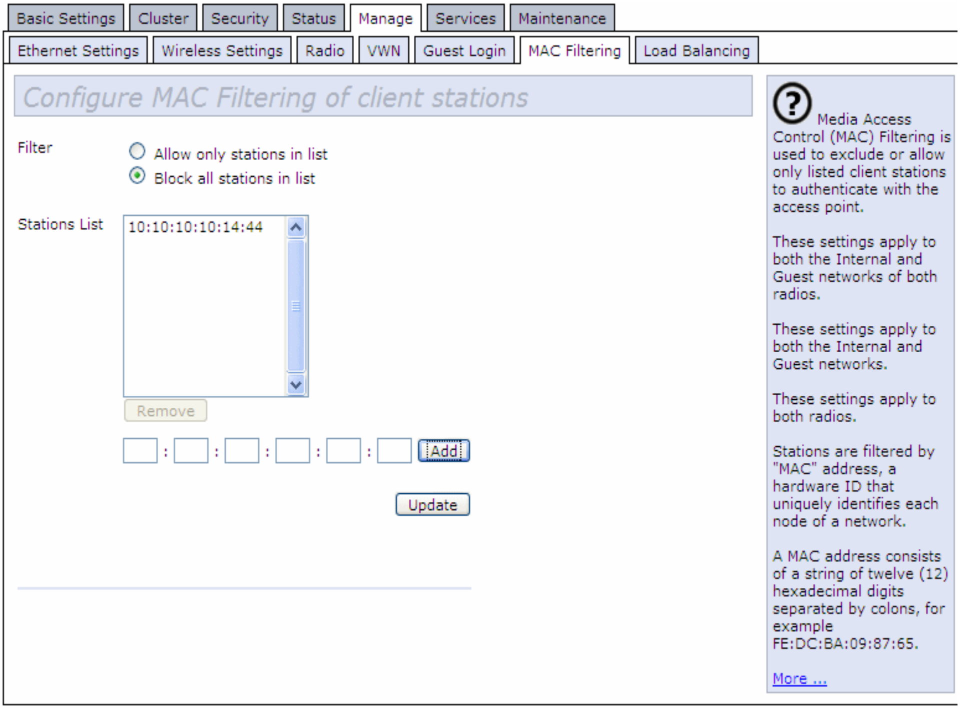
Each wireless network interface card (***NIC***) used by a wireless client has a unique MAC address.

You can control client access to your wireless network by switching on *MAC Filtering* and specifying a list of approved MAC addresses. When MAC Filtering is on, only clients with a listed MAC address can access the network.

The following sections describe how to use MAC address filtering on the 9160 G2 Wireless Gateway.

17.1 Navigating To MAC Filtering Settings

To enable filtering by MAC address, navigate to the *Manage > MAC Filtering* tab, and update the fields as described below.



Configure MAC Filtering of client stations

Filter ○ Allow only stations in list
● Block all stations in list

Stations List 10:10:10:10:14:44

Media Access Control (MAC) Filtering is used to exclude or allow only listed client stations to authenticate with the access point.

These settings apply to both the Internal and Guest networks of both radios.

These settings apply to both the Internal and Guest networks.

These settings apply to both radios.

Stations are filtered by "MAC" address, a hardware ID that uniquely identifies each node of a network.

A MAC address consists of a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

More ...

17.2 Using MAC Filtering

This page allows you to control access to the 9160 G2 Wireless Gateway based on *Media Access Control* (MAC) addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *prevent* access to the stations listed.

For the Guest interface, ***MAC*** Filtering settings apply to both ***BSS***es.

On a two-radio AP, MAC Filtering settings apply to both radios.

Field	Description
Filter	To set the MAC Address *Filter*, click one of the following radio buttons: • **Allow only stations in the list** • **Block all stations in list**
Stations List	To add a MAC Address to Stations List, enter its 48-bit MAC address into the lower text boxes, then click **Add**. The MAC Address is added to the Stations List. To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click **Remove**. The stations in the list will either be allowed or prevented from accessing the AP based on how you set the Filter.

Table 17.1 MAC Filtering Settings

17.3 Updating Settings

To update MAC settings:

1. Navigate to the *MAC Filtering* tab page.
2. Configure the MAC settings as required.
3. Click the **Update** button to apply the changes.

LOAD BALANCING 18

The 9160 G2 Wireless Gateway allows you to balance the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent scenarios where a single access point in your network shows performance degradation because it is handling a disproportionate share of the wireless traffic.

The following sections describe how to configure Load Balancing on your wireless network.

18.1 Understanding Load Balancing

Like most configuration settings on the 9160 G2 Wireless Gateway, load balancing settings are shared among clustered access points.

Note: *In some cases you might want to set limits for only one access point that is consistently over-utilized. You can apply unique settings to a particular access point if it is operating in standalone mode. (See ““Understanding Clustering” on page 56 and “Navigating To Access Points Management” on page 55.)*

18.1.1 Identifying Imbalance: Overworked Or Under-utilized Access Points

A typical scenario is that a comparison of Client Association data and Transmit/Receive data for multiple access points allows you to identify an access point that is consistently handling a disproportionately large percentage of wireless traffic. This can happen when location placement or other factors causes one access point to transmit the strongest signal to a majority of clients on a network. By default, that access point will receive most of the client requests while the other access points stay idle much of the time.

Imbalances in distribution of wireless traffic across access points will be evident in Client Association data and Transmit/Receive statistics, which will show higher “Utilization” rates on overworked APs and conversely, higher “Idle” times on under-utilized APs. An AP that is handling more than its fair share of traffic might also show slower data rates or lower transmit/receive rates due to the overload.

18.1.2 Specifying Limits For Utilization And Client Associations

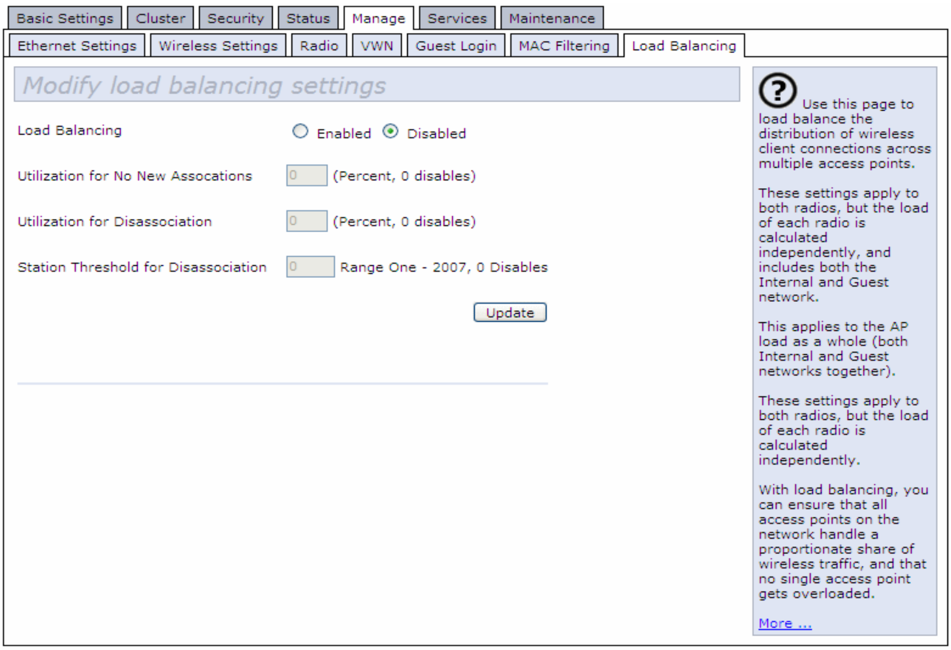
You can correct for imbalances in network AP utilization by enabling load balancing and setting limits on utilization rates and number of client associations allowed per access point.

18.1.3 Load Balancing And QoS

Load balancing also plays a part in contributing to *Quality of Service* (QoS) for *Voice Over IP* (VoIP) and other such time-sensitive applications competing for bandwidth and timely access to the air waves on a wireless network. For more information about configuring your network for QoS, see Chapter 19: “Quality of Service (QoS)”.

18.2 Navigating To Load Balancing Settings

On the Administration UI, navigate to the *Manage* > *Load Balancing* tab, and update the fields as described in the next section.



Modify load balancing settings

Load Balancing ○ Enabled ● Disabled

Utilization for No New Assocations 0 (Percent, 0 disables)

Utilization for Disassociation 0 (Percent, 0 disables)

Station Threshold for Disassociation 0 Range One - 2007, 0 Disables

Use this page to load balance the distribution of wireless client connections across multiple access points.

These settings apply to both radios, but the load of each radio is calculated independently, and includes both the Internal and Guest network.

This applies to the AP load as a whole (both Internal and Guest networks together).

These settings apply to both radios, but the load of each radio is calculated independently.

With load balancing, you can ensure that all access points on the network handle a proportionate share of wireless traffic, and that no single access point gets overloaded.

18.3 Configuring Load Balancing

To configure load balancing, *enable* **Load Balancing** and set limits and behaviour to be triggered by a specified utilization rate of the access point.

Notes: *Even when clients are disassociated from an AP, the network will still provide continuous service to client stations if another access point is within range so that clients can re-connect to the network. Clients should automatically retry the AP they were originally connected to and other APs on the subnet. Clients who are disassociated from one AP should experience a seamless transition to another AP on the same subnet.*

Load Balancing settings apply to the AP load as a whole. When Guest access is enabled, the settings apply to both Internal and Guest networks together.

On a two-radio access point, Load Balancing settings apply to both radios but the load of each radio is calculated independently and includes both the Internal and Guest network (when Guest access is enabled).

Field	Description
Load Balancing	To enable load balancing on this access point, click **Enable**. To disable load balancing on this access point, click **Disable**.
Utilization for No New Associations	Utilization rate limits relate to wireless bandwidth utilization. Provide a bandwidth utilization rate percentage limit for this access point to indicate when to stop accepting new client associations. When the utilization rate for this access point exceeds the specified limit, no new client associations will be allowed on this access point. If you specify **0** in this field, all new associations will be allowed regardless of the utilization rate.
Utilization for Disassociation	Utilization rate limits relate to wireless bandwidth utilization. Provide a bandwidth utilization rate percentage limit for this access point to indicate when to disassociate current clients. When the utilization rate exceeds the specified limit, a client currently associated with this access point will be disconnected. If you specify **0** in this field, current clients will never be disconnected regardless of the utilization rate.

Table 18.1 Load Balancing Settings

Field	Description
Stations Threshold for Disassociation	Specify the number of client stations you want as a “stations threshold” for disassociation. If the number of client stations associated with the AP at any one time is equal to or less than the number you specify here, no stations will be disassociated regardless of the *Utilization for Disassociation* value. Theoretically, the maximum number of client stations allowed is **2007**. ▶ We recommend setting the maximum to between **30** and **50** client stations. This allows for a workable load on the access point, given that bandwidth is shared among the AP clients.

Table 18.1 Load Balancing Settings

18.4 Updating Settings

To update load balancing settings:

1. Navigate to the *Load Balancing* tab page.
2. Configure the load balancing settings as required.
3. Click the **Update** button to apply the changes.

QUALITY OF SERVICE (QOS) 19

Quality of Service (***QoS***) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), other types of audio, video, and streaming media, as well as traditional IP data over the 9160 G2 Wireless Gateway.

The following sections describe how to configure Quality of Service queues on the 9160 G2 Wireless Gateway.

19.1 Understanding QoS

A primary factor that affects QoS is network congestion due to an increased number of clients attempting to access the air waves and higher traffic volume competing for bandwidth during a busy time of day. The most noticeable degradation in service on a busy, overloaded network will be evident in time-sensitive applications like Video, *Voice-over-IP* (VoIP), and streaming media.

Unlike typical data files which are less affected by variability in QoS, Video, VoIP and streaming media must be sent in a specific order at a consistent rate and with minimum delay between ***Packet*** transmission. If the quality of service is compromised, the audio or video will be distorted.

19.1.1 QoS And Load Balancing

By using a combination of load balancing (see Chapter 18: “Load Balancing”) and QoS techniques, you can provide a high quality of service for time-sensitive applications even on a busy network. Load balancing is a way of better distributing the traffic volume across access points. QoS is a means of allocating bandwidth and network access based on transmission priorities for different types of wireless traffic within a single access point.

19.1.2 802.11e And WMM Standards Support

QoS describes a range of technologies for controlling data streams on shared network connections. The ***IEEE 802.11e*** task group is in the process of defining a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion; limiting ***Jitter***, ***Latency***, and ***Packet Loss***; supporting dedicated bandwidth for time-sensitive or mission critical applications, and prioritizing wireless traffic for channel access.

As with all IEEE ***802.11*** working group standards, the goal is to provide a standard way of implementing QoS features so that components from different companies are interoperable.

The 9160 G2 Wireless Gateway provides QoS based on the *Wireless Multimedia* (***WMM***) specification and *Wireless Multimedia* (WMM) standards, which are implementations of a subset of ***802.11e*** features.

Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled.

19.1.3 QoS Queues And Parameters To Coordinate Traffic Flow

Configuring QoS options on the 9160 G2 Wireless Gateway consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

For example, time-sensitive Voice, Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

The 9160 G2 Wireless Gateway implements QoS based on the IEEE Wireless Multimedia (WMM) standard. A Linux-based queuing class is used to tag packets and establish multiple queues. The queues provided offer built-in prioritization and routing based on the type of data being transmitted.

The Administration UI provides a way for you to configure parameters on the queues.

19.1.3.1 QoS Queues And Type Of Service (ToS) On Packets

QoS on the 9160 G2 Wireless Gateway leverages ***WMM*** information in the ***IP*** packet header related to Type of Service (***ToS***). Every IP packet sent over the network includes a ToS field in the header that indicates how the data should be prioritized and transmitted over the network. The ToS field consists of a 3 to 7 bit value with each bit representing a different aspect or degree of priority for this data as well as other meta-information (low delay, high throughput, high reliability, low cost, and so on).

For example, the ToS for FTP data packets is likely to be set for maximum throughput since the critical consideration for FTP is the ability to transmit relatively large amounts of data in one go. Interactive feedback is a nice-to-have in this situation but certainly less critical. VoIP data packets are set for minimum delay because that is a critical factor in quality and performance for that type of data.

The access point examines the ToS field in the headers of all packets that pass through the AP. Based on the value in a packet's ToS field, the AP prioritizes the packet for transmission by assigning it to one of the queues. This process occurs automatically, regardless of whether you deliberately configure QoS or not.

A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

- Data 0 (Voice). Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.
- Data 1 (Video). High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.
- Data 2 (Best Effort). Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Data 3 (Background). Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Packets in a higher priority queue will be transmitted before packets in a lower priority queue. Interactive data in the queues labelled “Data 0” and “Data 1” is always sent first, best effort data in “Data 2” is sent next, and Background (bulk) data in “Data 3” is sent last. Each lower priority queue (class of traffic) gets bandwidth that is left over after the higher classes of traffic have been sent. At an extreme end if you have enough interactive data to keep the access point busy all the time, low priority traffic would never get sent.

Using the QoS settings on the Administration UI, you can configure *Enhanced Distributed Channel Access* (EDCA) parameters that determine how each queue is treated when it is sent by the access point to the client or by the client to the access point.

Note: *Wireless traffic travels:*

- *Downstream from the access point to the client station.*
- *Upstream from client station to access point.*
- *Upstream from access point to network.*
- *Downstream from network to access point.*

With WMM enabled, QoS settings on the 9160 G2 Wireless Gateway affect the first two of these; downstream *traffic flowing from the access point to client station (AP EDCA parameters) and the* upstream *traffic flowing from the station to the access point (station EDCA parameters).*

With WMM disabled, you can still set parameters on the downstream traffic flowing from the AP to the client station (AP EDCA parameters).

The other phases of the traffic flow (to and from the network) are not under control of the QoS settings on the AP.

19.1.3.2 EDCF Control Of Data Frames And Arbitration Interframe Spaces

Data is transmitted over 802.11 wireless networks in *frames*. A ***Frame*** consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network.

Note: *A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).*

Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection.

The 802.11 standard defines various *frame* types for management and control of the wireless infrastructure, and for data transmission. 802.11 frame types are: (1) *management frames*, (2) *control frames*, and (3) *data frames*. Management and control frames (which manage and control the availability of the wireless infrastructure) automatically have higher priority for transmission.

802.11e uses *interframe spaces* to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data.

Management and control frames wait a minimum amount of time for transmission; they wait a *short interframe space* (SIF). These wait times are built-in to 802.11 as infrastructure support and are not configurable.

The 9160 G2 Wireless Gateway supports the *Enhanced Distribution Coordination Function* (***EDCF***) as defined by the ***802.11e*** standard. EDCF, which is an enhancement to the ***DCF*** standard and is based on ***CSMA/CA*** protocol, defines the interframe space (IFS) between *data frames*. Data frames wait for an amount of time defined as the *arbitration interframe space* (AIFS) before transmitting.

This parameter is configurable.

Note: *Sending data frames in AIFS allows higher priority management and control frames to be sent in SIFs first.*

The AIFS ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free.

19.1.3.3 Random Backoff And Minimum/Maximum Contention Windows

If an access point detects that the medium is in use (busy), it uses the DCF *random backoff* timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum Contention Window*) increases exponentially up to a specified limit (*Maximum Contention Window*). The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.

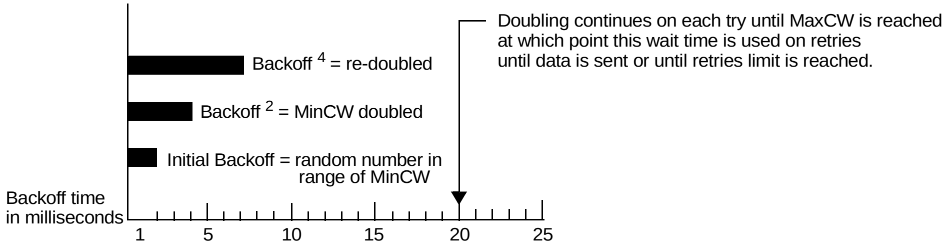


Figure 19.1 DCF Random Backoff Timer

The random backoff used by the access point is a configurable parameter. To describe the random delay, a "Minimum Contention Window" (MinCW) and a "Maximum Contention Window" (MaxCW) is defined.

- The value specified for the *Minimum Contention Window* is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the *Maximum Contention Window* is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

19.1.3.4 Packet Bursting For Better Performance

The 9160 G2 Wireless Gateway includes 802.11e based *packet bursting* technology that increases data throughput and speed of transmission over the wireless network. Packet bursting enables the transmission of multiple packets without the extra overhead of header information. The effect of this is to increase network speed and data throughput. The size of packet bursts allowed (maximum burst length) is a configurable parameter.

19.1.3.5 Transmission Opportunity (TXOP) Interval For Client Stations

The *Transmission Opportunity* (TXOP) is an interval of time when a Wi-Fi Multimedia (WMM) client station has the right to initiate transmissions onto the wireless medium (WM).

19.1.4 802.1p And DSCP Tags

IEEE ***802.1p*** is an extension of the IEEE 802 standard and is responsible for QoS provision. The primary purpose of 802.1p is to prioritize network traffic at the data link/MAC layer. 802.1p offers the ability to filter multicast traffic to ensure it doesn't increase over layer 2 switched networks. It uses tag frames for the prioritization scheme. To be compliant with this standard, layer 2 switches must be capable of grouping incoming LAN packets into separate traffic classes.

The 802.1p header includes a three-bit field for prioritization, which allows packets to be grouped into various traffic classes. Eight priority levels are defined. The highest priority is seven, which might go to network-critical traffic (voice). Higher priority packets are always transmitted first. Lower priority packets are not transmitted if higher priority packets are still in transmission, rather they are held in a queue until the higher packets have been successfully transmitted.The lowest priority level is zero, this is used as a best-effort default, it is invoked automatically when no other value has been set.

Note: *It is important to note that 802.1p will not work unless QoS and WMM are enabled. WMM must be enabled on both the AP and on the client connecting to the AP.*

The flow diagram in Figure 19.2 outlines the way in which tags are retrieved and traffic prioritized on a network.

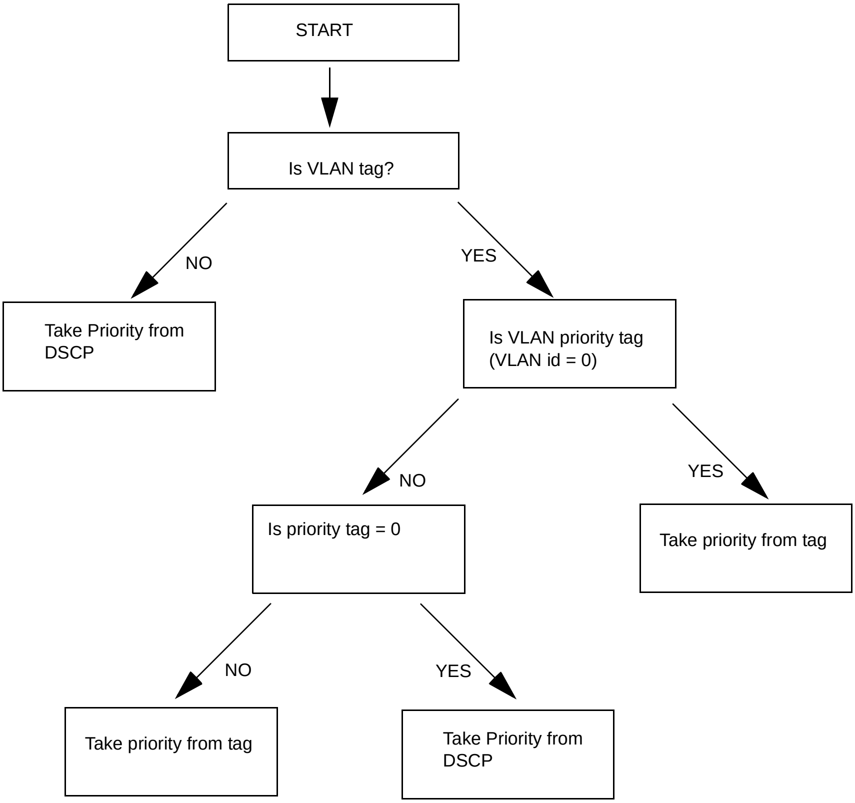


Figure 19.2 Prioritization Of Network Traffic

19.1.4.1 VLAN Priority

Table 19.1 outlines the priority tags and their associated values taken from a VLAN tag.

VLAN ID Tag	Priority
0 - default DHCP value	Best Effort
1	Background
2	Background
3	Best Effort
4	Video
5	Video
6	Voice
7	Voice

Table 19.1 VLAN Tag Priorities

19.1.4.2 DSCP Priority

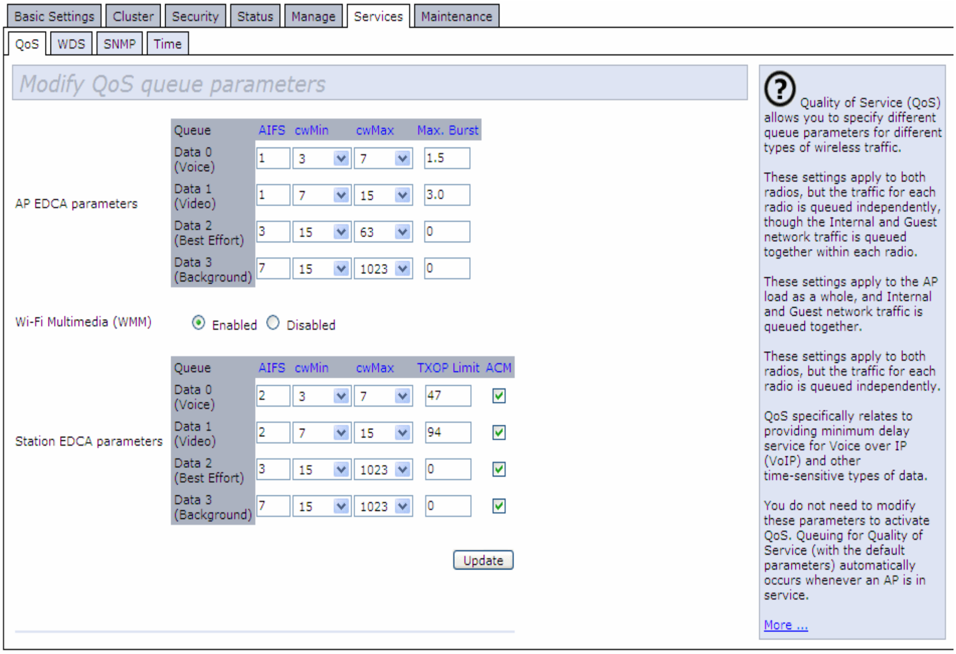
Table 19.2 outlines the DSCP values, the associated ID, and the priority level.

ID Tag	Priority	DSCP Value
0 - default DHCP value	Best Effort	0
1	Background	16
2	Background	8
3	Best Effort	24
4	Video	32
5	Video	40
6	Voice	48
7	Voice	56

Table 19.2 DSCP Tag Priorities

19.2 Configuring QoS Queues

To set up queues for QoS, navigate to the *Services* > *QoS* tab, and configure settings as described below.



Modify QoS queue parameters

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Wi-Fi Multimedia (WMM) ● Enabled ○ Disabled

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit	ACM
Data 0 (Voice)	2	3	7	47	☑
Data 1 (Video)	2	7	15	94	☑
Data 2 (Best Effort)	3	15	1023	0	☑
Data 3 (Background)	7	15	1023	0	☑

Quality of Service (QoS) allows you to specify different queue parameters for different types of wireless traffic.

These settings apply to both radios, but the traffic for each radio is queued independently, though the Internal and Guest network traffic is queued together within each radio.

These settings apply to the AP load as a whole, and Internal and Guest network traffic is queued together.

These settings apply to both radios, but the traffic for each radio is queued independently.

QoS specifically relates to providing minimum delay service for Voice over IP (VoIP) and other time-sensitive types of data.

You do not need to modify these parameters to activate QoS. Queuing for Quality of Service (with the default parameters) automatically occurs whenever an AP is in service.

Configuring Quality of Service (**QoS**) on the 9160 G2 Wireless Gateway consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (via *Contention Windows*) for transmission. The settings described here apply to data transmission behaviour on the access point only, not to that of the client stations.

Notes: *For the Guest interface, QoS queue settings apply to the access point load as a whole (both BSSes together).*

On a two-radio access point these settings apply to both radios but the traffic for each radio is queued independently. (The exception to this is guest traffic as noted below.)

Internal and Guest network traffic is always queued together within each radio. This is the case on both one-radio and two-radio APs.

Configuring Quality of Service includes:

- "Configuring AP EDCA Parameters" on page 192.
- "Enabling/Disabling Wi-Fi Multimedia" on page 193.
- "Updating Settings" on page 195.

19.2.1 Configuring AP EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station.

Field	Description
Queue	Queues are defined for different types of data transmitted from AP-to-station: **Data 0 (Voice)** High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1(Video)** High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (best effort)** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For more information, see "QoS Queues And Parameters To Coordinate Traffic Flow" on page 184.
AIFS *(Inter-Frame Space)*	The *Arbitration Inter-Frame Spacing* (AIFS) specifies a wait time (in milliseconds) for *data frames*. Valid values for AIFS are **1** through **255**. For more information, see "EDCF Control Of Data Frames And Arbitration Interframe Spaces" on page 186.

Table 19.3 AP EDCA Parameters

Field	Description
cwMin (Minimum Contention Window)	This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the *Minimum Contention Window* is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for the "`cwmin`" are **1, 3, 7, 15, 31, 63, 127, 255, 511**, or **1023**. For more information, see "Random Backoff And Minimum/Maximum Contention Windows" on page 187.
cwMax (Maximum Contention Window)	The value specified here in the *Maximum Contention Window* is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "`cwmax`" are **1, 3, 7, 15, 31, 63, 127, 255, 511**, or **1023**. For more information, see "Random Backoff And Minimum/Maximum Contention Windows" on page 187.
Max. Burst Length	**AP EDCA Parameter Only** (The Max. Burst Length applies only to traffic flowing from the access point to the client station.) This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A *packet burst* is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are **0.0** through **999.9**. For more information, see "Packet Bursting For Better Performance" on page 188.

Table 19.3 AP EDCA Parameters

19.2.2 Enabling/Disabling Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the 9160 G2 Wireless Gateway control *downstream* traffic flowing from the access point to client station (AP EDCA parameters) and the *upstream* traffic flowing from the station to the access point (station EDCA parameters).

Disabling WMM will deactivate QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the access point

With WMM disabled, you can still set parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters).

- To disable WMM extensions, click **Disabled**.
- To enable WMM extensions, click **Enabled**.

19.2.3 Configuring Station EDCA Parameters

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

Field	Description
Queue	Queues are defined for different types of data transmitted from station-to-AP: **Data 0 (Voice)** Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1(Video)** Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (Best Effort)** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For more information, see “QoS Queues And Parameters To Coordinate Traffic Flow” on page 184.
AIFS *(Inter-Frame Space)*	The *Arbitration Inter-Frame Spacing* (*AIFS*) specifies a wait time (in milliseconds) for *data frames*. For more information, see “EDCF Control Of Data Frames And Arbitration Interframe Spaces” on page 186.

Table 19.4 Station EDCA Parameters

Field	Description
cwMin (Minimum Contention Window)	This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the *Minimum Contention Window* is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. For more information, see "Random Backoff And Minimum/Maximum Contention Windows" on page 187.
cwMax (Maximum Contention Window)	The value specified here in the *Maximum Contention Window* is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. For more information, see "Random Backoff And Minimum/Maximum Contention Windows" on page 187.
TXOP Limit	**Station EDCA Parameter Only** (The TXOP Limit applies only to traffic flowing from the client station to the access point.) The *Transmission Opportunity* (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the *Transmission Opportunity* (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

Table 19.4 Station EDCA Parameters

19.3 Updating Settings

To update QoS settings:

1. Navigate to the QoS tab page.
2. Configure the *QoS* settings as required.
3. Click the **Update** button to apply the changes.

WIRELESS DISTRIBUTION SYSTEM 20

The 9160 G2 Wireless Gateway lets you connect multiple access points using a Wireless Distribution System (***WDS***). WDS allows access points to communicate with one another wirelessly. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

The following sections describe how to configure the WDS on the 9160 G2 Wireless Gateway.

20.1 Understanding The Wireless Distribution System

A *Wireless Distribution System* (***WDS***) is a technology that wirelessly connects access points, known as Basic Service Sets (***BSS***), to form what is known as an *Extended Service Set* (***ESS***).

Note: *A BSS generally equates to an access point (deployed as a single-AP wireless "network"), except in cases where multi-BSSID features make a single access point look like two or more access points to the network. In such cases, the access point has multiple unique BSSIDs.*

20.1.1 Using WDS To Bridge Distant Wired LANs

In an ***ESS***, a network of multiple access points, each access point serves part of an area which is too large for a single access point to cover. You can use WDS to bridge distant Ethernets to create a single ***LAN***. For example, suppose you have one access point which is connected to the network by Ethernet and serving multiple client stations in the Conference Room (LAN Segment 1), and another Ethernet-wired access point serving stations in the West Wing offices (LAN Segment 2). You can bridge the Conference Room and West Wing access points with a WDS link to create a single network for clients in both areas (see Figure 20.1 on page 200).

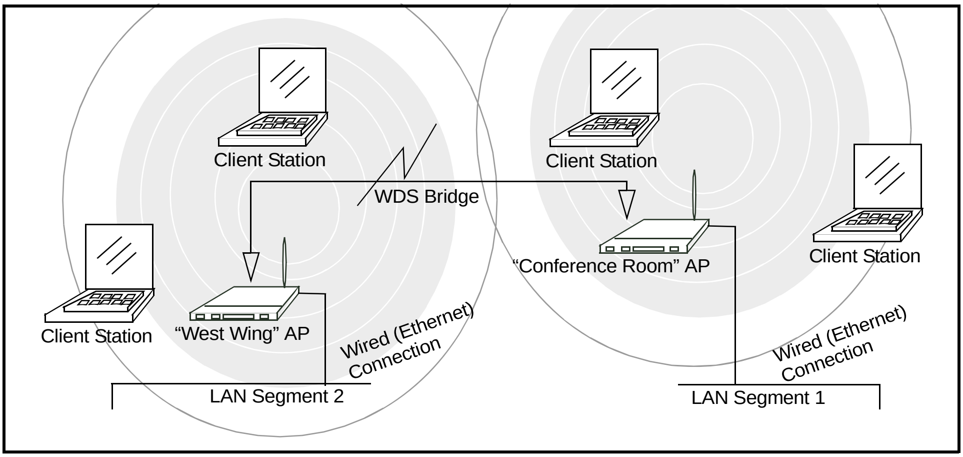


Figure 20.1 Bridged Distant Wired LANs

20.1.2 Using WDS To Extend Network Beyond The Wired Coverage Area

An ***ESS*** can extend the reach of the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have an access point which is connected to the network by Ethernet and serving multiple client stations in one area ("East Wing" in our example), but cannot reach others which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with Ethernet cabling. You can solve this problem by placing a second access point closer to the second group of stations ("Poolside" in our example in Figure 20.2 on page 201) and bridge the two APs with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations (see Figure 20.2 on page 201).

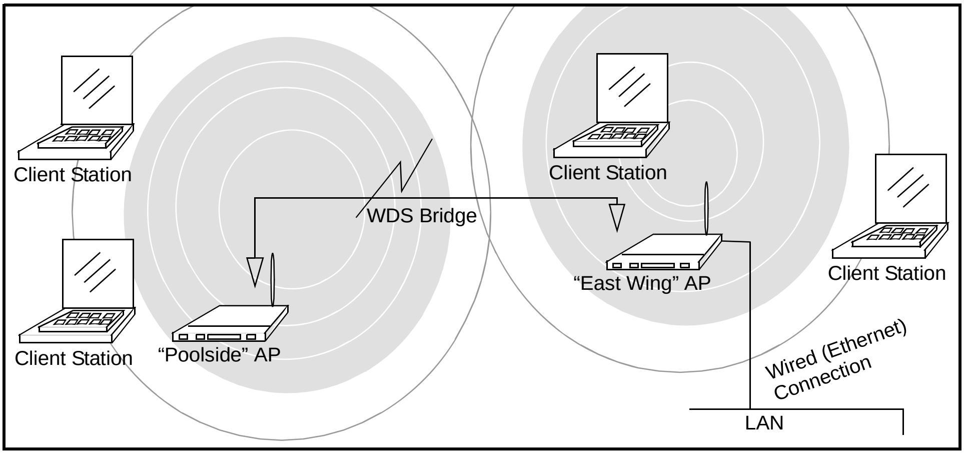


Figure 20.2 Extended Network Beyond The Wired Coverage Area

20.1.3 Using WDS To Create Backup Links

Another use for WDS bridging is the creation of backup links. With *Spanning Tree Protocol (**STP**)* automatically enabled on the 9160 G2 Wireless Gateway, WDS can be used to configure backup paths between access points across the network. For example, between two access points you could have both a primary path via Ethernet and a secondary (backup) wireless path via a WDS link. If the Ethernet connection goes down, STP reconfigures its map of the network and effectively fixes the down network segment by activating the backup wireless path.

20.2 Security Considerations Related To WDS Links

It is important to set some type of security on WDS links. You can set any type of security on the WDS link, regardless of the security setting applied to the APs on the link. For example, you may have the security on AP1 set to **None** and the security on AP2 set to **WEP**. Even though both settings are different, you can choose to set the security on the WDS link as either None or WEP. The only exception to this rule is in the case of WPA (PSK). The WPA (PSK) security setting can only be set on the WDS link if you have set security on both AP1 and AP2 to either WPA Personal or WPA Enterprise.

20.2.1 Understanding Static WEP Data Encryption

Static *Wired Equivalent Privacy* (***WEP***) is a data encryption protocol for 802.11 wireless networks. Both access points in a given WDS link must be configured with the same security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

You can enable Static ***WEP*** on the WDS link (bridge). When WEP is enabled, all data exchanged between the two access points in a WDS link is encrypted using a fixed WEP key that you provide.

Static WEP does not provide effective data protection to the level of other security modes available for service to client stations. If you use Static WEP on a ***LAN*** intended for secure wireless traffic you are putting your network at risk. Therefore, we recommend using WPA (PSK) encryption on any WDS links on an internal network. Do not use Static WEP-based WDS to bridge access points on the Internal network unless you have no concerns about the security risk for data traffic on that network. For more information on WPA (PSK), see “Understanding WPA (PSK) Data Encryption”, below.

For more information about the effectiveness of the different security modes, see Chapter 10: “Configuring Security”. This topic also covers use of the unencrypted security mode for AP-to-station traffic on the Guest network, which is intended for less sensitive data traffic.

20.2.2 Understanding WPA (PSK) Data Encryption

Wi-Fi Protected Access (Pre-Shared Key) or WPA (PSK) is a more robust form of security than Static WEP. Formerly known as ‘WPA-Home’, WPA (PSK) works using a pre-shared key which is basically a shared password between the APs on a bridged link. WPA (PSK) provides enhanced 802.11 wireless security without the need for a RADIUS authentication infrastructure, which is both complicated and expensive to implement.

Since WPA (PSK) encryption relies upon a shared key, both APs on the WDS link must be set with the same key, otherwise they will not be able to communicate and share information.

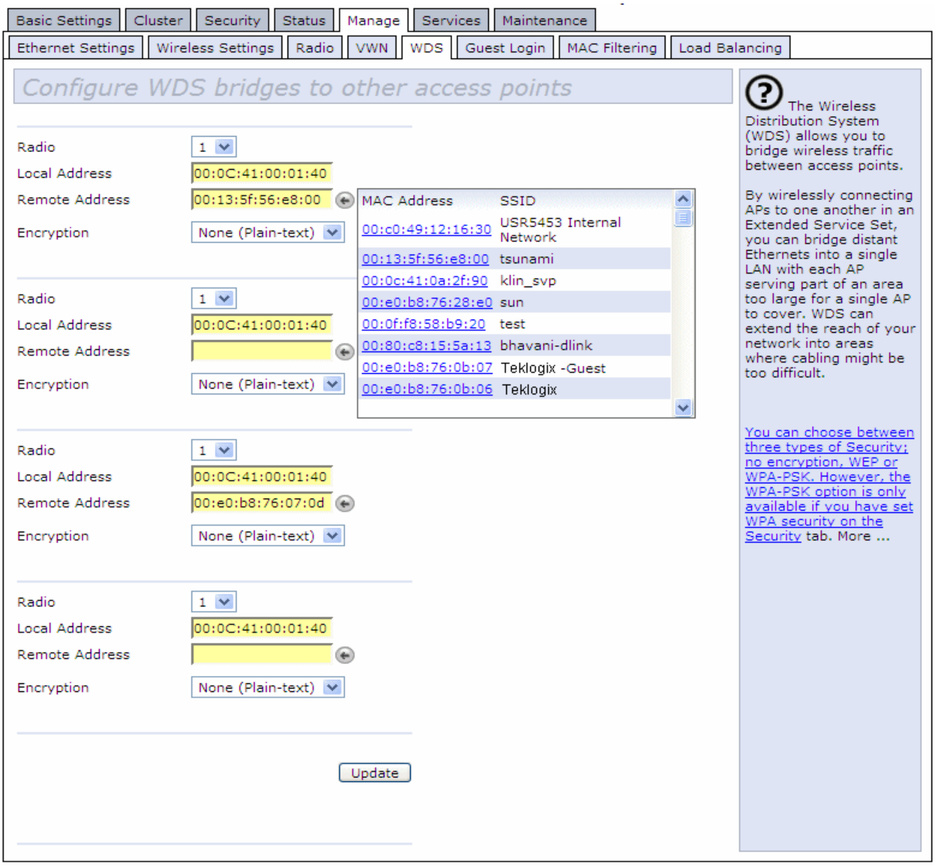
Note: *For security reasons it is recommended you change the shared keys on your WDS bridge on a regular basis.*

For more information about the effectiveness of the different security modes, see Chapter 10: “Configuring Security”.

20.3 Configuring WDS Settings

To specify the details of traffic exchange from this access point to others, navigate to the *Manage* > *WDS* tab, and update the fields as described below.

Note: *Figure 20.3 shows the WDS settings page for the two-radio AP. The Administration Web page for the one-radio AP will look slightly different.*



Configure WDS bridges to other access points

Radio: 1
Local Address: 00:0C:41:00:01:40
Remote Address: 00:13:5f:56:e8:00
Encryption: None (Plain-text)

Radio: 1
Local Address: 00:0C:41:00:01:40
Remote Address:
Encryption: None (Plain-text)

Radio: 1
Local Address: 00:0C:41:00:01:40
Remote Address: 00:e0:b8:76:07:0d
Encryption: None (Plain-text)

Radio: 1
Local Address: 00:0C:41:00:01:40
Remote Address:
Encryption: None (Plain-text)

MAC Address	SSID
00:c0:49:12:16:30	USR5453 Internal Network
00:13:5f:56:e8:00	tsunami
00:0c:41:0a:2f:90	klin_svp
00:e0:b8:76:28:e0	sun
00:0f:f8:58:b9:20	test
00:80:c8:15:5a:13	bhavani-dlink
00:e0:b8:76:0b:07	Teklogix -Guest
00:e0:b8:76:0b:06	Teklogix

? The Wireless Distribution System (WDS) allows you to bridge wireless traffic between access points.

By wirelessly connecting APs to one another in an Extended Service Set, you can bridge distant Ethernets into a single LAN with each AP serving part of an area too large for a single AP to cover. WDS can extend the reach of your network into areas where cabling might be too difficult.

You can choose between three types of Security; no encryption, WEP or WPA-PSK. However, the WPA-PSK option is only available if you have set WPA security on the Security tab. More ...

Figure 20.3 Wireless Distribution System Settings

The following notes summarize some critical guidelines regarding ***WDS*** configuration. Please read all the notes before proceeding with WDS configuration.

Notes:
- *When using WDS, be sure to configure WDS settings on* both *access points participating in the WDS link.*
- *You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.*
- *Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See Chapter 16: "Configuring 802.11 Radio Settings" for information on configuring the Radio mode and channel.)*
- *When* ***802.11h*** *is operational, setting up WDS links can be difficult. See "802.11h Regulatory Domain Control" on page 142.*

To configure WDS on this access point, describe each AP intended to receive hand-offs and send information to this AP. Each destination AP needs the following description, as shown in Table 20.4.

Field	Description
Radio	The 9160 G2 Wireless Gateway is available as a one-radio or two-radio access point. **One-Radio AP:** On the one-radio version of the 9160 G2 Wireless Gateway, this field is not included on the *WDS* tab. **Two-Radio AP:** For each WDS link on a two-radio AP, select **Radio One** or **Radio Two**. The rest of the settings for the link apply to the radio selected in this field. The read-only "Local Address" will change depending on which Radio you select here.

Table 20.4 Destination Access Point Settings

Field	Description
Local Address	Indicates the Media Access Control (***MAC***) addresses for this access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point or interface. **One-Radio AP:** On a one-radio access point, a single MAC address is shown at the top of the *WDS* settings page. The address shown for the one-radio AP is the MAC address for that radio AP. This is the address by which the AP is known externally to other networks. **Two-Radio AP:** For each WDS link on a two-radio AP, the *Local Address* reflects the MAC address for the internal interface on the selected radio (Radio One on `WLAN0` or Radio Two `WLAN1`).
Remote Address	Specify the MAC address of the destination access point; that is, the access point to which data will be sent or “handed-off” and from which data will be received (in other words, the AP to which you are creating the WDS bridge). Click the **arrow** to the right of the *Remote Address* field to see a list of all the available MAC Addresses and their associated SSIDs on the network. Select the appropriate MAC address from the list. ***Note:*** *The SSID displayed in the drop-down list is simply to help you identify the correct MAC Address for the destination access point. This SSID is a separate SSID to that which you set for the WDS link. The two do not (and should not) be the same value or name.*

Table 20.4 Destination Access Point Settings

Field	Description
Encryption	If you are unconcerned about security issues on the WDS link you may decide not to set any type of encryption. Alternatively, if you have security concerns you can choose between Static WEP, and WPA (PSK). ***Note:*** *The types of encryption options available here will depend on the settings you have specified on the* Security *tabbed page.The WPA (PSK) option will only be an available option on the* WDS *page if you set the Mode on the* Security *tabbed page to* ***WPA Personal*** *or* ***WPA Enterprise***. **None** (Plain Text): If you set encryption to **None**, the data sent between the APs across the WDS bridge will not be encrypted, but rather will be sent as plain text. **WEP**: Specify whether you want Wired Equivalent Privacy (***WEP***) encryption enabled for the WDS link. Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. **Both** access points on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. For more information on WEP security, see “Static WEP” on page 102. **WPA (PSK)**: Specify whether you want ***WPA*** (***PSK***) encryption enabled for the WDS link. Wi-Fi Protected Access Pre-Shared Key, WPA (PSK) is a more secure form of encryption than WEP. When you use WPA (PSK) encryption, each AP on your network must be set with the same unique key, otherwise the APs will not be able to communicate with one another. The WPA (PSK) option will only be an available option on the *WDS* page if you set the Mode on the *Security* tabbed page to **WPA Personal** or **WPA Enterprise**. For more information on Security, see “Understanding Security Issues On Wireless Networks” on page 91. For more information on WPA (PSK) security, see “WPA Personal” on page 109.

Table 20.4 Destination Access Point Settings

20.3.1 Example Of Configuring A WDS Link

When using WDS, be sure to configure *WDS* settings on *both* access points on the WDS link. For example, to create a WDS link between a pair of access points “**MyAP1**” and “**MyAP2**” do the following:

1. Open the Administration Web pages for MyAP1, by entering the IP address for MyAP1 as a URL in the Web browser address bar in the following form:

   http://IPAddressOfAccessPoint

   where *IPAddressOfAccessPoint* is the address of MyAP1.

2. Navigate to the *WDS* tab on MyAP1 Administration Web pages.

   The MAC address for MyAP1 (the access point you are currently viewing) will show as the “Local Address” at the top of the page.

3. Configure a WDS interface for data exchange with MyAP2.

   Start by entering the MAC address for MyAP2 as the “Remote Address” and fill in the rest of the fields to specify the network (guest or internal), security, and so on. Save the settings (click **Update**).

4. Navigate to the radio settings on the Administration Web pages (*Manage* > *Radio*) to verify or set the mode and the radio channel on which you want MyAP1 to broadcast.

   Remember that the two access points participating in the link, MyAP1 and MyAP2, must be set to the same Mode and be transmitting on the same channel.

   For our example, let’s say we’re using IEEE 802.11b Mode and broadcasting on Channel 6. (We’d choose Mode and Channel from the drop-down menus on the Radio tab.)

5. Now repeat the same steps for MyAP2:

   - Open Administration Web pages for MyAP2 by using MyAP2’s IP address in a URL.
   - Navigate to the *WDS* tab on MyAP2 Administration Web pages. (MyAP2’s MAC address will show as the “Local Address”.)
   - Configure a WDS interface for data exchange with MyAP1, starting with the MAC address for MyAP1.
   - Navigate to the radio settings for MyAP2 to verify that it is using the same mode and broadcasting on the same channel as MyAP1. (For our example Mode is 802.11b and the channel is 6.)
   - Be sure to save the settings by clicking **Update**.

20.4 Updating Settings

To update WDS settings:

1. Navigate to the *WDS* tab page.
2. Configure the WDS settings as required.
3. Click the **Update** button to apply the changes.

CONFIGURING SNMP 21

The following sections describe how to configure SNMP and related settings on the 9160 G2 Wireless Gateway Enterprise-Manager API:

21.1 Understanding SNMP Settings

Simple Network Management Protocol (SNMP) defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a management system. The agents store data about their devices in Management Information Bases (MIBs) and return this data to the SNMP manager when requested. Managed devices can be network nodes such as access point base stations, routers, switches, bridges, hubs, servers, or printers.

The 9160 G2 Wireless Gateway can function as an SNMP-managed device for seamless integration into network management systems such as HP OpenView or Devicescape Wireless Operations Center.

MIBs are a collection of objects or files that exist in a virtual database on a network. SNMP uses a specific set of commands and queries to obtain information from the MIB.

The 9160 G2 Wireless Gateway supports the following standard SNMP MIBs:

- Bridge MIB 802.1d (RFC 1493).
- SNMPv2 MIB (RFC 3418).
- IEEE Std 802.11 MIB (base).
- Interfaces Group MIB (RFC 2233).
- Two proprietary MIBs (Wireless MIB and System MIB) based on the upcoming IEEE 802.11k MIB. They provide information about the 9160 G2 Wireless Gateway client association list and AP detection table, respectively. The proprietary System MIB provides maintenance functionality such as system reboot or firmware upgrade.

The 9160 G2 Wireless Gateway also supports SNMP traps. Figure 21.1 illustrates how SNMP works on a network.

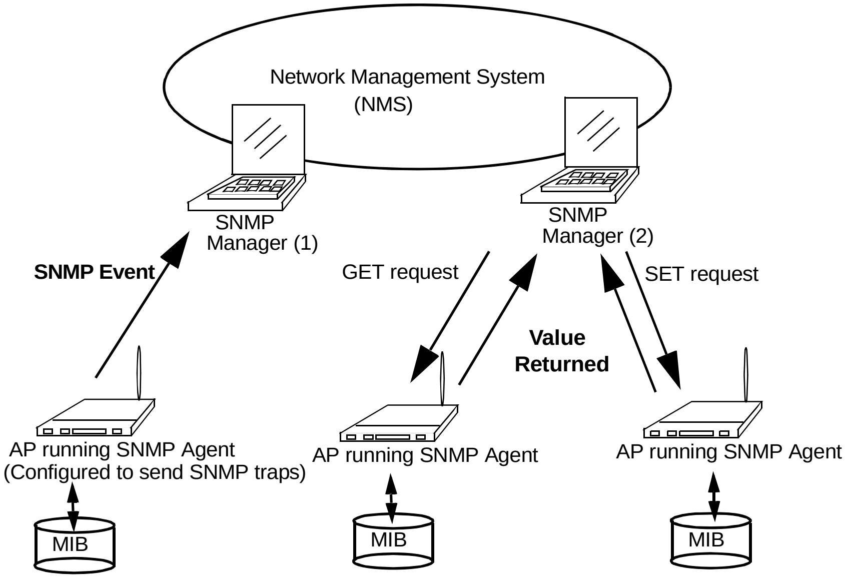
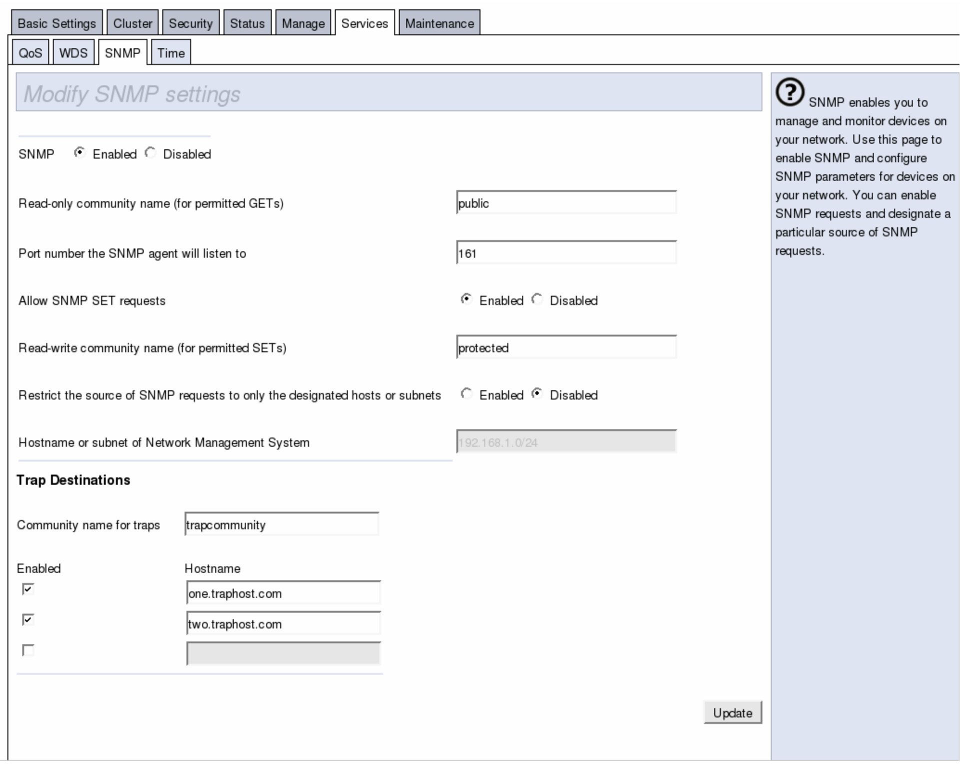


Figure 21.1 SNMP Running On A Network

21.2 Navigating To SNMP Settings

To configure SNMP settings, navigate to *Services > SNMP*, and update the fields as described below.



Modify SNMP settings

SNMP ● Enabled ○ Disabled

Read-only community name (for permitted GETs): public

Port number the SNMP agent will listen to: 161

Allow SNMP SET requests: ● Enabled ○ Disabled

Read-write community name (for permitted SETs): protected

Restrict the source of SNMP requests to only the designated hosts or subnets: ○ Enabled ● Disabled

Hostname or subnet of Network Management System: 192.168.1.0/24

Trap Destinations

Community name for traps: trapcommunity

Enabled	Hostname
☑	one.traphost.com
☑	two.traphost.com
□	

SNMP enables you to manage and monitor devices on your network. Use this page to enable SNMP and configure SNMP parameters for devices on your network. You can enable SNMP requests and designate a particular source of SNMP requests.

21.3 Configuring SNMP Settings

Start/stop control of SNMP agents, community password configuration, access to MIBs, and configuration of SNMP Trap destinations is provided through the 9160 G2 Wireless Gateway, as described below.

Field	Description
SNMP Enabled/Disabled	You can choose whether or not you want to enable SNMP on your network. By default SNMP is disabled. • To enable SNMP, click **Enabled**. • To disable SNMP, click **Disabled**. ***Note:*** *If you do not enable SNMP, all remaining fields on the SNMP page will be disabled.*
Read-only community name for permitted GETs	Enter a read-only community name. The community name, as defined in SNMPv2c, acts as a simple authentication mechanism to restrict the machines on the network that can request data to the SNMP agent. The name functions as a password and the request is assumed to be authentic if the sender knows the password. The community name can be in any alphanumeric format.
Port number the SNMP agent will listen to	By default an SNMP agent only listens to requests from port 161. However, you can configure this so the agent listens to requests on another port. Enter the port number on which you want the SNMP agents to listen to requests.
Allow SNMP SET Requests	You can choose whether or not to allow SNMP SET requests. Enabling SET requests means that machines on the network can execute SET requests to the configured agent on the AP. ***Note:*** *SET requests are restricted to the proprietary System MIB.* • To enable SNMP SET requests, click **Enabled**. • To disable SNMP SET requests, click **Disabled**.
Read-write community name for permitted SETs	If you have enabled SNMP SET requests, you can set a read-write community name. Setting a community name is similar to setting a password. Only requests from the machines that identify themselves with this community name will be accepted. The community name can be in any alphanumeric format.

Table 21.2 SNMP Settings

Field	Description
Restrict the source of SNMP requests to only the designated hosts or subnets	You can restrict the source of permitted SNMP requests. • To restrict the source of permitted SNMP requests, click **Enabled**. • To permit any source submitting an SNMP request, click **Disabled**.
Hostname or subnet of Network Management System	Specify the DNS hostname or subnet of the machines that can execute GET and SET requests to the managed devices. As with community names, this provides a level of security on SNMP settings. The SNMP agent will only accept requests from the hostname or subnet specified here. To specify a subnet, enter one or more subnetwork address ranges in the form *AddressRange/MaskLength*, where *AddressRange* is an IP address and *MaskLength* is the number of mask bits. Both formats 'NetAddress/NetMask' and 'NetAddress/MaskLength' are supported. Individual hosts can be provided for this, i.e. I.P Address or Hostname. For example, if you enter a range of `192.168.1.0/24` this specifies a subnetwork with address `192.168.1.0` and a subnet mask of `255.255.255.0`. The address range is used to specify the subnet of the designated NMS. Only machines with IP addresses in this range are permitted to execute GET and SET requests on the managed device. Given the example above, the machines with addresses from `192.168.1.1` through `192.168.1.254` can execute SNMP commands on the device. (The address identified by suffix `.0` in a subnetwork range is always reserved for the subnet address, and the address identified by `.255` in the range is always reserved for the broadcast address). As another example, if you enter a range of `10.10.1.128/25`, machines with IP addresses from `10.10.1.129` through `10.10.1.254` can execute SNMP requests on managed devices. In this example, `10.10.1.128` is the network address and `10.10.1.255` is the broadcast address. `126` addresses would be designated.

Table 21.2 SNMP Settings

21.3.1 Configuring SNMP Traps

SNMP Traps facilitate asynchronous communication of messages from SNMP managed devices (like the 9160 G2 Wireless Gateway) to designated hosts. If a Network Management System (NMS) is responsible for monitoring a large number of devices on a network, it is not practical to periodically query every device on the network. By enabling SNMP event traps on the AP, individual devices can send messages directly to SNMP Managers or to other designated hosts on the NMS regarding some network events, such as network interfaces going up or down, clients failing to associate or authenticate with the access point, system power up or down and changes in the network topology..

SNMP traps save on network resources by eliminating redundant SNMP requests.They also make it easier for SNMP Managers to troubleshoot their network. For example, if an SNMP manager is responsible for a large network that supports many devices, and each device has a large number of objects, it is impractical to request information from every object on every device. The optimum solution is for each agent on the managed device to notify the manager of any unusual events. It does this by sending a trap of the event. After receiving the event information, the manager can choose what action, if any, to take.

Field	Description
Community name for traps	Enter the global community string associated with SNMP traps. Traps sent from the device will provide this string as a community name.
Hostname	Enter the DNS hostname of the computer to which you want to send SNMP traps. An example of a DNS hostname is: snmptraps.teklogix.com Since SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. Ensure you select the **Enabled** checkbox beside the appropriate hostname.

Table 21.3 SNMP Trap Settings

21.3.2 Updating SNMP Settings

To update SNMP settings:

1. Navigate to the SNMP tab page.
2. Configure the SNMP settings as required.
3. Click the **Update** button to apply the changes.

THE 9160 G2 AS BASE STATION 22

22.1 Overview

The 9160 G2 Wireless Gateway can function as either a wired or wireless Base Station, or as a Remote Radio Module (RRM), using a radio link and Psion Teklogix proprietary protocols to facilitate communications with the terminals (see “Radio Protocols” on page 220).

As a wired base station, the 9160 G2 can communicate with wireless terminals using Adaptive Polling/Contention Protocol (page 220), and is connected to the network controller over a network.

As a wireless base station, the 9160 G2 communicates with the wired base station and mobile terminals using 802.11 WDS.

As an RRM, the operation and timing of the 9160 G2’s radio link to the terminals is directly controlled by a network controller that uses a timeplexing radio protocol (see “Timeplexing And Cellular Switching”, below). It is connected to the network controller over a network.

Timeplexing And Cellular Switching

There are two methods of operating on the radio link. The first method is called *cellular switching*. It is similar in concept to cellular telephone systems. Here, each base station uses a different radio channel. The terminals monitor the radio link and automatically switch to the channel with best radio reception. This cellular switching capability is transparent to the host.

The second method is called *timeplexing*. Here, all Remote Radio Module (RRM) bases at the site use the same channel. Over a UDP/IP network, a network controller coordinates the polling sequence so that the RRMs do not transmit simultaneously. This timeplexing capability is also transparent to the host. Timeplexing is suited for sites with low transaction rates.

Cellular switching and timeplexing can be combined within one Psion Teklogix system: a site may operate on two or more channels, with several grouped timeplexed bases using each channel, and cellular switching between the channels.

In all of these cases, the operator may move freely throughout the site without loss of communication. The Psion Teklogix system handles channel-switching and handovers between bases without alerting the user.

For operation as a base station or RRM, the parameters in the *Base Station Configuration* pages on the *Configuration Main Menu* screen should be set appropriately, as described in the sections that follow. In addition, the appropriate radio and host parameters must be applied. The radio parameters are found in the *Radio* pages for *Narrow Band* radios, as described in Section 22.3.1. The parameters for the hosts are described in Section 22.5 “Hosts” on page 243.

Note: *The 9160 G2 main parameters should first be set up as described in Chapter 4: “Quick Steps For Setup And Launch” and Chapter 5: “Configuring Basic Settings”. For details on the RF protocols, see the following sections.*

22.2 Radio Protocols

RF protocols allow terminals to communicate with a base station by sharing the use of a radio channel in an efficient way. Psion Teklogix systems use one of two types of RF protocols: the Psion Teklogix Adaptive Polling/Contention protocol or the non-proprietary IEEE 802.11 protocol. When used as a base station or RRM, the 9160 G2 uses the Adaptive Polling/Contention protocol. The 9160 G2 supports simultaneous base station and 802.11 access point operation.

22.2.1 Adaptive Polling/Contention Protocol

The Adaptive Polling/Contention protocol is always used on Narrow Band radio systems with baud rates of up to 19.2 kb/s, and may also be used on Spread Spectrum systems at higher rates.

Terminals operating with this protocol do not transmit unless they receive polls from the 9160 G2. Terminals are generally polled en masse. Following each poll, groups of terminals are assigned response windows in which they may respond to the poll. If a “collision” occurs—more than one terminal attempts to respond in a particular window—the 9160 G2 that is polling divides and reassigns that group until the colliding terminals can respond without a collision.

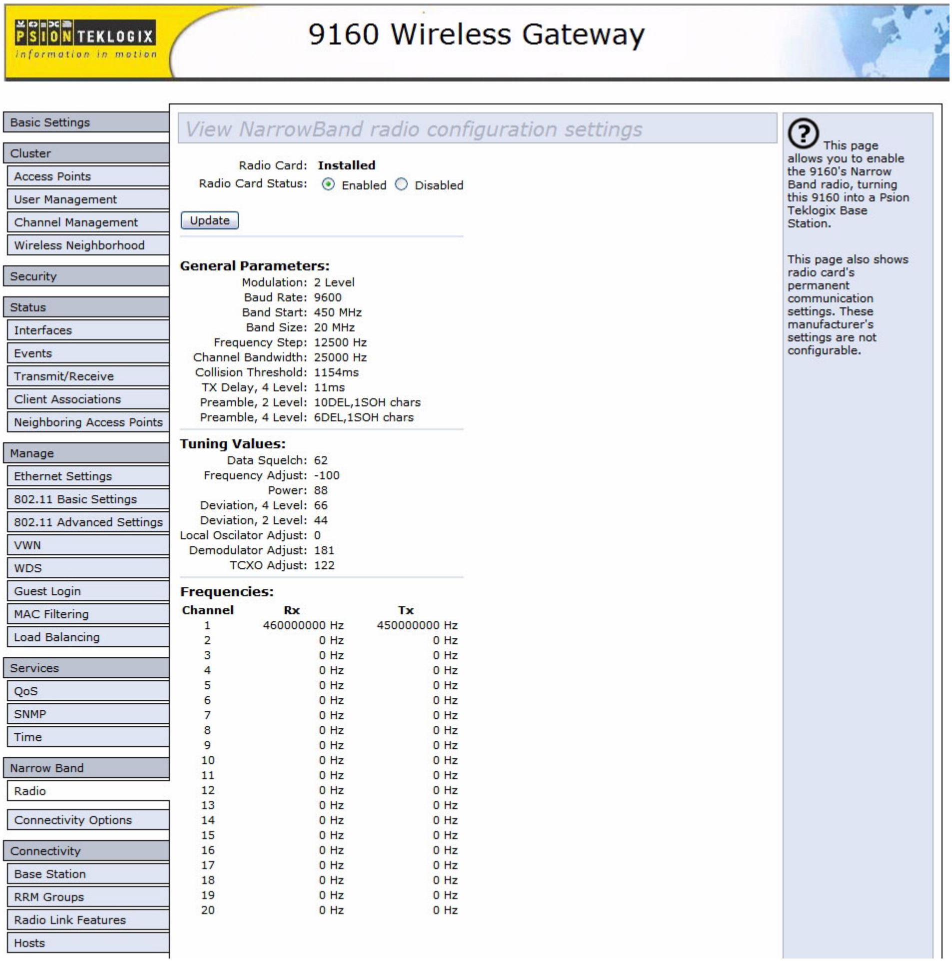
Adaptive features of this protocol allow the response windows to be adjusted to accommodate high or low RF traffic conditions, and to prevent data from being queued too long when a particular terminal has a burst of data to send or receive.

Systems using adaptive polling/contention can use the cellular option so that terminal operators can roam the site, maintaining uninterrupted communication as they pass between coverage areas. If cellular base is not enabled, a “RESET: Press Enter” message appears on the terminal screen each time an operator moves from one base station coverage area to another.

22.3 Narrow Band Menus

22.3.1 Narrow Band Radio Configuration Settings

When you select the *Radio* sub-menu from the *Narrow Band* menu options, the 9160 G2 displays the *Narrow Band Radio Configuration Settings* of the operating mode for which the 9160 G2 is set (base station or RRM). The page displayed allows you to set the status of the 9160 G2, and to retrieve the RA1001A radio card's permanent communications settings.



View NarrowBand radio configuration settings

Radio Card: **Installed**
Radio Card Status: ● Enabled ○ Disabled

General Parameters:

Modulation:	2 Level
Baud Rate:	9600
Band Start:	450 MHz
Band Size:	20 MHz
Frequency Step:	12500 Hz
Channel Bandwidth:	25000 Hz
Collision Threshold:	1154ms
TX Delay, 4 Level:	11ms
Preamble, 2 Level:	10DEL,1SOH chars
Preamble, 4 Level:	6DEL,1SOH chars

Tuning Values:

Data Squelch:	62
Frequency Adjust:	-100
Power:	88
Deviation, 4 Level:	66
Deviation, 2 Level:	44
Local Oscilator Adjust:	0
Demodulator Adjust:	181
TCXO Adjust:	122

Frequencies:

Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

? This page allows you to enable the 9160's Narrow Band radio, turning this 9160 into a Psion Teklogix Base Station.

This page also shows radio card's permanent communication settings. These manufacturer's settings are not configurable.

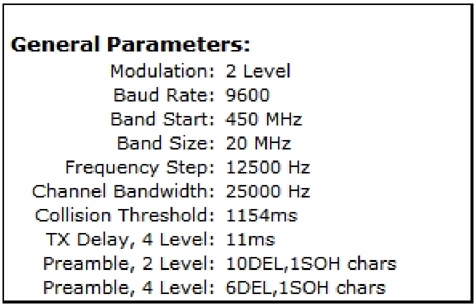
Figure 22.1 Overview Of Narrow Band Radio Settings

Radio Card Status

This parameter **enables** or **disables** the Narrow Band Radio. The card may be **disabled** temporarily when, for testing purposes, it is required that there be no radio interference. Press the **Update** button to initialize the change.

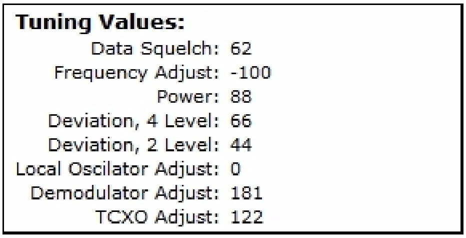
22.3.1.1 RA1001A Radio Parameters

The *Narrow Band Radio Configuration Settings* page displays the *General*, *Frequencies*, and *Tuning Values* parameters for the RA1001A Narrow Band radio. These manufacturer's settings are not configurable. The settings are shown in the following figures.



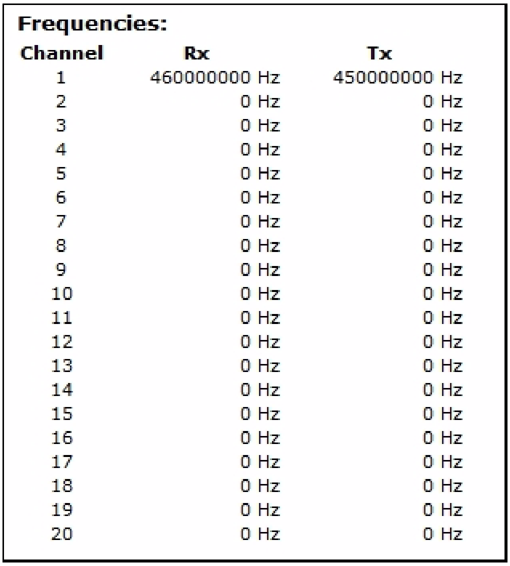
```
General Parameters:
           Modulation:  2 Level
            Baud Rate:  9600
           Band Start:  450 MHz
            Band Size:  20 MHz
       Frequency Step:  12500 Hz
    Channel Bandwidth:  25000 Hz
  Collision Threshold:  1154ms
     TX Delay, 4 Level:  11ms
   Preamble, 2 Level:  10DEL,1SOH chars
   Preamble, 4 Level:  6DEL,1SOH chars
```

Figure 22.2 RA1001A Radio Parameters



```
Tuning Values:
           Data Squelch:  62
       Frequency Adjust:  -100
                  Power:  88
     Deviation, 4 Level:  66
     Deviation, 2 Level:  44
Local Oscilator Adjust:  0
     Demodulator Adjust:  181
            TCXO Adjust:  122
```

Figure 22.3 RA1001A Radio Tuning Values



Frequencies:

Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

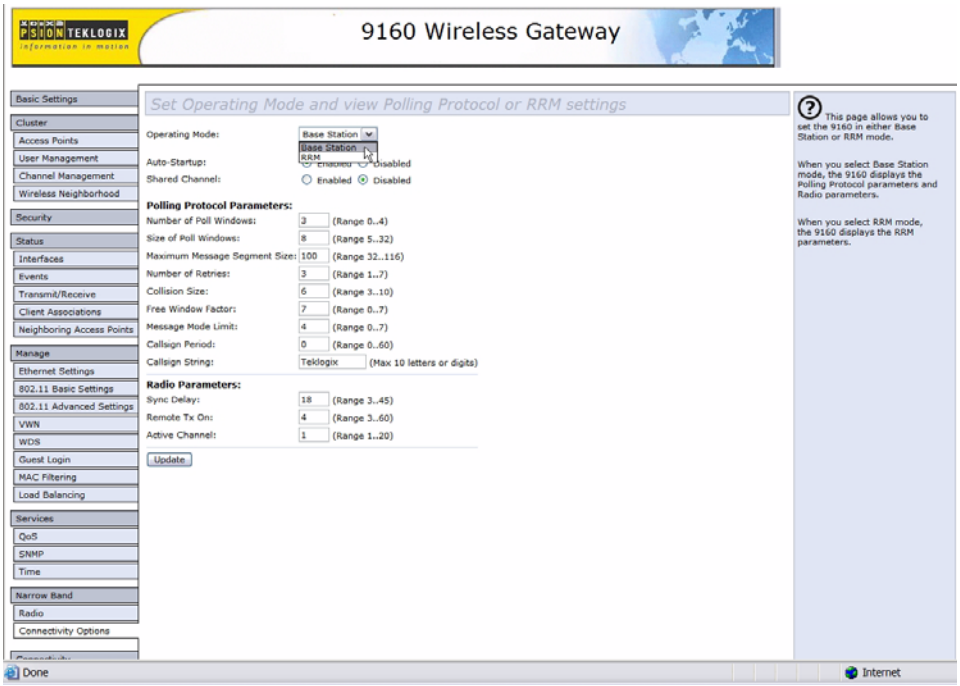
Figure 22.4 RA1001A Radio Frequencies

22.3.2 Connectivity Options

When you select this sub-menu, the page displayed allows you to set the operating options for the 9160 G2 in either base station or RRM mode.

22.3.3 Connectivity Options: Base Station Mode

When you enter the *Connectivity Options* sub-menu for the 9160 G2 set in base station operating mode, the Polling Protocol and Radio Parameters are displayed.



Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode: Base Station (Base Station / RRM)

Auto-Startup: ○ Enabled ○ Disabled

Shared Channel: ○ Enabled ● Disabled

Polling Protocol Parameters:

Number of Poll Windows:	3	(Range 0..4)
Size of Poll Windows:	8	(Range 5..32)
Maximum Message Segment Size:	100	(Range 32..116)
Number of Retries:	3	(Range 1..7)
Collision Size:	6	(Range 3..10)
Free Window Factor:	7	(Range 0..7)
Message Mode Limit:	4	(Range 0..7)
Callsign Period:	0	(Range 0..60)
Callsign String:	Teklogix	(Max 10 letters or digits)

Radio Parameters:

Sync Delay:	18	(Range 3..45)
Remote Tx On:	4	(Range 3..60)
Active Channel:	1	(Range 1..20)

Update

This page allows you to set the 9160 in either Base Station or RRM mode.

When you select Base Station mode, the 9160 displays the Polling Protocol parameters and Radio parameters.

When you select RRM mode, the 9160 displays the RRM parameters.

Operating Mode

This parameter allows you to set the operating mode of the 9160 G2 as **Base Station** or **RRM**.

Auto-Startup

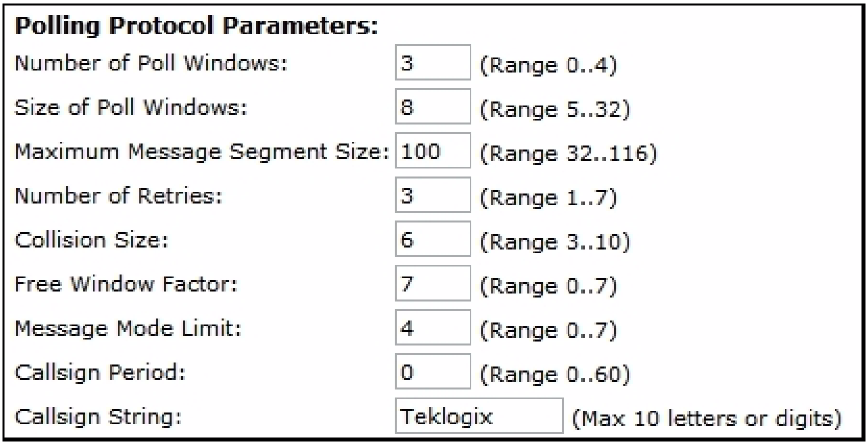
This parameter **enables** polling immediately when the 9160 G2 is rebooted. If *Auto-Startup* is **disabled**, the 9160 G2 will wait until polling is initialized from the network controller.

Shared Channel

Shared Channel is only used in Holland to accommodate government requirements. When **enabled**, it imposes timing restrictions for polling. Every 2 seconds of polling is followed by 0.5 seconds of silence—no polling occurs.

Further, if another carrier is detected on the channel, the 9160 G2 will cease radio transmissions on that channel until the path is clear.

22.3.3.1 Polling Protocol Parameters



Polling Protocol Parameters:

Number of Poll Windows:	3	(Range 0..4)
Size of Poll Windows:	8	(Range 5..32)
Maximum Message Segment Size:	100	(Range 32..116)
Number of Retries:	3	(Range 1..7)
Collision Size:	6	(Range 3..10)
Free Window Factor:	7	(Range 0..7)
Message Mode Limit:	4	(Range 0..7)
Callsign Period:	0	(Range 0..60)
Callsign String:	Teklogix	(Max 10 letters or digits)

Number of Poll Windows

This parameter defines the number of poll windows the 9160 G2 will use. The value assigned to this parameter is dependent on the number of terminals and the radio link protocol used. Table 22.5 indicates how the value assigned to the *Number of Poll Windows* parameter is determined.

Number of Terminals	Minimum # of Windows
1-16	2
17-81	3
82-256	4

Table 22.5 Number Of Poll Windows – Cellular Protocol

Size of Poll Windows

The value assigned to this parameter determines the largest message that can be passed between the 9160 G2 and the terminal in a normal poll window. The window size can be adjusted to accommodate anywhere from **5** to **32** characters.

Larger windows increase the polling period and can increase the response time. Smaller windows increase the number of message and long message polls, and can also increase the response time.

Important: ***In "Cellular" mode, the minimum value for this parameter is 8.***

Maximum Message Segment Size

This parameter determines the largest single message that can be passed *to* a terminal in message mode or *from* a terminal in long message mode. In a 9160 G2 base station, the value entered in this parameter must be greater than or equal to the value entered in the network controller or 9160 G2 mini-controller. The range of this parameter is between 32 and 116 characters. (Longer messages are broken into several packets.) The default value is **100**.

Number of Retries

This parameter determines how many times the 9160 G2 attempts to resend a message if an acknowledgement is not received from the terminal. (These retries do not necessarily occur in consecutive polls because incomplete messages are returned to the bottom of the message queue.) After all retries have been exhausted, the terminal is declared “offline”. The 9160 G2 does not transmit any messages to the terminal until the terminal declares itself “online”. The allowable values range from **1** to **7**.

Collision Size

This parameter reduces the probability that random noise on the radio link will be interpreted as a collision between terminals. Response time increases when the 9160 G2 resolves collisions unnecessarily.

Collision Size places an upper limit on the number of characters that are received prior to the receipt of an error message (CRC, CD lost, etc.). If eight is the value of this parameter, eight or less characters followed by an error message appearing over the radio link are considered noise. If there are more than eight characters, it is considered a collision. Acceptable values range from **3** to **10**.

Free Window Factor

The value entered in this parameter determines if “free window mode” will be used. In free window mode, all terminals that are not assigned any other window can use the free window.

Entering a value of **0** (zero) in this parameter **disables** free window mode. Increasing the value of this parameter increases the likelihood of a message being transmitted in the free window.

Message Mode Limit

This parameter defines an upper limit to the number of messages that must be queued for transmission before message mode polling starts. Accepted values range from **0** to **7**, where **0 disables** message mode.

Note: *The number of terminals and past events are also part of the algorithm that determines whether or not to start message mode.*

Callsign Period

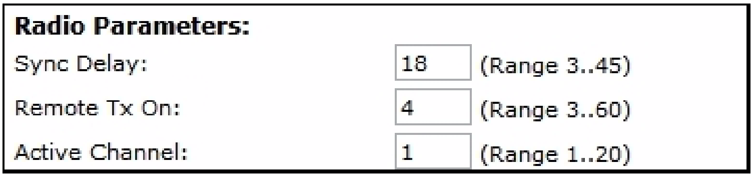
A call sign is periodically transmitted as an audible Morse code signal. This parameter specifies the interval in minutes between call sign transmissions. Acceptable values range from **0** to **60**. The federal agencies, Industry Canada and the Federal Communications Commission in the United States, require that each system transmit its own identification call sign every 15 minutes.

In countries where a call sign is not required, setting this parameter to **0** prevents the transmission of any call signs, allowing for shorter poll time-outs in terminals and faster channel switching.

Callsign String

This string can be a maximum of **10** characters long. All characters are either numbers or letters. The prefix “DE” (from) is added to the beginning of the transmitted call sign.

22.3.3.2 Radio Parameters



Radio Parameters:

Sync Delay:	18	(Range 3..45)
Remote Tx On:	4	(Range 3..60)
Active Channel:	1	(Range 1..20)

Sync Delay

Important: ***This parameter should not be changed from its factory setting without a clear understanding of the timing of the radio protocol.***

Sync Delay specifies the delay between the time of the base station transmission and the first response window, measured in character times. The value assigned to this parameter must be compatible with other base stations and terminals in the system. The RA1001A radio is available in either two level or four level modulation, providing baud rates of 4800 bps and 9600 bps, or 9600 bps and 19200 bps, respectively.

The default setting for a two level modulation narrow band radio, operating at 9600 baud, is **23**.

The default setting for a four level modulation narrow band radio, operating at 19200 baud, is **31**.

Remote Txon

Remote Txon accommodates the turn-on time of the radio in terminals (remotes). It specifies the number of fill characters sent to the radio before real data is output. Since this parameter is based on character times, the number is dependent on the radio link baud rate.

The value assigned to the *Remote Txon* parameter must be consistent across all terminals and base station equipment. The allowable value range is **3** to **60**.

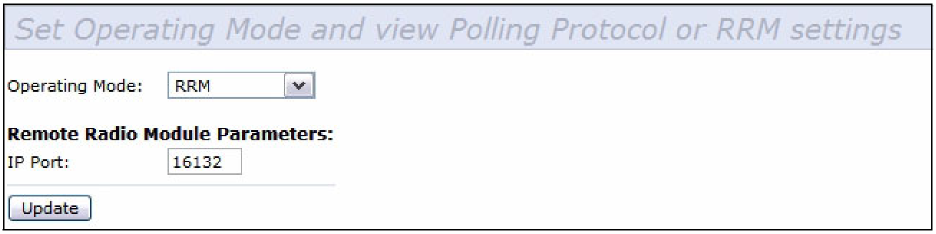
Important: ***This parameter should not be changed from its factory setting without an understanding of the timing of the radio protocol.***

Active Channel

This parameter determines the operating radio channel of the 9160 G2. This makes the channel available for channel searching by the terminals. The channel selected must be one of those that have been configured with frequencies, as indicated on the *Narrow Band Radio Configuration Settings* page. See Figure 22.4 on page 223 for the list of associated channels and frequencies.

22.3.4 Connectivity Options: RRM Mode

When you enter the *Connectivity Options* sub-menu for the 9160 G2 set in RRM operating mode, the 9160 G2 displays the RRM parameters.



Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode: RRM

Remote Radio Module Parameters:

IP Port: 16132

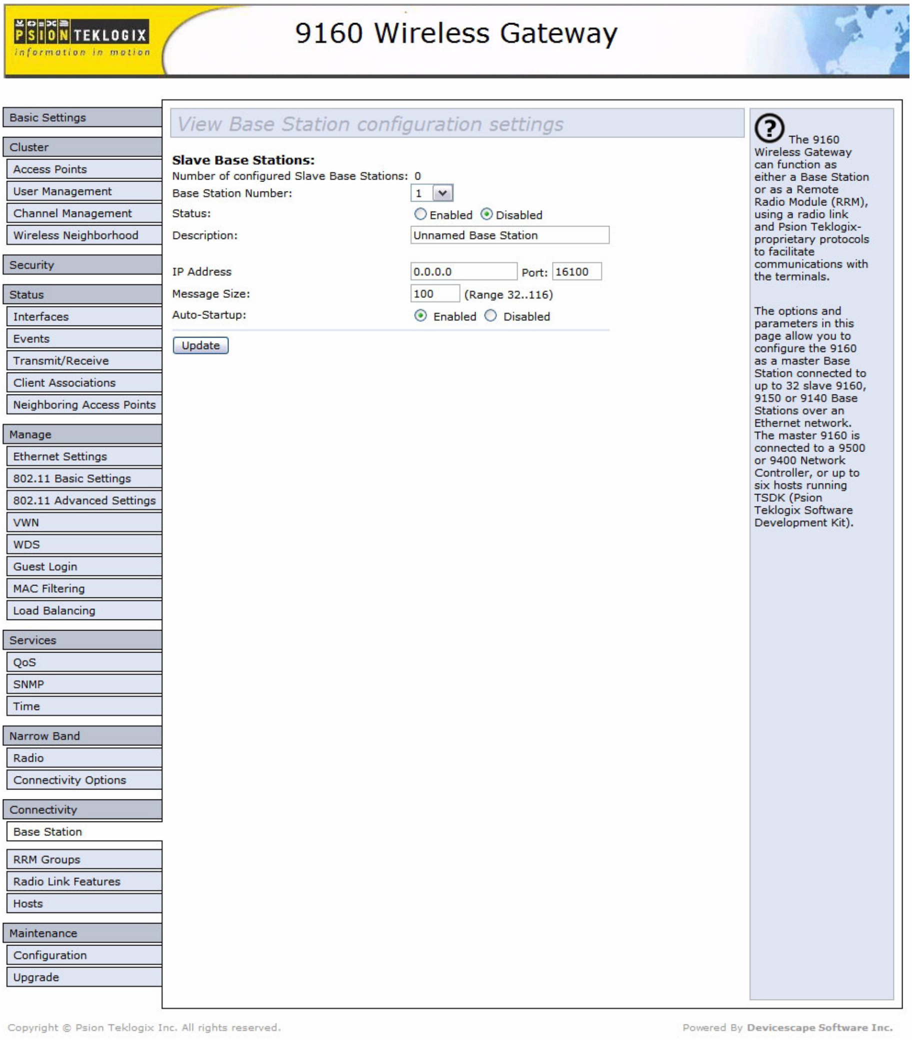
IP Port

This parameter allows you to enter the port number of the 9160 G2. The port number can range from **1024** to **32767**.

Important: ***The port number entered here must match the port number entered for this 9160 G2 in the network controller's RRM configuration.***

22.4 Connectivity Menus

The 9160 G2 Wireless Gateway can operate as a base station or remote radio module (RRM), facilitating the communications between terminals and wireless base stations and a network controller (Psion Teklogix 9500 Network Controller or 9160 G2 Wireless Gateway), using a range of host platforms. Alternatively, the network controller can be a host running a Psion Teklogix SDK (handler). The 9160 G2 can also act as a slave base station to another 9160 G2 on the network.



View Base Station configuration settings

Slave Base Stations:

Number of configured Slave Base Stations: 0

Base Station Number: 1

Status: ○ Enabled ● Disabled

Description: Unnamed Base Station

IP Address: 0.0.0.0 Port: 16100

Message Size: 100 (Range 32..116)

Auto-Startup: ● Enabled ○ Disabled

The 9160 Wireless Gateway can function as either a Base Station or as a Remote Radio Module (RRM), using a radio link and Psion Teklogix-proprietary protocols to facilitate communications with the terminals.

The options and parameters in this page allow you to configure the 9160 as a master Base Station connected to up to 32 slave 9160, 9150 or 9140 Base Stations over an Ethernet network. The master 9160 is connected to a 9500 or 9400 Network Controller, or up to six hosts running TSDK (Psion Teklogix Software Development Kit).

Copyright © Psion Teklogix Inc. All rights reserved.

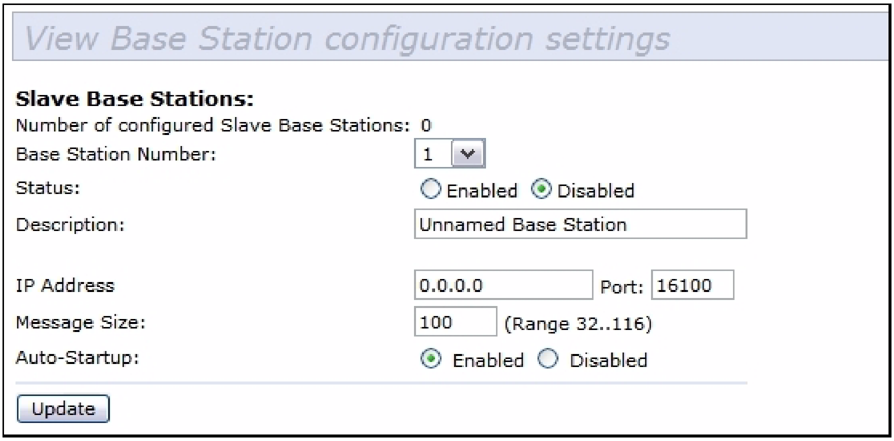
Powered By Devicescape Software Inc.

22.4.1 Base Station Configuration Settings

Base stations communicate over the radio link using Psion Teklogix proprietary protocols. Base stations can be connected to network controllers using TCP/IP over Ethernet networks. As a base station communicating with terminals through a radio link, the 9160 G2 uses the Adaptive Polling/Contention RF protocol (see *'Radio Protocols'* on page 220 for details on the protocols). The 9160 G2 controls the radio link's operation and timing. Each base station uses a different radio channel, and terminals use cellular switching to roam between stations.

The options and parameters on the following pages allow you to configure the 9160 G2 as a master base station connected to up to 32 slave 9160 G2 base stations over an Ethernet network. The master 9160 G2 is connected to a 9500 Network Controller, or up to six hosts running the Psion Teklogix Software Development Kit. The *Base Station* option under *Connectivity*, will enable you to add a new slave base station to the system or change the parameters on an existing slave base station.

Pressing the **Update** button will save your settings.



View Base Station configuration settings

Slave Base Stations:

Number of configured Slave Base Stations: 0

Base Station Number: 1

Status: ○ Enabled ● Disabled

Description: Unnamed Base Station

IP Address 0.0.0.0 Port: 16100

Message Size: 100 (Range 32..116)

Auto-Startup: ● Enabled ○ Disabled

Number of Configured Slave Base Stations

You can configure up to **32** slave 9160 G2 base stations.

Base Station Number

Each slave base station must be assigned a number.

Status

This parameter **enables** or **disables** this slave base station.

Description

The name entered in this parameter is used as an alternate way of identifying the IP address of a slave base station.

IP Address

This parameter provides the corresponding IP address for the slave base station. The *IP Address* **must be a unique value** so that each slave base station can be identified on the network.

The acceptable value ranges from **0.0.0.0** to **239.255.255.255**.

The default value for the IP port is **16100**.

Message Size

Message Size determines the largest single message that can be passed to a terminal. The range of this parameter is between **32** and **380** characters. (Longer messages are broken into several packets.)

For polling protocol base stations, the upper limit is **116**.

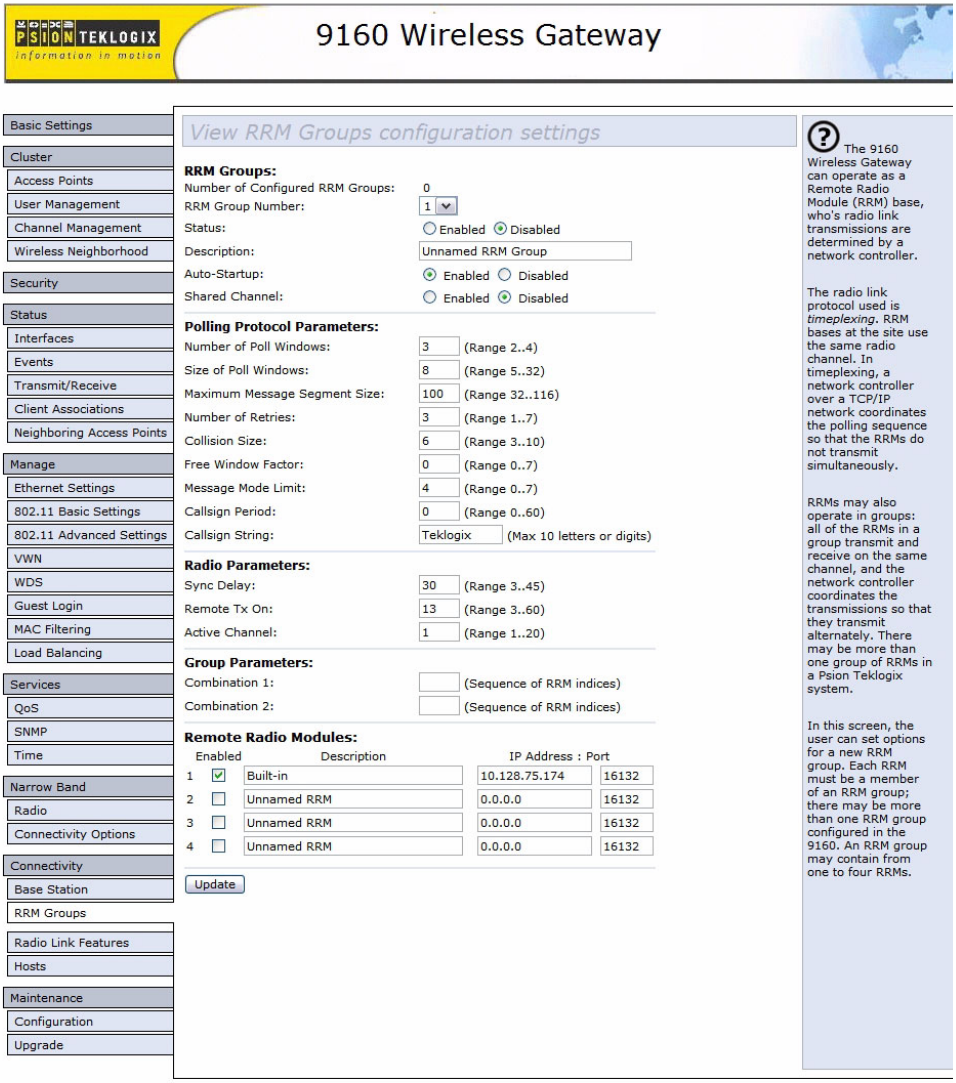
Auto-Startup

When this parameter is **enabled**, the slave base stations will start polling when the **master 9160 G2** boots up. When *Auto-Startup* is **disabled**, the base stations will not start polling until they receive a *start polling* command from the **host**.

22.4.2 RRM Groups Configuration Settings

While the 9160 G2 can operate as a Remote Radio Module (RRM, see “Connectivity Options: RRM Mode” on page 229), it can also control other RRMs. For a 9160 G2 to control RRMs, RRM groups must be configured. Once an RRM group has been defined, from one to four RRMs can be members of a group.

All RRMs in a group operate on the same radio channel. The 9160 G2 coordinates the transmissions of all the RRMs in a group (for this reason, the controlling 9160 G2 is sometimes referred to as the “Timeplexing Master”).



View RRM Groups configuration settings

RRM Groups:

Number of Configured RRM Groups:	0
RRM Group Number:	1
Status:	○ Enabled ● Disabled
Description:	Unnamed RRM Group
Auto-Startup:	● Enabled ○ Disabled
Shared Channel:	○ Enabled ● Disabled

Polling Protocol Parameters:

Number of Poll Windows:	3	(Range 2..4)
Size of Poll Windows:	8	(Range 5..32)
Maximum Message Segment Size:	100	(Range 32..116)
Number of Retries:	3	(Range 1..7)
Collision Size:	6	(Range 3..10)
Free Window Factor:	0	(Range 0..7)
Message Mode Limit:	4	(Range 0..7)
Callsign Period:	0	(Range 0..60)
Callsign String:	Teklogix	(Max 10 letters or digits)

Radio Parameters:

Sync Delay:	30	(Range 3..45)
Remote Tx On:	13	(Range 3..60)
Active Channel:	1	(Range 1..20)

Group Parameters:

Combination 1:		(Sequence of RRM indices)
Combination 2:		(Sequence of RRM indices)

Remote Radio Modules:

	Enabled	Description	IP Address	: Port
1	☑	Built-in	10.128.75.174	16132
2	□	Unnamed RRM	0.0.0.0	16132
3	□	Unnamed RRM	0.0.0.0	16132
4	□	Unnamed RRM	0.0.0.0	16132

Update

The 9160 Wireless Gateway can operate as a Remote Radio Module (RRM) base, who's radio link transmissions are determined by a network controller.

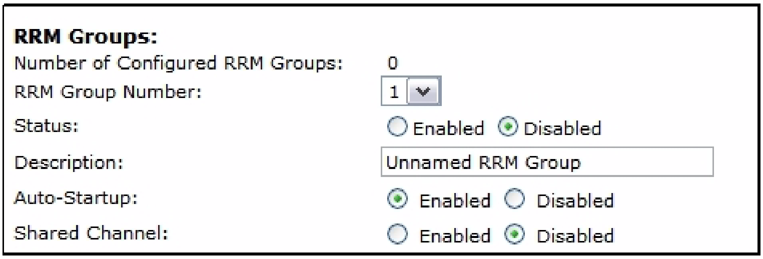
The radio link protocol used is *timeplexing*. RRM bases at the site use the same radio channel. In timeplexing, a network controller over a TCP/IP network coordinates the polling sequence so that the RRMs do not transmit simultaneously.

RRMs may also operate in groups: all of the RRMs in a group transmit and receive on the same channel, and the network controller coordinates the transmissions so that they transmit alternately. There may be more than one group of RRMs in a Psion Teklogix system.

In this screen, the user can set options for a new RRM group. Each RRM must be a member of an RRM group; there may be more than one RRM group configured in the 9160. An RRM group may contain from one to four RRMs.

Figure 22.6 Overview Of RRM Groups Configuration Settings

22.4.2.1 RRM Groups



RRM Groups:

Number of Configured RRM Groups:	0
RRM Group Number:	1
Status:	○ Enabled ● Disabled
Description:	Unnamed RRM Group
Auto-Startup:	● Enabled ○ Disabled
Shared Channel:	○ Enabled ● Disabled

In this screen the user can set options for a new RRM group. Each RRM must be a member of an RRM group; there may be more than one RRM group configured in the 9160 G2. An RRM group may contain from one to four RRMs.

This screen is very similar to the one in “Connectivity Options: Base Station Mode” on page 223, the difference being that the parameters configured in those radio menus apply to the RA1001A radio resident in the 9160 G2, while the parameters configured here apply to the other, remote 9160 G2s (the RRMs).

Number of Configured RRM Groups

Displays the number of RRM groups configured in this 9160 G2.

RRM Group Number

Each RRM Group must be assigned an identifying number.

Status

This parameter **enables** or **disables** this RRM group.

Description

This textbox allows the user to enter a name for the new RRM group. The value is any text string. The default is **Unnamed RRM Group**.

Auto-Startup

When this parameter is **enabled**, the 9160 G2 establishes communication with the RRMs in this RRM group when it boots, and starts polling automatically. When *Auto-Startup* is **disabled**, the 9160 G2 establishes communication with the RRMs in this group when it boots, but does not start polling in this RRM group until a start polling command is received from the host. Polling starts if at least one of the RRMs in the RRM group is operating when the 9160 G2 boots.

Shared Channel

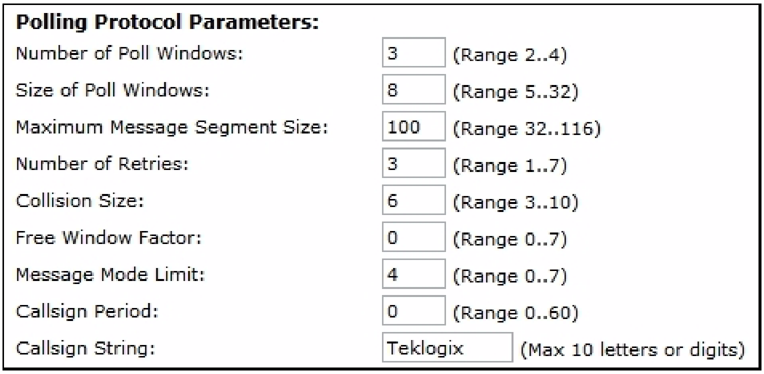
If this parameter is **enabled**, the 9160 G2 checks for other traffic on the radio channel used by this RRM group, before polling.

If this parameter is **disabled**, the 9160 G2 assumes that it has exclusive use of the radio channel for this RRM group, and polls without checking for radio traffic.

This parameter is required for systems installed in the Netherlands.

22.4.2.2 Polling Protocol Parameters

Warning: ***These parameters are pre-configured for your system, and should not be changed without a proper understanding of how they affect the radio link.***



Polling Protocol Parameters:

Number of Poll Windows:	3	(Range 2..4)
Size of Poll Windows:	8	(Range 5..32)
Maximum Message Segment Size:	100	(Range 32..116)
Number of Retries:	3	(Range 1..7)
Collision Size:	6	(Range 3..10)
Free Window Factor:	0	(Range 0..7)
Message Mode Limit:	4	(Range 0..7)
Callsign Period:	0	(Range 0..60)
Callsign String:	Teklogix	(Max 10 letters or digits)

Number of Poll Windows

This textbox allows the user to specify the number of poll windows in which the RRM listens for terminal responses after sending a poll. The allowable values range from **2 to 4**. The default value is **3**.

Size of Poll Windows

This textbox allows the user to specify the size of the poll windows in which the RRMs of this RRM group listen for terminal replies. The allowable values range from **5 to 32**. The default value is **8**.

Maximum Message Segment Size

This textbox allows the user to specify the size of the largest message segment, in bytes, that will be sent over the Psion Teklogix radio network. Larger messages are broken into parts. The allowable values range from **32 to 116**. The default value is **100**.

Number of Retries

This textbox allows the user to specify the number of times the RRM retransmits a message to a terminal, after receiving no acknowledgement from the terminal, before it declares the terminal offline. The allowable values range from **1 to 7**. The default value is **3**.

Collision Size

This textbox allows the user to specify the smallest number of characters of noise received by the RRM, that will be interpreted as interfering transmissions from Psion Teklogix equipment. When this threshold is exceeded, the RRM starts collision resolution. The allowable values range from **3 to 10**. The default value is **6**.

Free Window Factor

This textbox allows the user to specify the probability that the RRM will include a free window in its poll, during which any terminal may transmit. The allowable values range from **0 to 7**. The default value is **0**.

Message Mode Limit

This textbox allows the user to specify the probability of including a message-mode poll in its poll transmission. The allowable values range from **0 to 7**. The default value is **4**.

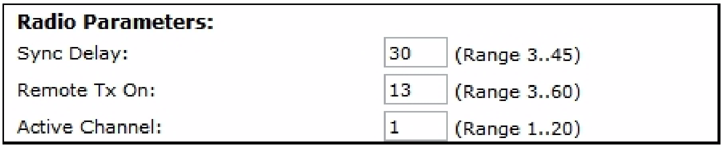
Callsign Period

This textbox allows the user to specify the amount of time between transmissions of the callsign. This parameter is in minutes. A value of 0 (zero) indicates that no callsign is transmitted. The allowable values range from **0 to 60**. The default value is **0**.

Callsign String

This textbox allows the user to specify the text to be transmitted as the RRM's callsign. The text is transmitted as Morse code. The default value is **Teklogix**.

22.4.2.3 Radio Parameters



Radio Parameters:

Sync Delay: 30 (Range 3..45)

Remote Tx On: 13 (Range 3..60)

Active Channel: 1 (Range 1..20)

Because some of the radio parameters are identical for a given group of timeplexed RRMs, they may be configured by the user once on the 9160 G2; the 9160 G2 then passes them to the RRMs in the group. These parameters include the synchronization delay (*Sync Delay*), the remote transmit on-time (*Remote Txon*), and the channel number to be used (*Active Channel*).

Although the RA1001A narrow band radio in each RRM in the group is configured separately, the 9160 G2 assumes they will be configured identically. To ensure this, the 9160 G2 looks at certain parameters returned by each of the RRMs. These parameters include the radio baud rate and the transmit-on time.

These parameters are compared against the values returned by other RRMs within the same group. Error messages are displayed should these values not match, but the worst case value is chosen for use.

Warning: ***These parameters are pre-configured for your system, and should not be changed without a proper understanding of how they affect the radio link.***

Sync Delay

This textbox allows the user to specify the number of delay characters inserted between the RRM's transmission and the first response window. The allowable values range from **3 to 45**. The default value is **30**.

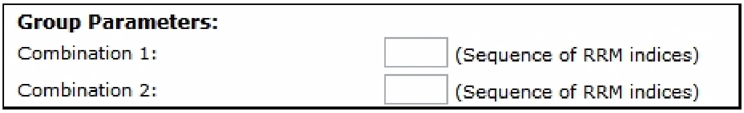
Remote Txon

This textbox allows the user to specify the number of fill characters sent by the terminal radios before the terminals send message data. The allowable values range from **3 to 60**. The default value is **13**.

Active Channel

This textbox allows the user to specify the radio channel to be used by all the RRMs in the RRM group. The allowable values range from **1 to 20**. The default value is **1**.

22.4.2.4 Group Parameters



Group Parameters:

Combination 1:		(Sequence of RRM indices)
Combination 2:		(Sequence of RRM indices)

Combination

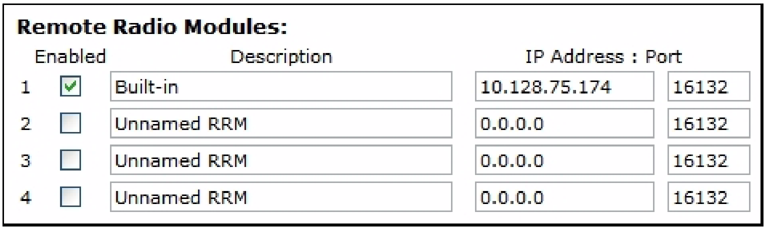
These textboxes allow the user to specify RRM subgroups called *combinations*. If the coverage areas of two or more of the RRMs in this RRM group do not overlap, the non-overlapping RRMs may poll at the same time. This improves system response time and reduces the amount of signalling on the network. RRMs that are not assigned to combinations poll individually, after the combinations poll.

As an example, if the RRM group has 3 RRMs, and RRMs 1 and 3 don't overlap, RRMs 1 and 3 may be placed in one subgroup (*Combination 1*). They will then poll simultaneously. RRM 2 may be placed in another subgroup (*Combination 2*). Polling alternates between the two subgroups.

To configure a combination, place the numbers of the RRMs in the textbox for that combination. The numbers correspond to the numbers of the RRMs named in the RRM list on the *Remote Radio Modules* menu (see page 238). For instance, “13” in the textbox for *Combination 1* places RRMs 1 and 3 in that subgroup.

Note: *When configuring RRM combinations, make sure the configured RRMs are sequential, and are not missing numbers, which can happen when RRMs are deleted and added. The combinations use the RRMs in the order that they appear in the list, not how they are numbered in the list.*

22.4.2.5 Remote Radio Modules



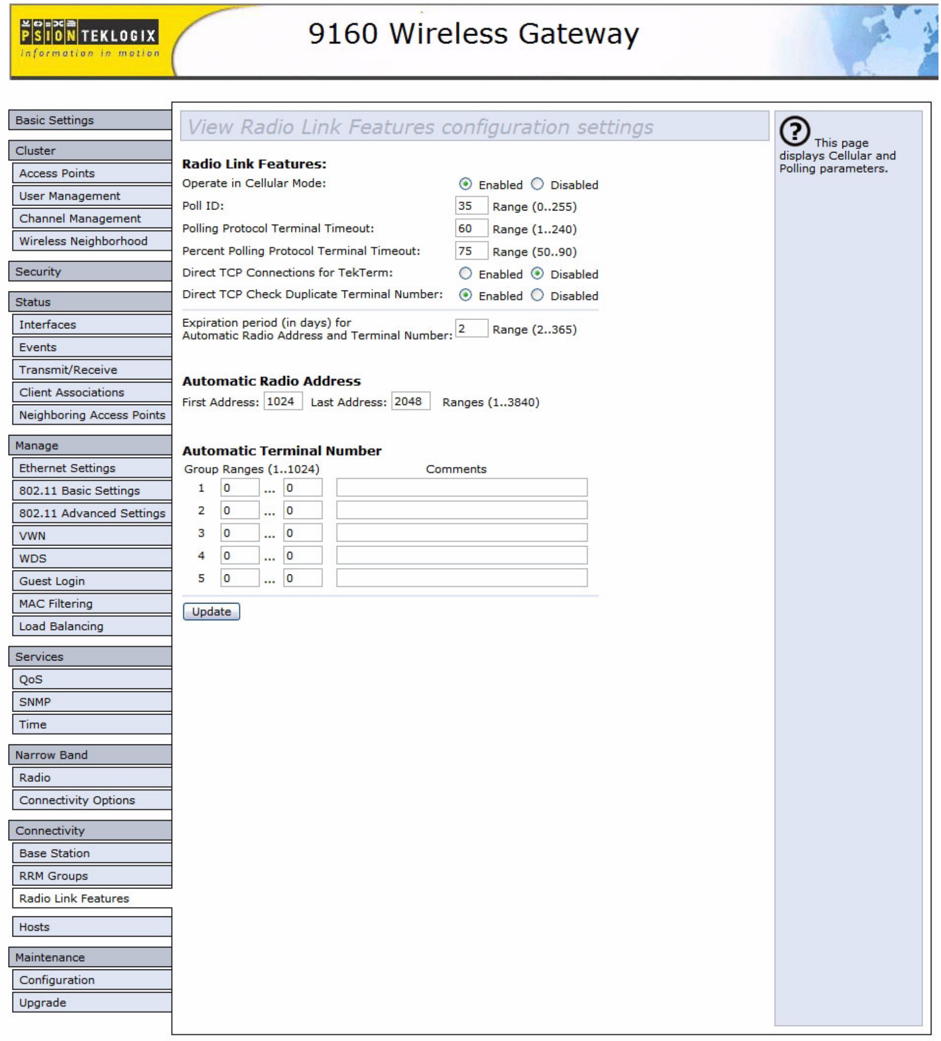
Remote Radio Modules:

	Enabled	Description	IP Address : Port	
1	☑	Built-in	10.128.75.174	16132
2	☐	Unnamed RRM	0.0.0.0	16132
3	☐	Unnamed RRM	0.0.0.0	16132
4	☐	Unnamed RRM	0.0.0.0	16132

This menu displays the RRMs that comprise this RRM Group, including each Description, IP address, and Port number as set in the *Connectivity Options* sub-menu for the 9160 G2s set in RRM operating mode (see “Connectivity Options: RRM Mode” on page 229). Each RRM may be enabled or disabled from this menu.

22.4.3 Radio Link Features Configuration Settings

From the *Connectivity* options list, entering *Radio Link Features* will open the configuration settings page for the polling and cellular parameters.



View Radio Link Features configuration settings

This page displays Cellular and Polling parameters.

Radio Link Features:

Operate in Cellular Mode: ● Enabled ○ Disabled

Poll ID: 35 Range (0..255)

Polling Protocol Terminal Timeout: 60 Range (1..240)

Percent Polling Protocol Terminal Timeout: 75 Range (50..90)

Direct TCP Connections for TekTerm: ○ Enabled ● Disabled

Direct TCP Check Duplicate Terminal Number: ● Enabled ○ Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number: 2 Range (2..365)

Automatic Radio Address

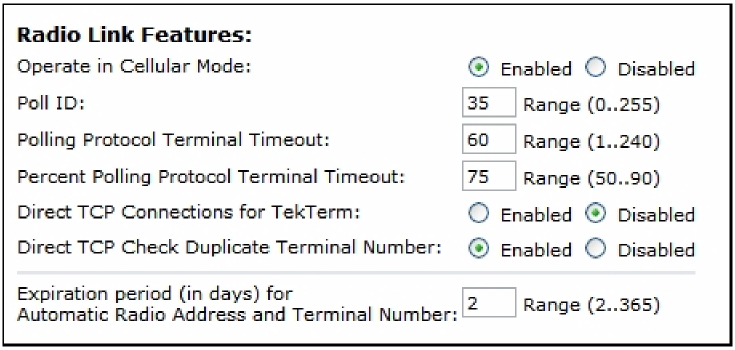
First Address: 1024 Last Address: 2048 Ranges (1..3840)

Automatic Terminal Number

Group Ranges (1..1024)				Comments
1	0	...	0	
2	0	...	0	
3	0	...	0	
4	0	...	0	
5	0	...	0	

Figure 22.7 Overview Of Radio Link Features Configuration Settings

22.4.3.1 Radio Link Features



Radio Link Features:

Operate in Cellular Mode: ● Enabled ○ Disabled

Poll ID: 35 Range (0..255)

Polling Protocol Terminal Timeout: 60 Range (1..240)

Percent Polling Protocol Terminal Timeout: 75 Range (50..90)

Direct TCP Connections for TekTerm: ○ Enabled ● Disabled

Direct TCP Check Duplicate Terminal Number: ● Enabled ○ Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number: 2 Range (2..365)

Operate in Cellular Mode

To operate as a cellular base station, this parameter should be **enabled**.

Note: *The 9500 Network Controller must also be set to cellular mode.*

Poll ID

In Adaptive Polling/Contention protocol for narrow band radios, *Poll ID* is used to assign a unique address to each base station. As the terminals move from one base station to another, this address is transmitted by the base stations to the terminals, identifying each 9160 G2 in a multiple base station system.

Polling Protocol Terminal Timeout

This parameter determines the time in minutes that a terminal can be inactive before the 9160 G2 declares it offline. Before this happens, the terminal will be declared offline by the *Percent Polling Protocol Terminal Timeout* parameter (see below).

After the terminal is removed from the system, it will need to re-initialize in order to communicate with the 9160 G2. This parameter reduces the overhead on the radio link caused when terminals which are not communicating are supported. The allowable values range from **1** to **240**.

Percent Polling Protocol Terminal Timeout

This parameter determines the time that a terminal is allowed to be inactive before the 9160 G2 declares it offline. This time is expressed as a percentage of the *Polling Protocol Terminal Timeout* parameter (see above). For example, if the *Polling Pro-*

tocol Terminal Timeout is 60, and this parameter is set to 75%, then the timeout would be 60 min x 75% = 45 minutes.

An offline terminal is still considered part of the system. Messages to offline terminals are queued at the 9160 G2. The terminal remains offline until it transmits an online message. Values for this parameter range from **50** to **90**.

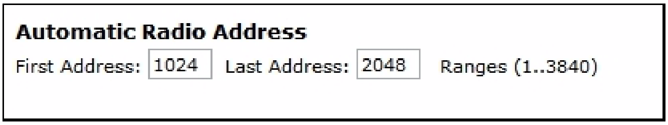
Direct TCP Connections for TekTerm

Enabling this parameter allows the *TekTerm* program resident in Psion Teklogix terminals to connect directly to the 9160 G2, when it is acting as a base station to a host via TCP/IP.

Direct TCP Check Duplicate Terminal Number

When this parameter is enabled, the 9160 G2 will reject Direct TCP terminals which try to connect using a terminal number already in use by another terminal. When disabled, the most recent terminal to connect will take precedence over the other terminals using the same terminal number.

22.4.3.2 Automatic Radio Address



Automatic Radio Address

First Address: 1024 Last Address: 2048 Ranges (1..3840)

Each Psion Teklogix terminal using the radio link has a unique radio address number, which can be assigned automatically by the 9160 G2 by enabling this parameter.

To **enable** this parameter, the values for the first and last radio address numbers must lie between **1** and **3840**. The default values for the range are **1024 ... 2084**. To **disable** the parameter, set the values to **0**.

Notes: *When enabling this parameter:*

1. Direct TCP Connections for TekTerm *must be disabled (see page 241).*
2. *The* Auto ID *parameter in the terminal must be enabled in order for the radio address to be automatically assigned.*

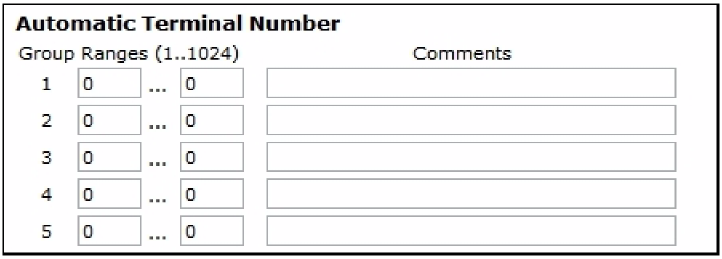
Expiration Period

This parameter dictates how long, in days, a particular radio address or terminal number should be inactive, before the 9160 G2 declares it to be “expired”. An expired address or terminal number may be reassigned to another radio or session.

Note: *For this feature, it is recommended that you enable SNTP and to have an SNTP server available for accurate expiration times.*

22.4.3.3 Automatic Terminal Number

A terminal number is assigned for every application session created in a terminal. This number helps to uniquely identify all transmissions to and from that session.



Automatic Terminal Number

Group Ranges (1..1024)				Comments
1	0	...	0	
2	0	...	0	
3	0	...	0	
4	0	...	0	
5	0	...	0	

Terminal numbers can be assigned automatically to application sessions. The controller also provides a group number for use with TESS and ANSI sessions. Up to five groups of terminal sessions can be defined, and each group can be given a different range of terminal numbers for automatic assignment. These ranges may not overlap between groups.

These groups apply to TESS and ANSI sessions only. In the terminal, TESS or ANSI terminal applications specify which group they belong to, and use the Automatic Terminal Number assignment range that belongs to that group.

All other session types assume an Automatic Terminal Number assignment range of 1 to 3840, and do not use the “group” parameter. Non-ANSI and non-TESS emulations that use Automatic Terminal Number assignment (for example, Remote Sockets) must have their terminal range set starting from 1, and this range must be large enough to accommodate all terminals.

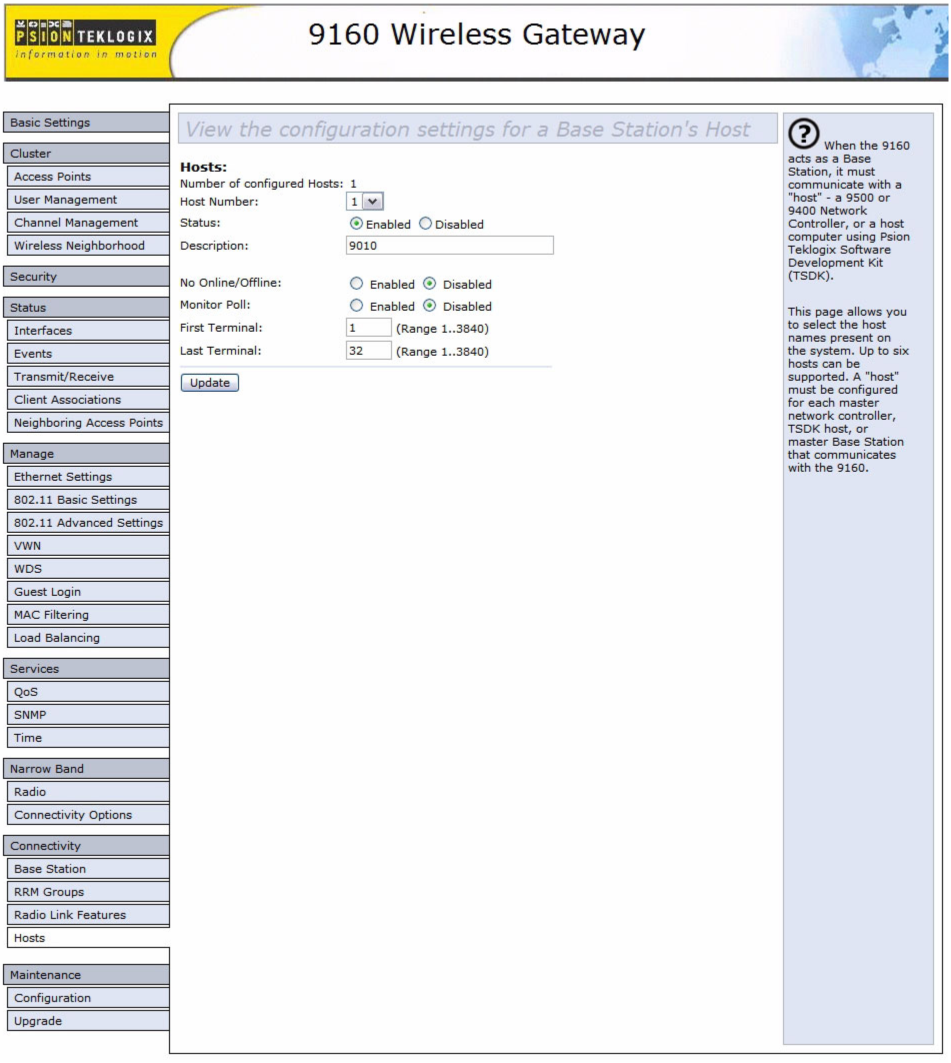
The *Radio Link Features* screen provides several parameters for each Automatic Terminal Number group: a range specified by a lower terminal number and an upper terminal number, and a comment. The comment is a string of ASCII text that can be used to describe the group.

Notes: *When enabling Automatic Terminal Number:*

1. Direct TCP Connections for TekTerm *must be disabled (see page 241).*
2. *The* Auto Session *parameter in the terminal must be enabled in order for the terminal session number to be automatically assigned.*

22.5 Hosts

When the 9160 G2 acts as a base station, it must communicate with a “host”—a 9500 Network Controller, or a host computer using a Psion Teklogix Software Development Kit (SDK). Therefore each master network controller, SDK host, or master base station that communicates with the 9160 G2 must be configured as a host. The *Hosts* page of the *Connectivity* options shows the description of the host chosen from the drop-down list (see Figure 22.8 on page 244).



View the configuration settings for a Base Station's Host

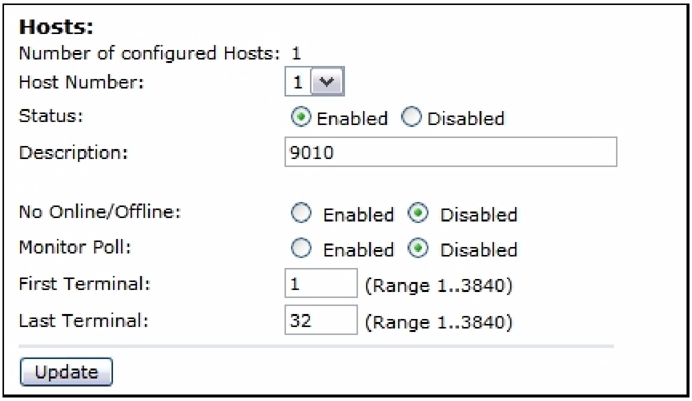
Hosts:
Number of configured Hosts: 1
Host Number: 1
Status: ● Enabled ○ Disabled
Description: 9010

No Online/Offline: ○ Enabled ● Disabled
Monitor Poll: ○ Enabled ● Disabled
First Terminal: 1 (Range 1..3840)
Last Terminal: 32 (Range 1..3840)

When the 9160 acts as a Base Station, it must communicate with a "host" - a 9500 or 9400 Network Controller, or a host computer using Psion Teklogix Software Development Kit (TSDK).

This page allows you to select the host names present on the system. Up to six hosts can be supported. A "host" must be configured for each master network controller, TSDK host, or master Base Station that communicates with the 9160.

Figure 22.8 Overview Of Base Station's Host Configuration Settings



Hosts:

Number of configured Hosts: 1

Host Number: 1

Status: ● Enabled ○ Disabled

Description: 9010

No Online/Offline: ○ Enabled ● Disabled

Monitor Poll: ○ Enabled ● Disabled

First Terminal: 1 (Range 1..3840)

Last Terminal: 32 (Range 1..3840)

Number Of Configured Hosts

The *Hosts* page of the *Connectivity* options shows the number of hosts configured on the system. Up to six hosts can be supported.

Host Number

This parameter indicates the assigned host number. Choosing the **Host Number** from the drop-down list displays the parameters that can be modified or deleted for that host. New hosts can be added by selecting an unassigned number and configuring the parameters for it.

The host number also appears on the RF terminal when switching between hosts in a multiple-host environment.

Status

The Status must be **Enabled** for terminals to communicate with this host.

Description

This textbox allows you to name the protocol used by the host. Protocols are the methods by which terminals communicate with host computers over various physical media such as Ethernet and radio-link connections.

When the 9160 G2 functions as a base station, it communicates with a **9010/ TCP/IP** host using a network connection. The 9010 protocol is a proprietary asynchronous protocol developed by Psion Teklogix which uses TESS (Teklogix Screen Subsystem) or ANSI data streams to communicate with terminals. For detailed information, please refer to the appropriate *Psion Teklogix User Manual* for: *9500 Network Controller, SDK, TESS* or *ANSI*.

No Online/Offline

If this parameter is **Enabled**, the 9160 G2 base station **does not** notify the host if the status of a terminal changes between offline and online. If this parameter is **Disabled**, the 9160 G2 **does** notify the host regarding any terminal status changes. The default for this parameter is **Disabled**.

Monitor Poll

Hosts usually send messages or null polls to the 9160 G2 within a period of approximately 40 seconds. If the parameter is **enabled**, the 9160 G2 base station monitors messages and polls from this host; if it does not receive a message or poll within 40 seconds, it closes the connection. The default for this parameter is **disabled**.

First Terminal/Last Terminal

The values entered in these parameters designate the first and last terminals in the range of terminals that will communicate with the host. These terminal numbers are mapped to this particular host. Terminal numbers may range from **1** to **3840**.

NETWORK TIME PROTOCOL SERVER 23

The *Network Time Protocol* (***NTP***) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

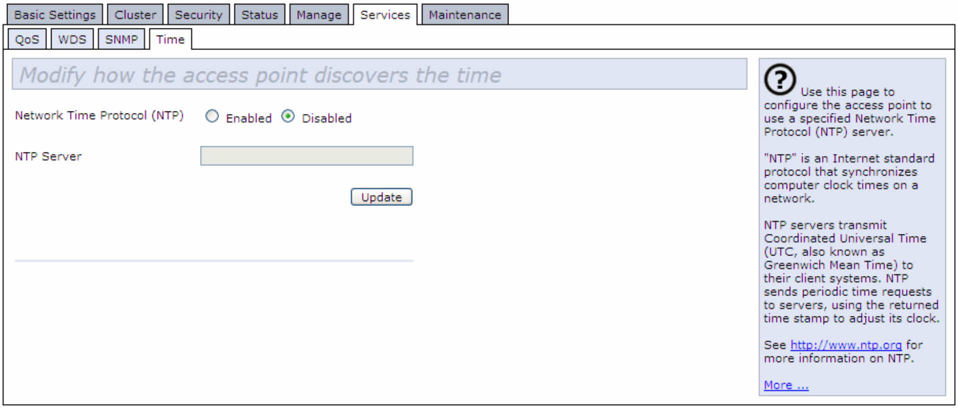
The timestamp will be used to indicate the date and time of each event in log messages.

See *http://www.ntp.org* for more general information on NTP.

The following sections describe how to configure the 9160 G2 Wireless Gateway to use a specified NTP server.

23.1 Navigating To Time Protocol Settings

To enable an ***NTP*** server, navigate to the *Services > Time Protocol* tab, and update the fields as described below.



Modify how the access point discovers the time

Network Time Protocol (NTP) ○ Enabled ● Disabled

NTP Server

Use this page to configure the access point to use a specified Network Time Protocol (NTP) server.

"NTP" is an Internet standard protocol that synchronizes computer clock times on a network.

NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

See http://www.ntp.org for more information on NTP.

More ...

23.2 Enabling Or Disabling A Network Time Protocol (NTP) Server

To configure your access point to use a network time protocol (***NTP***) server, first **enable** the use of NTP, and then select the NTP server you want to use. (To shut down NTP service on the network, disable NTP on the access point.)

Field	Description
Network Time Protocol (NTP)	NTP provides a way for the access point to obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information. For more information on NTP, see http://www.ntp.org. Choose to either enable or disable the use of a network time protocol (NTP) server: • To enable the NTP server, click **Enabled**. • To disable the NTP server, click **Disabled**.
NTP Server	If NTP is enabled, select the NTP server you want to use. You can specify the NTP server by host name or IP address, although using the IP address is not recommended as these can change more readily.

Table 23.1 NTP Settings

23.3 Updating Settings

To update time settings:

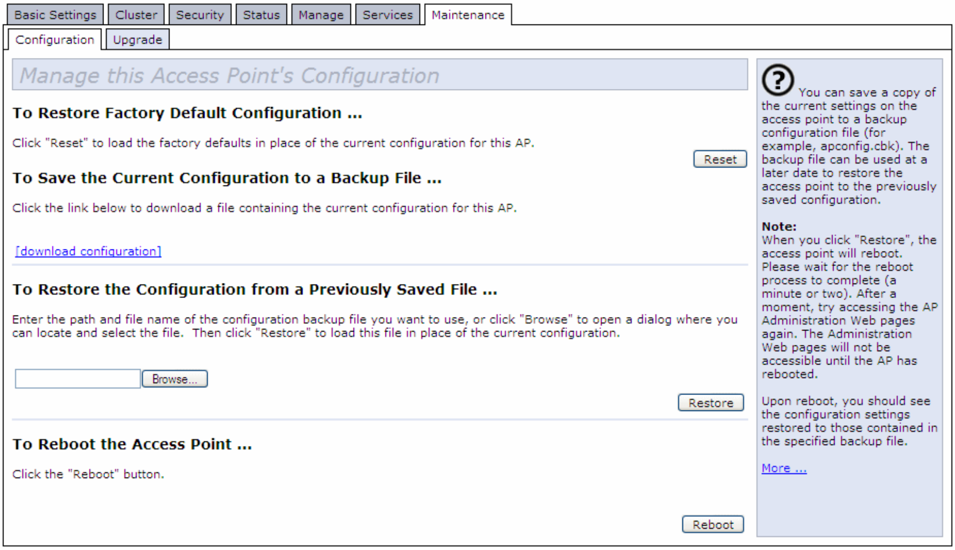
1. Navigate to the *Time* tab page.
2. Configure the time settings as required.
3. Click the **Update** button to apply the changes.

BACKING UP & RESTORING CONFIGURATION 24

You can save a copy of the current settings on the 9160 G2 Wireless Gateway to a backup configuration file. The backup file can be used at a later date to restore the access point to the previously saved configuration.

24.1 Navigating To The AP's Configuration Settings

To manage the configuration of an access point, navigate to the *Maintenance > Configuration* tab and use the interface as described below.



Manage this Access Point's Configuration

To Restore Factory Default Configuration ...

Click "Reset" to load the factory defaults in place of the current configuration for this AP.

To Save the Current Configuration to a Backup File ...

Click the link below to download a file containing the current configuration for this AP.

[download configuration]

To Restore the Configuration from a Previously Saved File ...

Enter the path and file name of the configuration backup file you want to use, or click "Browse" to open a dialog where you can locate and select the file. Then click "Restore" to load this file in place of the current configuration.

To Reboot the Access Point ...

Click the "Reboot" button.

You can save a copy of the current settings on the access point to a backup configuration file (for example, apconfig.cbk). The backup file can be used at a later date to restore the access point to the previously saved configuration.

Note:
When you click "Restore", the access point will reboot. Please wait for the reboot process to complete (a minute or two). After a moment, try accessing the AP Administration Web pages again. The Administration Web pages will not be accessible until the AP has rebooted.

Upon reboot, you should see the configuration settings restored to those contained in the specified backup file.

More ...

24.2 Resetting Factory Default Configuration

If you are experiencing problems with the 9160 G2 Wireless Gateway and have tried all other troubleshooting measures, use the *Reset Configuration* function. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

1. Click the **Maintenance** > **Configuration** tab.
2. Click the **Reset** button.

Factory defaults are restored.

Note: *Keep in mind that if you do reset the configuration from this page, you are doing so for this access point only; not for other access points in the cluster.*

For information on the factory default settings, see "Default Settings For The 9160 G2 Wireless Gateway" on page 27.

24.3 Saving The Current Configuration To A Backup File

To save a copy of the current settings on an access point to a backup configuration file (`.cbk` format):

1. Click the **download configuration** link.

   A *File Download or Open* dialog is displayed.

2. Choose the **Save** option on this first dialog.

   This brings up a file browser.

3. Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

   You can keep the default file name (`config.cbk`) or rename the backup file, but be sure to save the file with a `.cbk` extension.

24.4 Restoring The Configuration From A Previously Saved File

To restore the configuration on an access point to previously saved settings:

1. Select the backup configuration file you want to use, either by typing the full path and file name in the *Restore* textbox or click **Browse** and select the file.

   (Only those files that were created with the Backup function and saved as `.cbk` backup configuration files are valid to use with Restore; for example, `config.cbk`.)

Important: ***It is only possible to restore the configuration file to a 9160 of the same model as the one from which the configuration file was obtained.***

For example, a 9160 G2 model "9160 Wireless Gateway" will not restore a configuration file saved from a 9160 G2 model "9160 Wireless Gateway (Dual Radio)".

2. Click the **Restore** button.

   The access point will reboot.

Note: *When you click* **Restore***, the access point will reboot. A "reboot" confirmation dialog and follow-on "rebooting" status message will be displayed. Please wait for the reboot process to complete (a minute or two). After a moment, try accessing the Administration Web pages as described in the next step; they will not be accessible until the AP has rebooted.*

When the access point has rebooted, access the Administration Web pages either by clicking again on one of the tabs (if the UI is still displayed) or by typing the IP address of the access point into your browser. Now you should see the configuration settings restored to the original settings you retrieved from the Backup file.

24.5 Rebooting The Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the 9160 G2 Wireless Gateway as follows.

1. Click the *Maintenance* > *Configuration* tab.
2. Click the **Restore** button.

   The access point will reboot.

24.6 Upgrading The Firmware

As new versions of the 9160 G2 Wireless Gateway firmware become available, you can upgrade the firmware on your devices to take advantage of new features and enhancements.

Important: ***Do not upgrade the firmware from a wireless client that is associated with the access point you are upgrading. Doing so will cause the upgrade to fail. Furthermore, all wireless clients will be disassociated and no new associations will be allowed.***

If you encounter this scenario, the solution is to use a wired client to gain access to the access point:

- ***Create a wired Ethernet connection from a PC to the access point.***
- ***Bring up the Administration UI.***

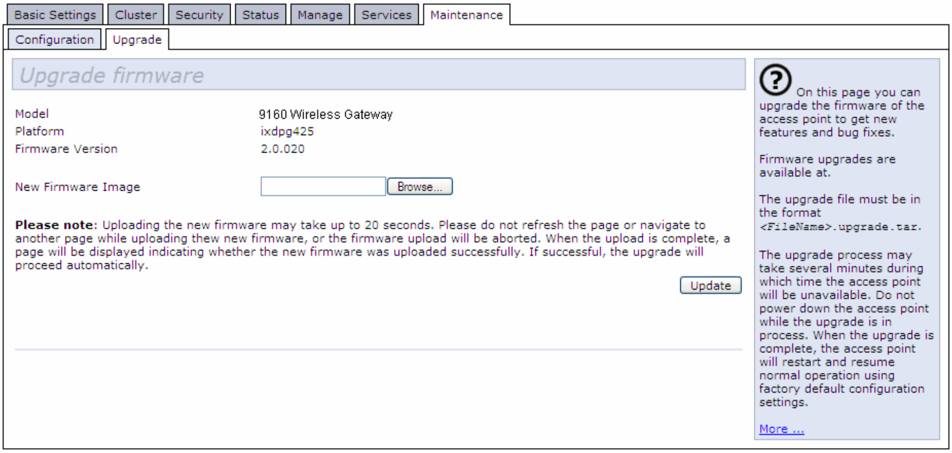
Repeat the upgrade process with the wired client.

Note: *You must do this for each access point; you cannot upgrade firmware automatically across the cluster.*

Keep in mind that a successful firmware upgrade restores the access point configuration to the factory defaults. (See "Default Settings For The 9160 G2 Wireless Gateway" on page 27.)

To upgrade the firmware on a particular access point:

1. Navigate to *Maintenance* > *Upgrade* on the Administration Web pages for that access point.



Upgrade firmware

Model	9160 Wireless Gateway
Platform	ixdpg425
Firmware Version	2.0.020
New Firmware Image	

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading thew new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

On this page you can upgrade the firmware of the access point to get new features and bug fixes.

Firmware upgrades are available at.

The upgrade file must be in the format *<FileName>.upgrade.tar*.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation using factory default configuration settings.

Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.

2. If you know the path to the New Firmware Image file, enter it in the *New Firmware Image* textbox. Otherwise, click the **Browse** button and locate the firmware image file.

Note: *The firmware upgrade file supplied must be in the format* `<FileName>.upgrade.tar`
Do not attempt to use `<FileName>.bin` *files or files of other formats for the upgrade—these will not work.*

24.6.1 Update

1. Click **Update** to apply the new firmware image.

   Upon clicking Update for the firmware upgrade, a popup confirmation window is displayed that describes the upgrade process.

2. Click **OK** to confirm the upgrade, and start the process

Important: ***The firmware upgrade process begins once you click*** **Update** ***and then*** **OK** ***in the popup confirmation window.***

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation using the factory default configuration settings.

24.6.2 Verifying The Firmware Upgrade

To verify that the firmware upgrade completed successfully, check the firmware version shown on the *Upgrade* tab (and also on the *Basic Settings* tab). If the upgrade was successful, the updated version name or number will be indicated.

SPECIFICATIONS 25

Note: *Performance specifications are nominal and subject to change without notice.*

25.1 Physical Description

Enclosure:	Jet black in colour, FR2000 bay blend material
Dimensions:	≤ 30 x 20 x 12.5 cm (11.8 x 7.9 x 4.9 in.)
Weight:	≤ 2.25 kg (5.0 lbs.) (excludes radios, antennas, and options)

25.2 Environmental Requirements

Operating Temperature:	0°C to 55°C (32°F to 131°F)
Operating Rel. Humidity:	10% to 90%
Storage Temperature:	0°C to 70°C (32°F to 158°F)
Dust and Rain:	IP42 or greater
Vibration:	EH0002 (Shipping vibration only)
Reliability:	MTBF 25,000 Hours (MIL-HDBK-217F)

25.3 AC Power Requirements

AC universal input via a standard IEC320 connector. Disables Power over Ethernet (802.3af discovery) when connected.

Input voltage:	100 - 240 VAC nominal
Current:	5.0 A maximum

Warning: ***A ground wire, not exceeding 3 m in length, must be connected between the ground screw (located on the quick-release mount) and a suitable earth ground bonding point on any 9160 G2 connected to an antenna that is installed outdoors.***

25.4 Power Over Ethernet Requirements

Compliant with IEEE 802.3af (disabled when AC power is connected).

Input voltage:	37 - 57 VDC
On-board	
Power Supplies:	2.5W (Assume η=0.8 at full 12.5 watt from Ethernet)
Dual 802.11b radios:	4W
Main Logic Board:	6W

25.5 Processor And Memory

Intel IXP420 processor running at 266 MHz
8 MB Flash ROM
32 MB SDRAM

25.6 Network Interfaces

On-Board Ethernet:	10BaseT/100BaseT (10/100 Mb/s) card with auto-negotiation, half and full duplex. Data rate is auto-sensed.

25.7 Radios

Mini-PCI card 802.11A/G radio without integrated antenna
Mini-PCI card 802.11G radio without integrated antenna

Transmitter Power	100 mW for FCC countries; 50 mW for ETSI	
Frequency Range	2.4 - 2.5 GHz (802.11b/g); 5.15 - 5.825 GHz (802.11a)	
Data Rate	802.11b:	1, 2, 5.5, 11 Mb/s
	802.11a/g:	6, 9, 12, 18, 24, 36, 48, 54 Mb/s
No. of Channels	FCC:	11 (802.11b/g) and 12 (802.11a)
	ETSI:	13 (802.11b/g) and 19 (802.11a)
	China:	13 (802.11b/g) and 4 (802.11a)

Note: *All 802.11a channels are non-overlapping. There are non-overlapping channels in the 2.4 GHz band.*

RA1001A - Narrow Band Radio

Psion Teklogix Proprietary Narrowband Modulation (2/4 level FSK)

Type III PC Card Form Factor

Transmit Power	1W or 0.5W
Frequency Range	403-422 MHz, 419-435 MHz, 435-451 MHz, 450-470 MHz, 464-480 MHz, 480-496 MHz, 496-512 MHz
Rx Sensitivity	< -110dBm @ 19.2kbps (4 level FSK)
Data Rates	4800 bps, 9600 bps, 19.2 kbps

Appendix A

Support Services And Worldwide Offices

Psion Teklogix provides a complete range of product support services to its customers worldwide. These services include technical support and product repairs.

A.1 Technical Support

For technical support in **North America:**

Call Toll free:	+1 800 387 8898 Option 3 *or*
Direct Dial:	+1 905 813 9900 Ext. 1999 Option 3

For technical support in **EMEA** (Europe, Middle East and Africa), please contact the local office listed in the website below:
http://www.psionteklogix.com/EMEASupport

For technical support in **Asia**, please contact the local office listed in the website below:
http://www.psionteklogix.com

Technical Support for Mobile Computing Products is provided via e-mail through the Psion Teklogix customer and partner extranets. To reach the website, go to www.psionteklogix.com, and click on the appropriate Teknet link on the home page. Then click on the “Login” button or the “Register” button, depending on whether you have previously registered for Teknet. Once you have logged in, search for the “Support Request Form”.

A.2 Product Repairs

For repair service in **North America**:

Call Toll free:	+1 800 387 8898 Option 2 *or*
Direct Dial:	+1 905 813 9900 Ext. 1999 Option 2

For repair service in **EMEA** (Europe, Middle East and Africa), please contact the local office listed in the website below:
http://www.psionteklogix.com/EMEASupport

For repair service in **Asia**, please contact the local office listed in the website below:
http://www.psionteklogix.com

A.3 Worldwide Offices

Company Headquarters

Psion Teklogix Inc.
2100 Meadowvale Boulevard
Mississauga, Ontario
Canada L5N 7J9

Tel: +1 905 813 9900

Fax: +1 905 812 6300
E-mail:salescdn@psion.com

Canadian Service Centre

Psion Teklogix Inc.
7170 West Credit Ave., Unit #1
Mississauga, Ontario
Canada L5N 7J9

Tel: +1 800 387 8898Option 2 - or -
Direct: + 1 905 813 9900Ext. 1999, Option 2
Fax: + 1 905 812 6304
Web: www.psionteklogix.com

North American Headquarters And U.S. Service Centre

Psion Teklogix Corp.
1810 Airport Exchange Boulevard, Suite 500
Erlanger, Kentucky
USA 41018

Tel: +1 859 371 6006
Fax: +1 859 371 6422
E-mail:salesusa@psion.com

International Subsidiaries (see also www.psionteklogix.com)

Psion Teklogix S.A.
La Duranne
135 Rue Rene Descartes
BP 421000
13591 Aix-En-Provence
Cedex 3; France

Tel: +33 4 42 90 88 09
Fax: +33 4 42 90 88 88
E-mail:tekeuro@psion.com

APPENDIX B

PORT PINOUTS AND CABLE DIAGRAMS

B.1 Console Port

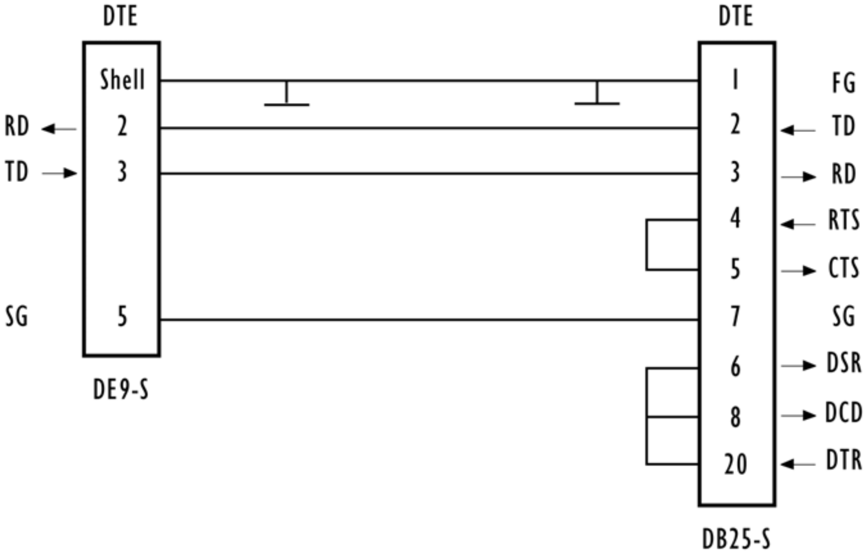
Pin No.	Name	Function	Direction
3	TD	Transmit Data	Out
2	RD	Receive Data	In
5	SG	Signal Ground	–
4*	DTR	Data Terminal Ready	Out
7*	RTS	Request to Send	Out

* always pulled high

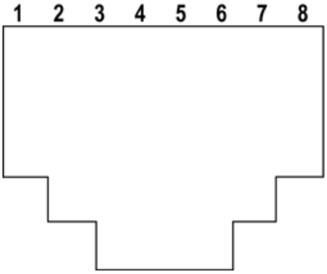
B.2 Serial Cable Descriptions

Cable No.	Function	Connection	Standard Length
19387	9160 G2 to Console	Direct	6 feet

Console Port Cable No. 19387



B.3 RJ-45 Connector Pinouts (10BaseT/100BaseT Ethernet)



9160 G2 using AC		9160 G2 using Power over Ethernet*	
Contact	Signal	Contact	Signal
1	TD+	1	TD+
2	TD–	2	TD–
3	RD+	3	RD+
4	Not used	4	
5	Not used	5	
6	RD–	6	RD–
7	Not used	7	
8	Not used	8	
		** The 9160 G2 can also accept 48 VDC power bias on the data line pairs (1,2) and (3,6) from such systems providing power over Ethernet.*	

Note: *Usually, a straight-through connection is needed to connect Twisted-Pair (10BaseT or 100BaseT) to the hub.*

APPENDIX C

SECURITY SETTINGS ON WIRELESS CLIENTS AND RADIUS SERVER SETUP

Typically, users will configure security on their wireless clients for access to many different networks (access points). The list of “Available Networks” will change depending on the location of the client and which APs are online and detectable in that location.[1] Once an AP has been detected by the client and security is configured for it, it remains in the client’s list of networks but shows as either reachable or unreachable depending on the situation. For each network (AP) you want to connect to, configure security settings on the client to match the security mode being used by that network.

We describe security setup on a client that uses Microsoft® Windows® client software for wireless connectivity. The Windows client software is used as the example because of its widespread availability on Windows computers and laptops. These procedures will vary slightly if you use different software on the client (such as Funk Odyssey®), but the configuration information you need to provide is the same.

Note: *The recommended sequence for security configuration is (1) set up security on the access point, and (2) configure security on each of the wireless clients.*

*We expect that initially, you will connect to an access point that has no security set (“None”) from an unsecure wireless client. With this initial connection, you can go to the access point Administration Web pages and configure a security mode (*Security*).*

When you re-configure the access point with a security setting and click **Update**, *your wireless client will be disassociated and you will lose connectivity to the AP Administration Web pages. In some cases, you may need to make additional changes to the AP security settings before configuring the client. Therefore, you must have a backup Ethernet (wired) connection.*

The following sections describe how to set up each of the supported security modes on wireless clients of a network served by the 9160 G2 Wireless Gateway.

[1] The exception to this is if the access point is set to prohibit the broadcast of its network name. In this case the SSID will not show up in the list of Available Networks on the client. Instead, the client must have the exact network name configured in the network connection properties before it will be able to connect.

C.1 Network Infrastructure And Choosing Between Built-in Or External Authentication Server

Network security configurations including *Public Key Infrastructures* (PKI), *Remote Authentication Dial-in User Server* (RADIUS) servers, and *Certificate Authority* (CA) can vary a great deal from one organization to the next in terms of how they provide *Authentication*, *Authorization*, and *Accounting* (AAA). Ultimately, the particulars of your infrastructure will determine how clients should configure security to access the wireless network. Rather than try to predict and address the details of every possible scenario, this document provides general guidelines about each type of client configuration supported by the 9160 G2 Wireless Gateway.

C.1.1 Using The Built-in Authentication Server (EAP-PEAP)

If you do not have a RADIUS server or PKI infrastructure in place and/or are unfamiliar with many of these concepts, we strongly recommend setting up the 9160 G2 Wireless Gateways with security that uses the *Built-in Authentication Server* on the AP. This will mean setting up the AP to use either IEEE 802.1x or WPA/WPA2 Enterprise (RADIUS) security mode. (The built-in authentication server uses EAP-PEAP authentication protocol.)

- If the 9160 G2 Wireless Gateway is set up to use IEEE 802.1x mode and the Built-in Authentication Server, then configure wireless clients as described in “IEEE 802.1x Client Using EAP/PEAP” on page C-11.
- If the 9160 G2 Wireless Gateway is configured to use WPA/WPA2 Enterprise (RADIUS) mode and the Built-in Authentication Server, configure wireless clients as described in “WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP” on page C-20.

C.1.2 Using An External RADIUS Server With EAP-TLS Certificates Or EAP-PEAP

We make the assumption that if you have an external RADIUS server and PKI/CA setup, you will know how to configure client security options appropriate to your security infrastructure beyond the fundamental suggestions given here. Topics covered here that particularly relate to client security configuration in a RADIUS - PKI environment are:

- “IEEE 802.1x Client Using EAP/TLS Certificate” on page C-15.
- “WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate” on page C-24.
- “Configuring An External RADIUS Server To Recognize The 9160 G2 Wireless Gateway” on page C-30.
- “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Details on how to configure an EAP-PEAP client with an external RADIUS server are not covered in this document.

C.2 Make Sure The Wireless Client Software Is Up-to-Date

Before starting out, please keep in mind that service packs, patches, and new releases of drivers and other supporting technologies for wireless clients are being generated at a fast pace. A common problem encountered in client security setup is not having the right driver or updates to it on the client. For example, if you are setting up WPA on the client, make sure you have a driver installed that supports WPA, which is a relatively new technology. Even many client cards currently available do not ship from the factory with the latest drivers.

C.3 Accessing The Microsoft Windows Wireless Client Security Settings

Generally, on Windows XP there are two ways to get to the security properties for a wireless client:

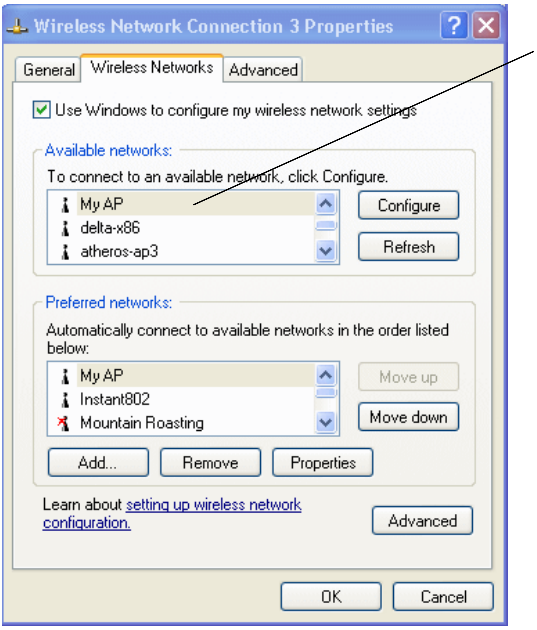
1. From the *Wireless Connection* icon on the Windows task bar:
   - Right-click on the Wireless connection icon in your Windows task bar and select **View available wireless networks**.
   - Select the SSID of the network to which you want to connect and click **Advanced** to bring up the *Wireless Network Connection Properties* dialog.

OR

1. From the Windows *Start* menu at the left end of the task bar:
   - From the Windows *Start* menu on the task bar, choose **Start, My Network Places** to bring up the Network Connections window.

- From the *Network Tasks* menu on the left, click **View Network Connections** to bring up the *Network Connections* window.
- Select the *Wireless Network Connection* you want to configure, right-mouse click and choose **View available wireless networks**.
- Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

  The *Wireless Networks* tab (which should be automatically displayed) lists *Available networks* and *Preferred networks*.



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

My AP
delta-x86
atheros-ap3

Automatically connect to available networks in the order listed below:

My AP
Instant802
Mountain Roasting

Learn about setting up wireless network configuration.

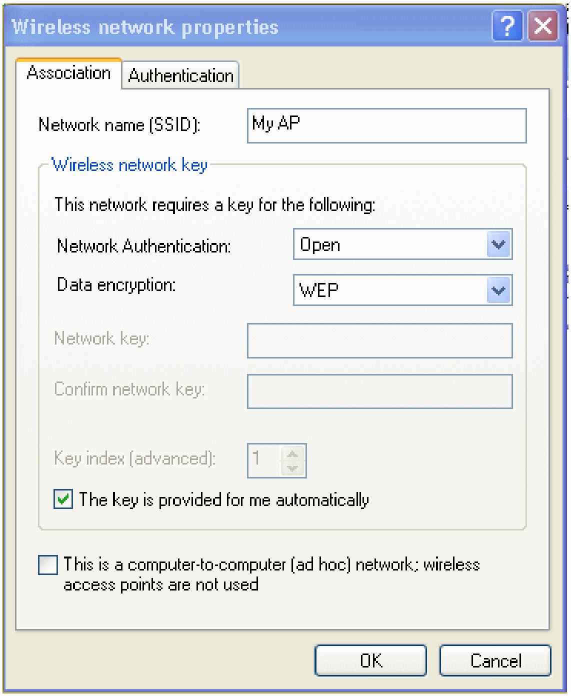
List of available networks will change depending on client location. Each network (or access point) that that is detected by the client shows up in this list. ("Refresh" updates the list with current information.)

For each network you want to connect to, configure security settings on the client to match the security mode being used by that network.

Note: The exception to this is if the AP is configured to prohibit broadcast of its network name, the name will not be show on this list. In that case you would need to type in the exact network name to be able to connect to it.

2. From the list of *Available networks*, select the SSID of the network to which you want to connect and click **Configure**.

   This brings up the *Wireless Network Connection Properties* dialog with the *Association* and *Authentication* tabs for the selected network.



Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

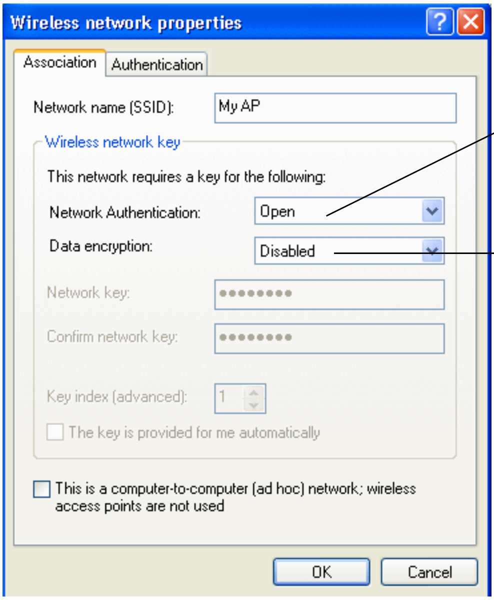
Use this dialog for configuring all the different types of client security described in the following sections. Make sure that the *Wireless Network Properties* dialog you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

C.4 Configuring A Client To Access An Unsecure Network (No Security)

If the access point or wireless network to which you want to connect is configured as “None”, that is no security, you need to configure the client accordingly. A client using no security to connect is configured with *Network Authentication* **Open** to that network and *Data Encryption* **Disabled**, as described below.

If you do have security configured on a client for properties of an unsecure network, the security settings actually can prevent successful access to the network because of the mismatch between client and access point security configurations.

To configure the client to not use any security, bring up the client *Network Properties* dialog, and configure the following settings.



Network name (SSID): My AP

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Set *Network Authentication* to **Open**

Set *Data Encryption* to **Disabled**

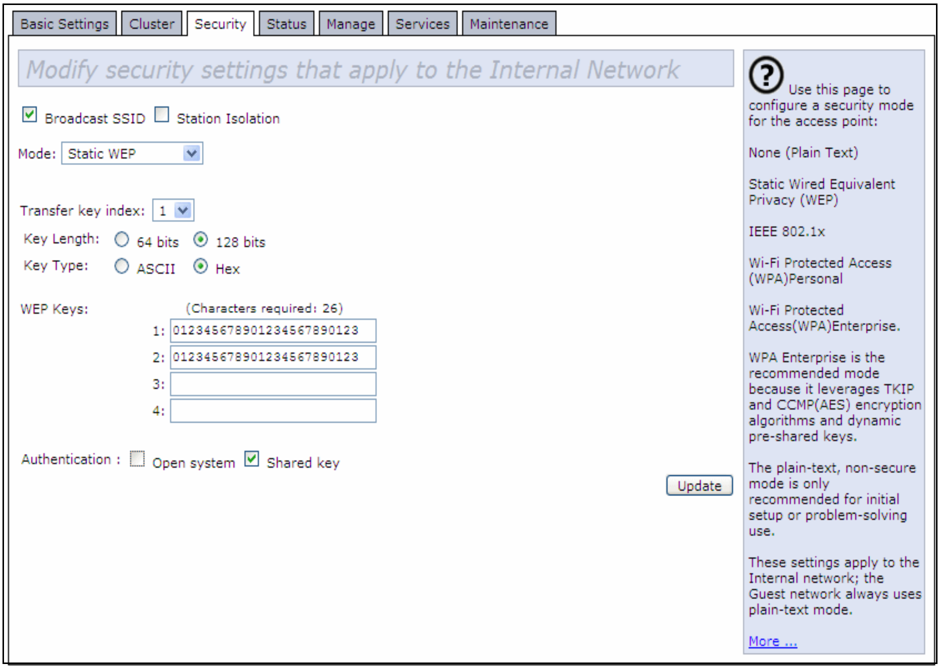
Network Authentication	**Open**
Data Encryption	**Disabled**

Table C.1 Association Settings

C.5 Configuring Static WEP Security On A Client

Static *Wired Equivalent Privacy* (WEP) encrypts data moving across a wireless network based on a static (non-changing) key. The encryption algorithm is a “stream” cipher called RC4. The access point uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the access point. Different clients can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you configured the 9160 G2 Wireless Gateway to use Static WEP security mode . . .



Modify security settings that apply to the Internal Network

☑ Broadcast SSID □ Station Isolation

Mode: Static WEP

Transfer key index: 1

Key Length: ○ 64 bits ● 128 bits

Key Type: ○ ASCII ● Hex

WEP Keys: (Characters required: 26)

1: 01234567890123456789012 3

2: 01234567890123456789012 3

3:

4:

Authentication : □ Open system ☑ Shared key

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

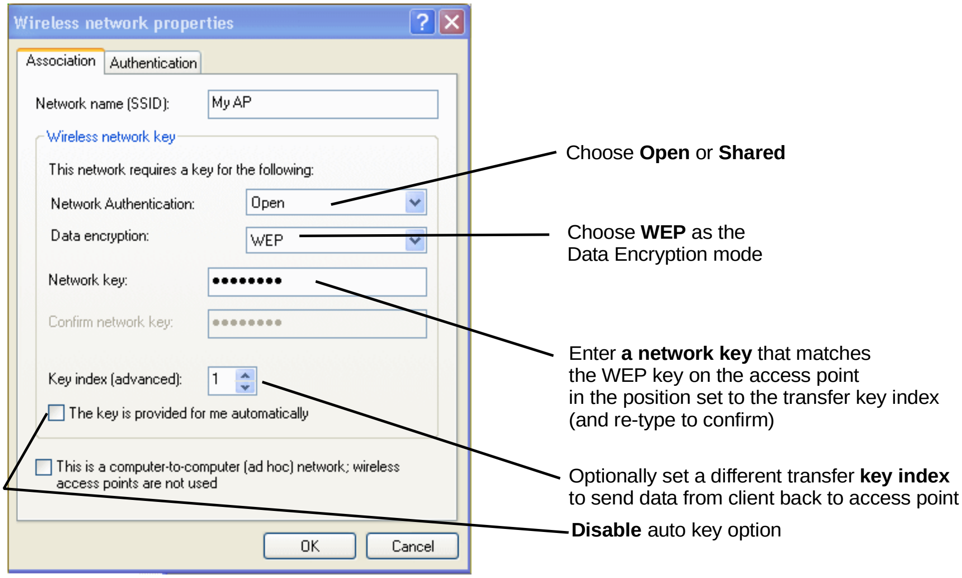
Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

. . . then configure WEP security on each client as follows.



Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Choose **Open** or **Shared**

Choose **WEP** as the
Data Encryption mode

Enter **a network key** that matches
the WEP key on the access point
in the position set to the transfer key index
(and re-type to confirm)

Optionally set a different transfer **key index**
to send data from client back to access point

Disable auto key option

Network Authentication	**Open** or **Shared**, depending on how you configured this option on the access point. ***Note:*** *When the Authentication Algorithm on the access point is set to* ***Both****, clients set to either* ***Shared*** *or* ***Open*** *can associate with the AP. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the AP. Clients configured to use WEP as an Open system can associate with the AP even without a valid WEP key (but a valid key will be required to actually view and exchange data). For more information, see Online Help on the access point.*
Data Encryption	**WEP**
Network Key	Provide the **WEP key** you entered on the access point *Security settings* in the Transfer Key Index position. For example, if the Transfer Key Index on the access point is set to **1**, then for the client Network Key specify the WEP Key you entered as **WEP Key 1** on the access point.
Key Index	Set key index to indicate which of the WEP keys specified on the access point *Security* page will be used to transfer data from the client back to the access point. For example, you can set this to **1, 2, 3,** or **4** if you have all four WEP keys configured on the access point.

Table C.2 Association Settings

The key is provided for me automatically	**Disable** this option (click to uncheck the box).

Table C.2 Association Settings

Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is **disabled** (box should be unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)

Table C.3 Authentication Settings

Click **OK** on the *Wireless Network Properties* dialog to close it and save your changes.

Connecting To The Wireless Network With A Static WEP Client

Static WEP clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a WEP key. The WEP key configured on the client security settings is automatically used when you connect.

C.6 Configuring IEEE 802.1x Security On A Client

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. *Extensible Authentication Protocol* (EAP) messages are sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

C.6.1 IEEE 802.1x Client Using EAP/PEAP

The Built-In Authentication Server on the 9160 G2 Wireless Gateway uses *Protected Extensible Authentication Protocol* (EAP) referred to here as “EAP/PEAP”.

- If you are using the Built-in Authentication server with “IEEE 802.1x” security mode on the 9160 G2 Wireless Gateway, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to:

  (1) Add the 9160 G2 Wireless Gateway to the list of RADIUS server cli-

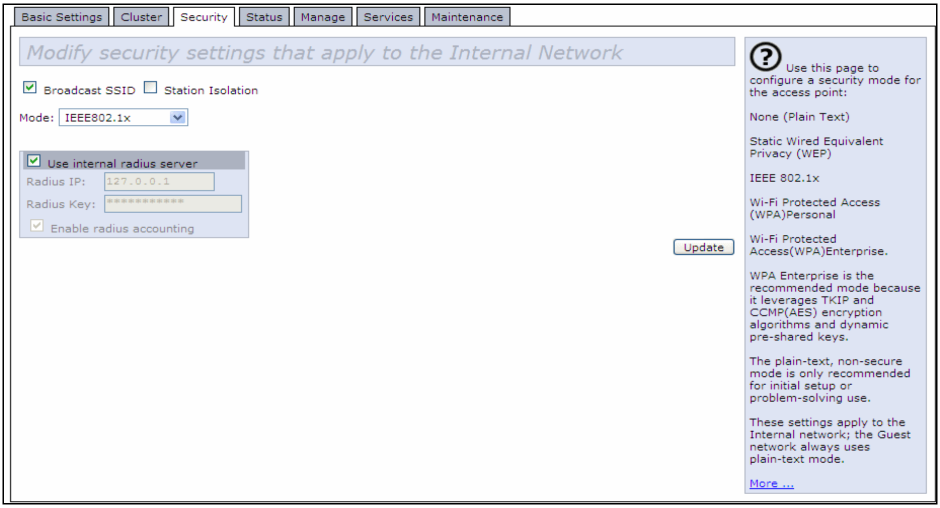
ents.

AND

(2) Configure your IEEE 802.1x wireless clients to use PEAP.

Note: *The following example assumes that you are using the Built-in Authentication server that comes with the 9160 G2 Wireless Gateway. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example, especially with regard to certificate validation.*

If you configured the 9160 G2 Wireless Gateway to use IEEE 802.1x security mode . . .



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☑ Use internal radius server

Radius IP: 127.0.0.1

Radius Key: ***********

☑ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

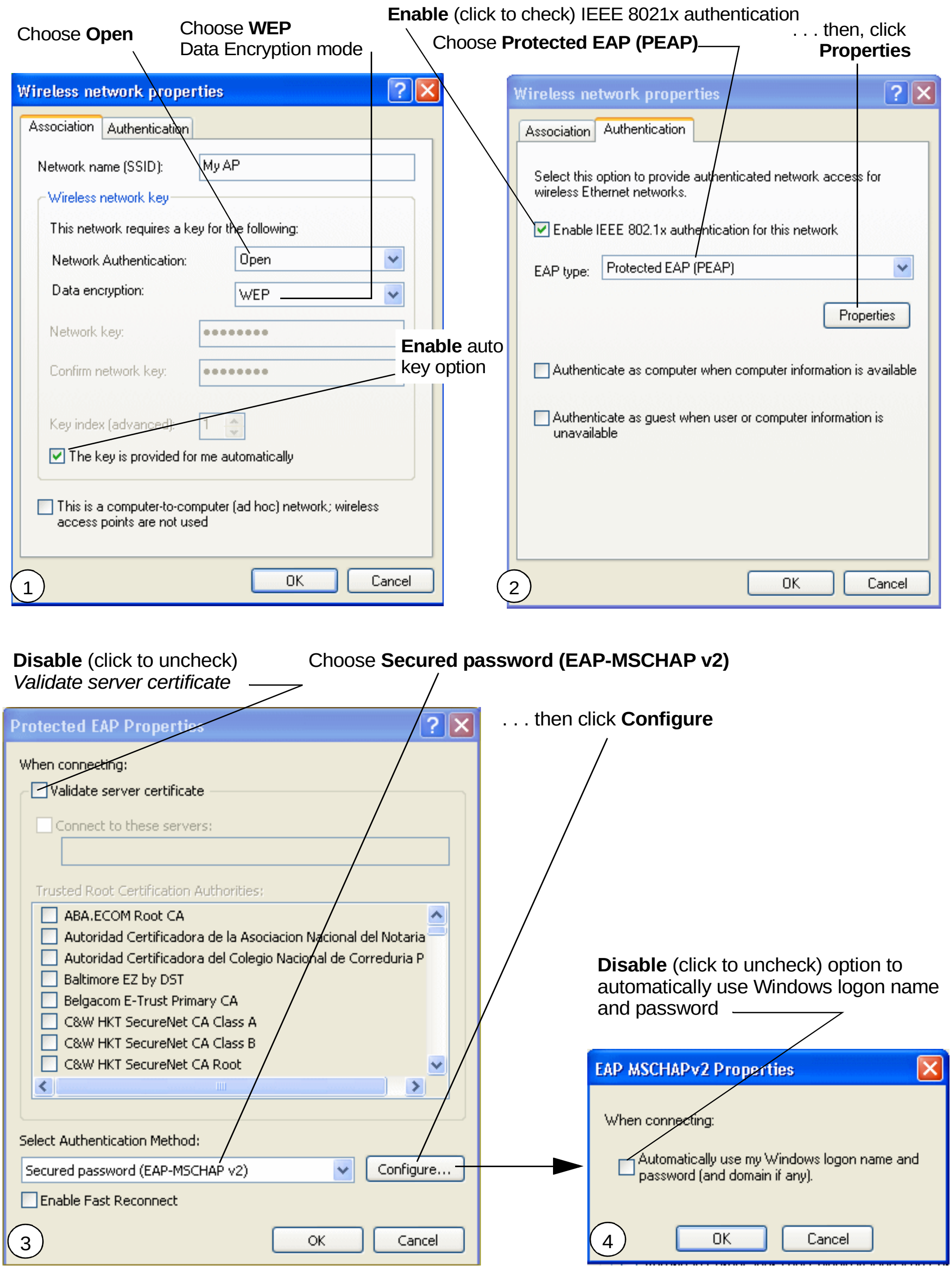
Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

. . . then configure IEEE 802.1x security with PEAP authentication on each client as follows:



Choose **Open**

Choose **WEP**
Data Encryption mode

Enable (click to check) IEEE 8021x authentication

Choose **Protected EAP (PEAP)**

. . . then, click
Properties

1

Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK | Cancel

Enable auto
key option

2

Wireless network properties

Association | Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

Properties

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

OK | Cancel

Disable (click to uncheck)
Validate server certificate

Choose **Secured password (EAP-MSCHAP v2)**

. . . then click **Configure**

3

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria P
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B
□ C&W HKT SecureNet CA Root

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

□ Enable Fast Reconnect

OK | Cancel

Disable (click to uncheck) option to automatically use Windows logon name and password

4

EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

1. Configure the following settings on the *Association* tab on the *Network Properties* dialog.

Network Authentication	**Open**
Data Encryption	**WEP** ***Note:*** *An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.*
This key is provided for me automatically	**Enable** (click to check) this option.

Table C.4 Association Settings

2. Configure this setting on the *Authentication* tab.

EAP Type	Choose **Protected EAP (PEAP)**.

Table C.5 Authentication Settings

3. Click **Properties** to bring up the *Protected EAP Properties* dialog and configure the following settings.

Validate Server Certificate	**Disable** this option (click to uncheck the box). ***Note:*** *This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.*
Select Authentication Method	Choose **Secured password (EAP-MSCHAP v2)**.

Table C.6 Protected EAP Properties Settings

4. Click **Configure** to bring up the *EAP MSCHAP v2 Properties* dialog.

   On this dialog, **disable** (click to uncheck) the option to *Automatically use my Windows logon name . . . etc.*

   Click **OK** on all dialogs (starting with the *EAP MSCHAP v2 Properties* dialog) to close and save your changes.

Logging On To The Wireless Network With An IEEE 802.1x PEAP Client

IEEE 802.1x PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

C.6.2 IEEE 802.1x Client Using EAP/TLS Certificate

Extensible Authentication Protocol (EAP) *Transport Layer Security* (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA/WPA2 Enterprise (RADIUS) and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Note: *If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network.*
It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are:
"How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://support.microsoft.com/default.aspx?scid=kb;en-us;231881 , and

"How to Configure a Certificate Server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

To use this type of security, you must do the following:

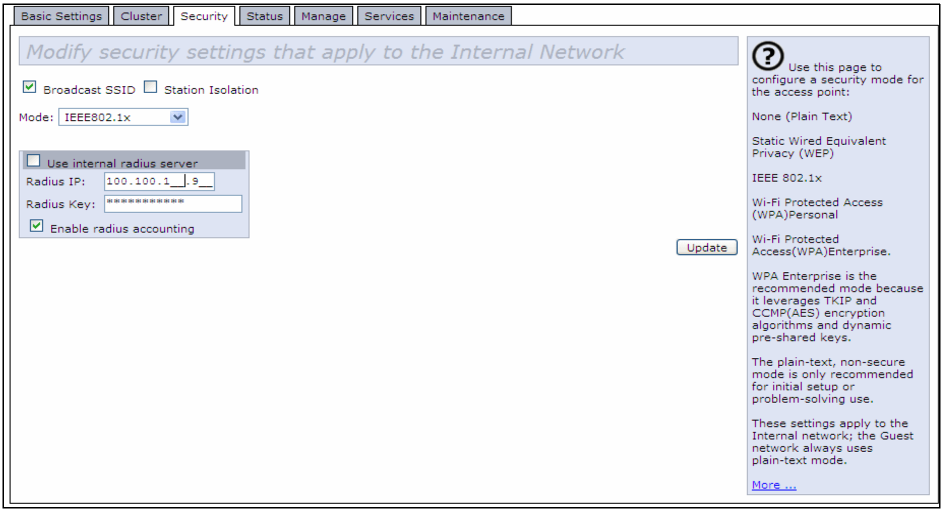
1. Add the 9160 G2 Wireless Gateway to the list of RADIUS server clients. (See "Configuring An External RADIUS Server To Recognize The 9160 G2 Wireless Gateway" on page C-30.)

2. Configure the 9160 G2 Wireless Gateway to use your RADIUS server (by providing the RADIUS server IP address as part of the "IEEE 802.1x" security mode settings).

3. Configure wireless clients to use IEEE 802.1x security and "Smart Card or other Certificate" as described in this section.

4. Obtain a certificate for this client as described in “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

If you configured the 9160 G2 Wireless Gateway to use IEEE 802.1x security mode with an external RADIUS server . . .



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 100.100.1__.9__

Radius Key: *************

☑ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

. . . then configure IEEE 802.1x security with certificate authentication on each client as follows:

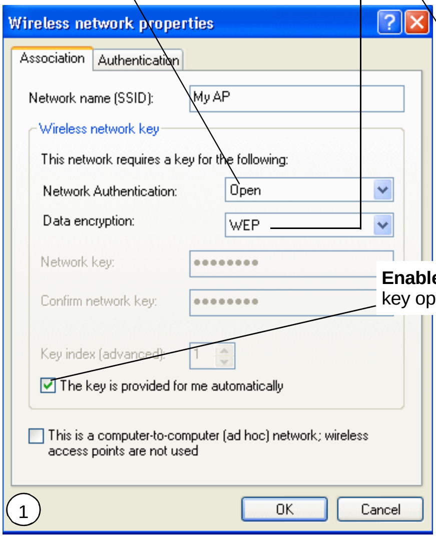
Choose **Open**

Choose **WEP**
Data Encryption mode

Enable (click to check) IEEE 8021x authentication

Choose **Smart Card/Certificate**

. . . then, click **Properties**



1

Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key: ••••••••

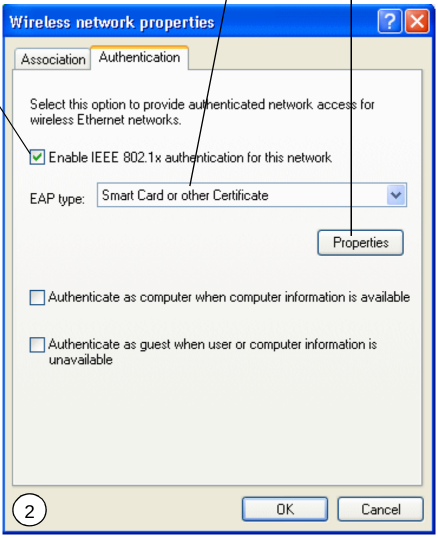
Confirm network key: ••••••••

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Enable auto
key option



2

Wireless network properties

Association | Authentication

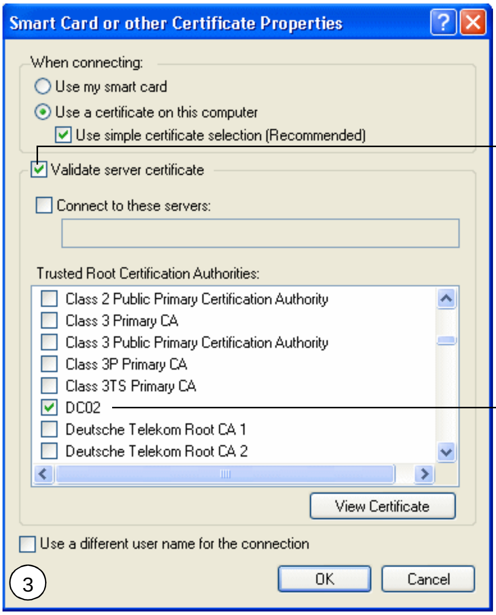
Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable



3

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ Class 2 Public Primary Certification Authority
□ Class 3 Primary CA
□ Class 3 Public Primary Certification Authority
□ Class 3P Primary CA
□ Class 3TS Primary CA
☑ DC02
□ Deutsche Telekom Root CA 1
□ Deutsche Telekom Root CA 2

□ Use a different user name for the connection

Enable (click to check)
Validate server certificate

Select (check) the name of certificate
on this client (downloaded from
RADIUS server in a prerequisite procedure)

1. Configure the following settings on the *Association* tab on the *Network Properties* dialog.

Network Authentication	**Open**
Data Encryption	**WEP** **Note:** *An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.*
This key is provided for me automatically	**Enable** (click to check) this option.

Table C.7 Association Settings

2. Configure these settings on the *Authentication* tab.

Enable IEEE 802.1x authentication for this network	**Enable** (click to check) this option.
EAP Type	Choose **Smart Card or other Certificate**.

Table C.8 Authentication Settings

3. Click **Properties** to bring up the *Smart Card or other Certificate Properties* dialog and enable the **Validate server certificate** option.

Validate Server Certificate	**Enable** this option (click to check the box).
Certificates	In the certificate list shown, select the **certificate** for this client.

Table C.9 Smart Card Or Other Certificate Properties Settings

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Connecting To The Wireless Network With An IEEE 802.1x Client Using A Certificate

IEEE 802.1x clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for logon information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

C.7 Configuring WPA/WPA2 Enterprise (RADIUS) Security On A Client

Wi-Fi Protected Access 2 (***WPA2***) with *Remote Authentication Dial-In User Service* (***RADIUS***) is an implementation of the Wi-Fi Alliance IEEE ***802.11h*** standard, which includes *Advanced Encryption Standard* (***AES***), *Counter mode/CBC-MAC Protocol* (***CCMP***), and *Temporal Key Integrity Protocol* (***TKIP***) mechanisms. This mode requires the use of a RADIUS server to authenticate users.

This security mode also provides backwards-compatibility for wireless clients that support only the original ***WPA***.

When you configure WPA/WPA2 Enterprise (RADIUS) security mode on the access point, you have a choice of whether to use the Built-in Authentication Server or an external RADIUS server that you provide.

The 9160 G2 Wireless Gateway Built-in Authentication Server supports *Protected Extensible Authentication Protocol* (EAP) known as “EAP/PEAP” and *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAP V2), which provides authentication for point-to-point (PPP) connections between a Windows-based computer and network devices such as access points.

So, if you configure the network (access point) to use security mode and choose the Built-in Authentication server, you must configure client stations to use WPA/WPA2 Enterprise (RADIUS) and EAP/PEAP.

If you configure the network (access point) to use this security mode with an external RADIUS server, you must configure the client stations to use WPA/WPA2 Enterprise (RADIUS) and whichever security protocol your RADIUS server is configured to use.

C.7.1 WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP

The Built-In Authentication Server on the 9160 G2 Wireless Gateway uses *Protected Extensible Authentication Protocol* (EAP) known as “EAP/PEAP”.

- If you are using the Built-in Authentication server with “WPA/WPA2 Enterprise (RADIUS)” security mode on the 9160 G2 Wireless Gateway, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to:

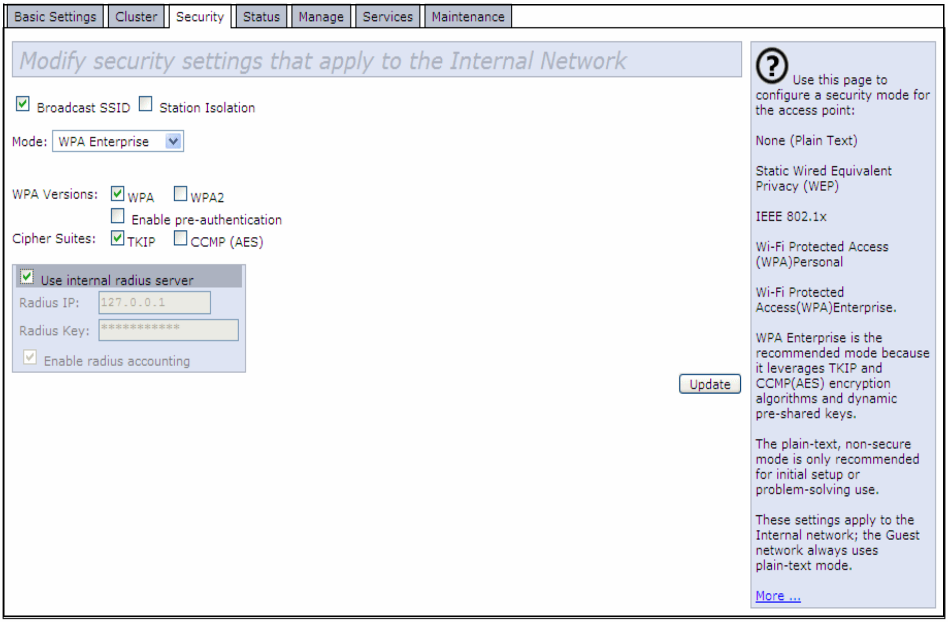
  (1) Add the 9160 G2 Wireless Gateway to the list of RADIUS server clients.

  AND

  (2) Configure your “WPA/WPA2 Enterprise (RADIUS)” wireless clients to use PEAP.

Note: *The following example assumes you are using the Built-in Authentication server that comes with the 9160 G2 Wireless Gateway. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.*

If you configured the 9160 G2 Wireless Gateway to use WPA/WPA2 Enterprise (RADIUS) security mode and to use either the Built-in Authentication Server or an external RADIUS server that uses EAP/PEAP . . .



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☑ WPA ☐ WPA2
☐ Enable pre-authentication
Cipher Suites: ☑ TKIP ☐ CCMP (AES)

☑ Use internal radius server
Radius IP: 127.0.0.1
Radius Key: ***********
☑ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

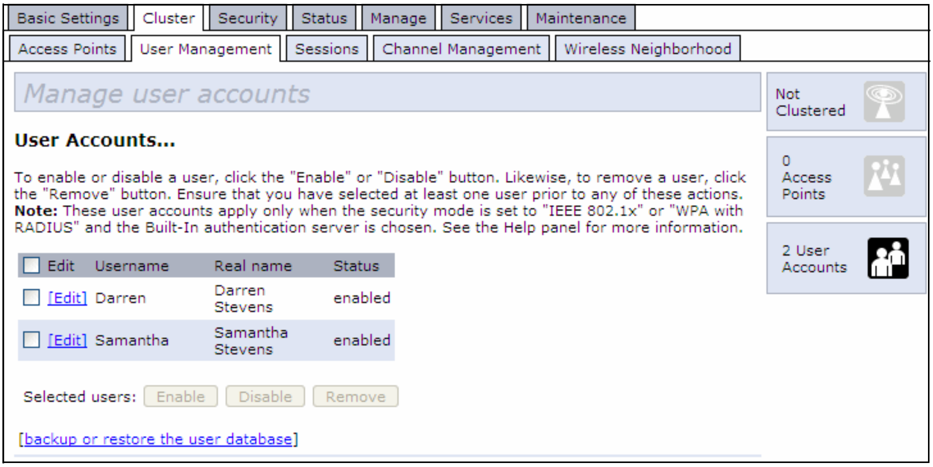
Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

. . . first set up user accounts on the access point (*Cluster, User Management*). . . .



Manage user accounts

User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions. **Note:** These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

☐ Edit	Username	Real name	Status
☐ [Edit]	Darren	Darren Stevens	enabled
☐ [Edit]	Samantha	Samantha Stevens	enabled

Selected users: Enable Disable Remove

[backup or restore the user database]

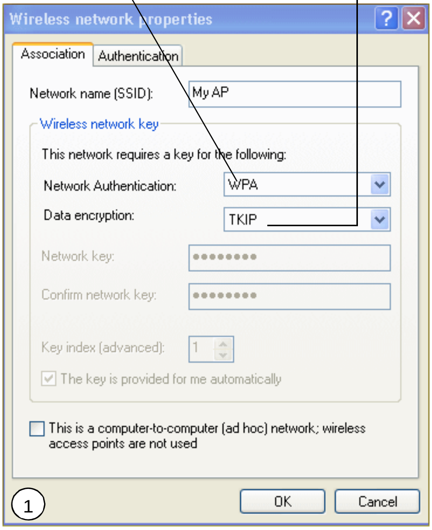
. . . then configure WPA security with PEAP authentication on each client as follows.

Choose **WPA**

Choose either **TKIP** or **AES** for the Data Encryption mode

Choose **Protected EAP (PEAP)**

. . . then, click **Properties**



Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key: ●●●●●●●●

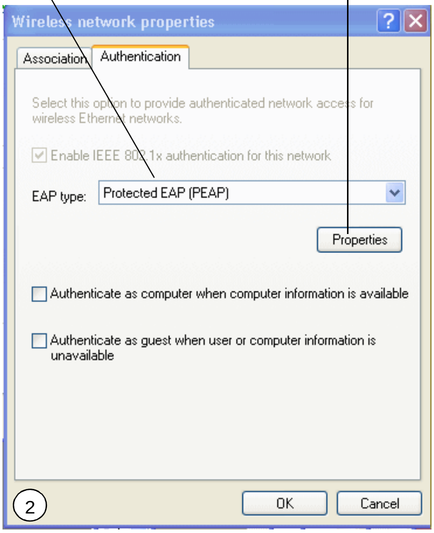
Confirm network key: ●●●●●●●●

Key index (advanced): 1

☑ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel



Wireless network properties

Association | Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

Properties

☐ Authenticate as computer when computer information is available

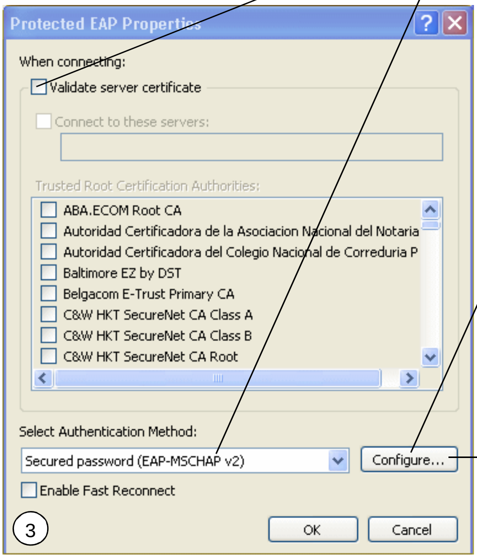
☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel

Disable (click to uncheck) *Validate server certificate*

Choose **Secured password (EAP-MSCHAP v2)**

. . . then click **Configure**



Protected EAP Properties

When connecting:

☐ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

☐ ABA.ECOM Root CA
☐ Autoridad Certificadora de la Asociacion Nacional del Notaria
☐ Autoridad Certificadora del Colegio Nacional de Correduria P
☐ Baltimore EZ by DST
☐ Belgacom E-Trust Primary CA
☐ C&W HKT SecureNet CA Class A
☐ C&W HKT SecureNet CA Class B
☐ C&W HKT SecureNet CA Root

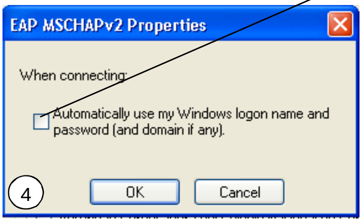
Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

☐ Enable Fast Reconnect

3 OK Cancel

Disable (click to uncheck) this option



EAP MSCHAPv2 Properties

When connecting:

☐ Automatically use my Windows logon name and password (and domain if any).

4 OK Cancel

1. Configure the following settings on the *Association* and *Authentication* tabs on the *Network Properties* dialog.

Network Authentication	**WPA**
Data Encryption	**TKIP** or **AES** depending on how this option is configured on the access point. ***Note:*** *When the Cipher Suite on the access point is set to* ***Both****, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Online Help on the access point.*

Table C.10 Association Settings

2. Configure this setting on the *Authentication* tab.

EAP Type	Choose **Protected EAP (PEAP)**

Table C.11 Authentication Settings

3. Click **Properties** to bring up the *Protected EAP Properties* dialog and configure the following settings.

Validate Server Certificate	**Disable** this option (click to uncheck the box). ***Note:*** *This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.*
Select Authentication Method	Choose **Secured password (EAP-MSCHAP v2**).

Table C.12 Protected EAP Properties Settings

4. Click **Configure** to bring up the *EAP MSCHAP v2 Properties* dialog.

   On this dialog, **disable** (click to uncheck) the option to *Automatically use my Windows logon name* . . . etc. so that upon logon you will be prompted for user name and password.

   Click **OK** on all dialogs (starting with the *EAP MSCHAP v2 Properties* dialog) to close and save your changes.

Logging On To The Wireless Network With A WPA/WPA2 Enterprise (RADIUS) PEAP Client

“WPA/WPA2 Enterprise (RADIUS)” PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

C.7.2 WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate

Extensible Authentication Protocol (EAP) *Transport Layer Security* (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA/WPA2 Enterprise (RADIUS) and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Note: *If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.*

Some good starting points available on the Web for the Microsoft Windows PKI software are:

“How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at http://support.microsoft.com/default.aspx?scid=kb;en-us;231881 , and

How to “Configure a Certificate Server” at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

To use this type of security, you must do the following:

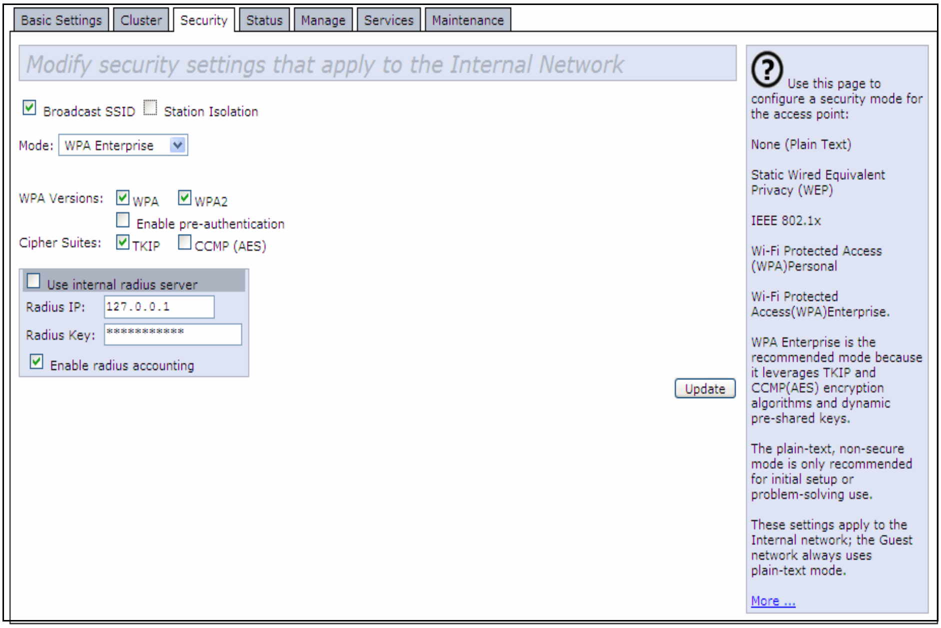
1. Add the 9160 G2 Wireless Gateway to the list of RADIUS server clients. (See “Configuring An External RADIUS Server To Recognize The 9160 G2 Wireless Gateway” on page C-30.)

2. Configure the 9160 G2 Wireless Gateway to use your RADIUS server (by providing the RADIUS server IP address as part of the “WPA/WPA2 Enterprise [RADIUS]” security mode settings).

3. Configure wireless clients to use WPA security and “Smart Card or other Certificate” as described in this section.

4. Obtain a certificate for this client as described in “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

If you configured the 9160 G2 Wireless Gateway to use WPA/WPA2 Enterprise (RADIUS) security mode with an external RADIUS server . . .



Modify security settings that apply to the Internal Network

☑ Broadcast SSID □ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☑ WPA ☑ WPA2
□ Enable pre-authentication

Cipher Suites: ☑ TKIP □ CCMP (AES)

□ Use internal radius server
Radius IP: 127.0.0.1
Radius Key: ************
☑ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

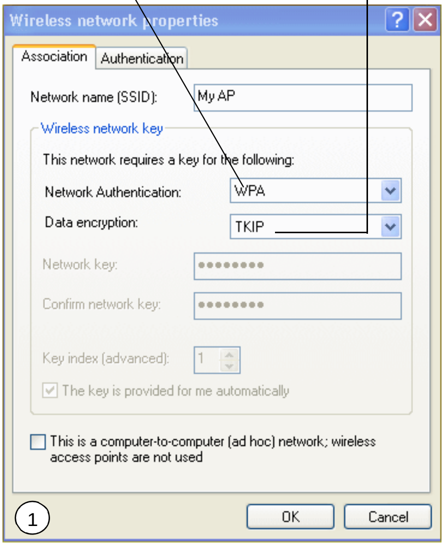
. . . then configure WPA security with certificate authentication on each client as follows.

Choose **WPA**

Choose either **TKIP** or **AES** for the Data Encryption mode

Choose **Smart Card or other Certificate** and enable **Authenticate as computer ....**

. . . then, click **Properties**



Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

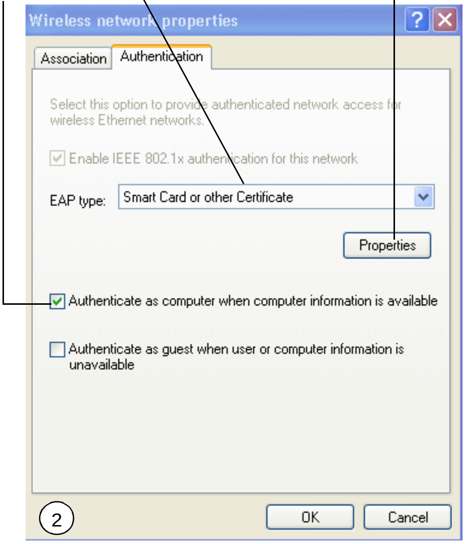
Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used



Wireless network properties

Association | Authentication

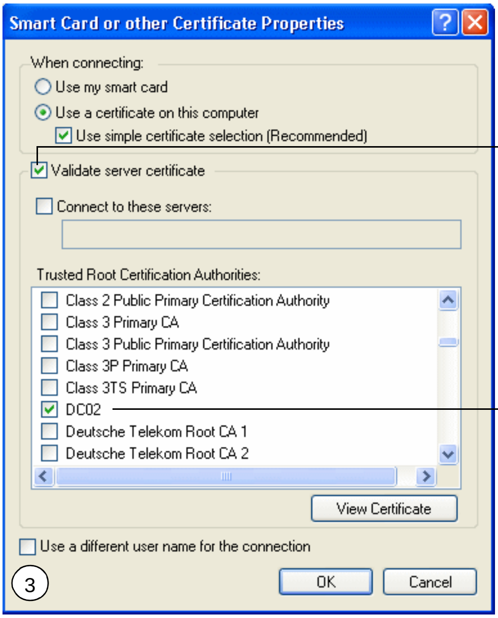
Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

- □ Class 2 Public Primary Certification Authority
- □ Class 3 Primary CA
- □ Class 3 Public Primary Certification Authority
- □ Class 3P Primary CA
- □ Class 3TS Primary CA
- ☑ DC02
- □ Deutsche Telekom Root CA 1
- □ Deutsche Telekom Root CA 2

□ Use a different user name for the connection

Enable (click to check) **Validate server certificate**

Select (check) the name of **certificate** on this client (downloaded from RADIUS server in a prerequisite procedure)

1. Configure the following settings on the *Association* tab on the *Network Properties* dialog.

Network Authentication	**WPA**
Data Encryption	**TKIP** or **AES** depending on how this option is configured on the access point. ***Note:*** *When the Cipher Suite on the access point is set to "Both", then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Online Help on the access point.*

Table C.13 Association Settings

2. Configure these settings on the *Authentication* tab.

Enable IEEE 802.1x authentication for this network	**Enable** (click to check) this option.
EAP Type	Choose **Smart Card or other Certificate**.

Table C.14 Authentication Settings

3. Click **Properties** to bring up the *Smart Card or other Certificate Properties* dialog and enable the **Validate server certificate** option.

Validate Server Certificate	**Enable** this option (click to check the box).
Certificates	In the certificate list shown, select the **certificate** for this client.

Table C.15 Smart Card Or Other Certificate Properties Settings

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see "Obtaining A TLS-EAP Certificate For A Client" on page C-34.

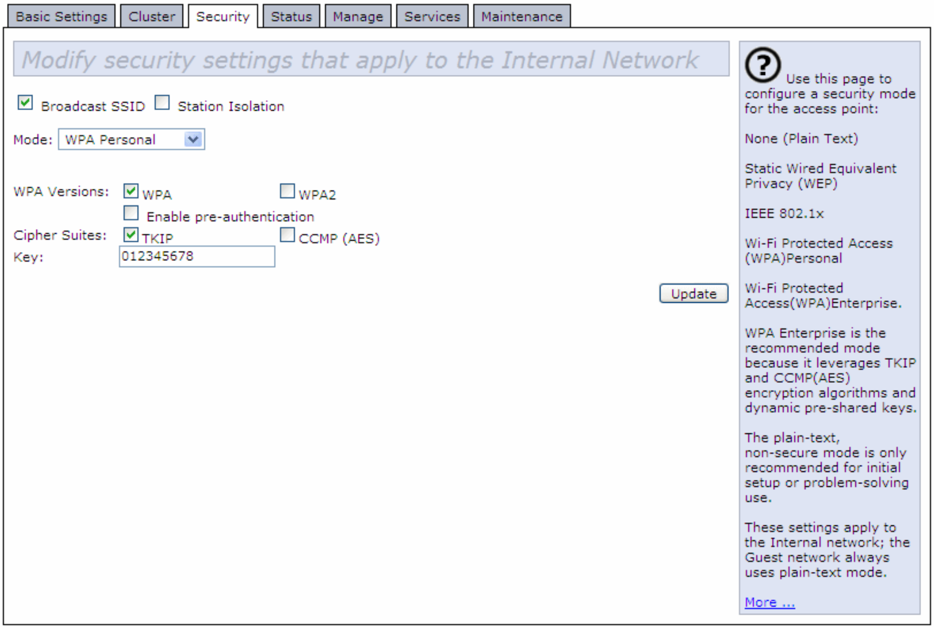
Logging On To The Wireless Network With A WPA Client Using A Certificate

WPA clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for logon information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

C.8 Configuring WPA/WPA2 Personal (PSK) Security On A Client

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Advanced Encryption Algorithm* (AES), and *Counter mode/CBC-MAC Protocol* (CCMP) mechanisms. PSK employs a pre-shared key for an initial check of client credentials.

If you configured the 9160 G2 Wireless Gateway to use WPA/WPA2 Personal (PSK) security mode . . .



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: WPA Personal

WPA Versions: ☑ WPA ☐ WPA2

☐ Enable pre-authentication

Cipher Suites: ☑ TKIP ☐ CCMP (AES)

Key: 012345678

Update

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

Wi-Fi Protected Access(WPA)Enterprise.

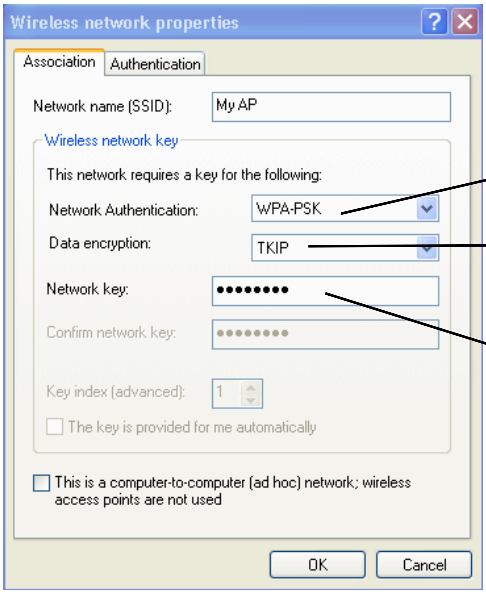
WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

More ...

. . . then configure WPA/WPA2 Personal (PSK) security on each client as follows.



Wireless network properties

Association | Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key: ●●●●●●●●

Confirm network key: ●●●●●●●●

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Choose **WPA-PSK.**

Choose either **TKIP** or **AES** for the Data Encryption mode.

Enter a network key that matches the one specified on the access point (and confirm by re-typing).

Network Authentication	**WPA-PSK**
Data Encryption	**TKIP** or **AES** depending on how this option is configured on the access point. ***Note:*** *When the Cipher Suite on the access point is set to **Both**, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Online Help on the access point.*
Network Key	Provide the key you entered on the access point Security settings for the cipher suite you are using. For example, if the key on the access point is set to use a TKIP key of "012345678", then a TKIP client specify this same string as the network key.
The key is provided for me automatically	This box should be disabled automatically based on other settings.

Table C.16 Association Settings

Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is **disabled** (unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)

Table C.17 Authentication Settings

Click **OK** on the Wireless Network Properties dialog to close it and save your changes.

Connecting To The Wireless Network With A WPA-PSK Client

WPA-PSK clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a key. The TKIP or AES key you configured on the client security settings is automatically used when you connect.

C.9 Configuring An External RADIUS Server To Recognize The 9160 G2 Wireless Gateway

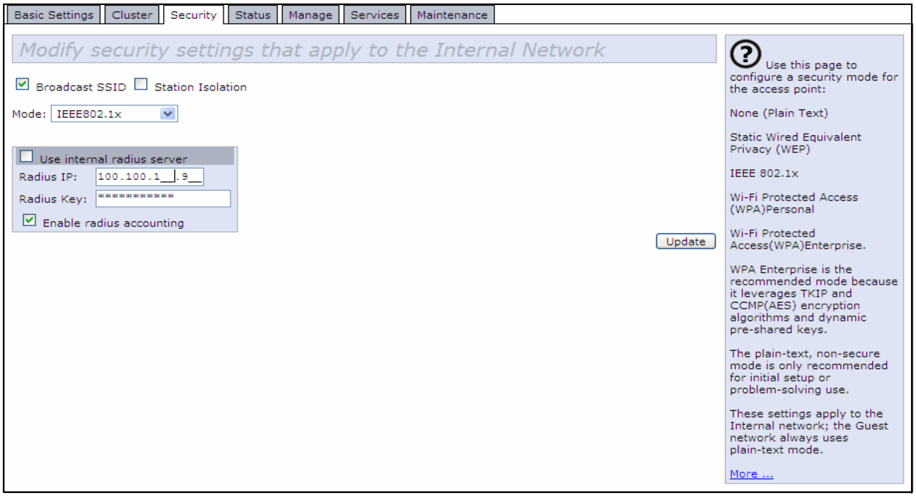
An external *Remote Authentication Dial-in User Server* (RADIUS) running on the network can support EAP-TLS smart card/certificate distribution to clients in a *Public Key Infrastructure* (PKI), as well as EAP-PEAP user account setup and authentication. By *external* RADIUS server, we mean an authentication server external to the access point itself. This is to distinguish between the scenario in which you use a network RADIUS server versus one in which you use the *Built-in Authentication Server* on the 9160 G2 Wireless Gateway.

This section provides an example of configuring an external RADIUS server for the purposes of authenticating and authorizing TLS-EAP certificates from wireless clients of a particular 9160 G2 Wireless Gateway configured for either “WPA/WPA2 Enterprise (RADIUS)” or “IEEE 802.1x” security modes. The intention of this section is to provide some idea of what this process will look like; procedures will vary depending on the RADIUS server you use and how you configure it. For this example, we use the Internet Authentication Service that comes with Microsoft Windows 2003 server.

Note: *This document does not describe how to set up Administrative users on the RADIUS server. In this example, we assume you already have RADIUS server user accounts configured. You will need a RADIUS server user name and password for both this procedure and the following one that describes how to obtain and install a certificate on the wireless client. Please consult the documentation for your RADIUS server for information on setting up user accounts.*

The purpose of this procedure is to identify your 9160 G2 Wireless Gateway as a “client” to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the AP. This procedure is required *per access point*. If you have more than one access point with which you plan to use an external RADIUS server, you need to follow these steps for each of those APs.

Keep in mind that the information you need to provide to the RADIUS server about the access point corresponds to settings on the access point (*Security*) and vice versa. You should have already provided the RADIUS server IP Address to the AP; in the steps that follow you will provide the access point IP address to the RADIUS server. The RADIUS Key provided on the AP is the “shared secret” you will provide to the RADIUS server.



Modify security settings that apply to the Internal Network

☑ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 100.100.1__.9__

Radius Key: ************

☑ Enable radius accounting

Use this page to configure a security mode for the access point:

None (Plain Text)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA)Personal

Wi-Fi Protected Access(WPA)Enterprise.

WPA Enterprise is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys.

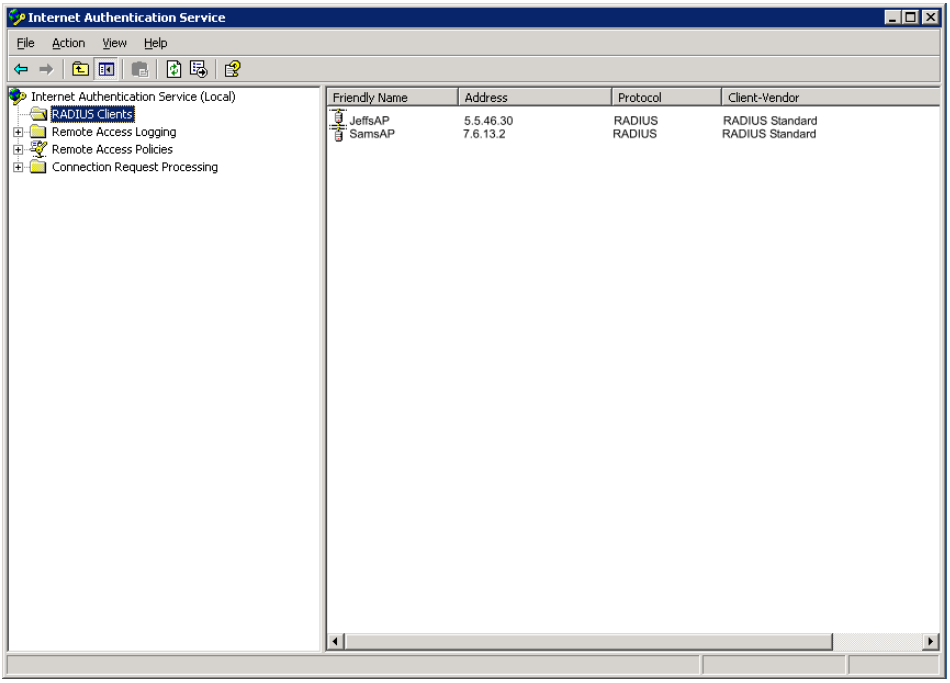
The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

More ...

Note: *The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the 9160 G2 Wireless Gateway, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The 9160 G2 Wireless Gateway is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)*

1. Log on to the system hosting your RADIUS server and bring up the Internet Authentication Service.


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

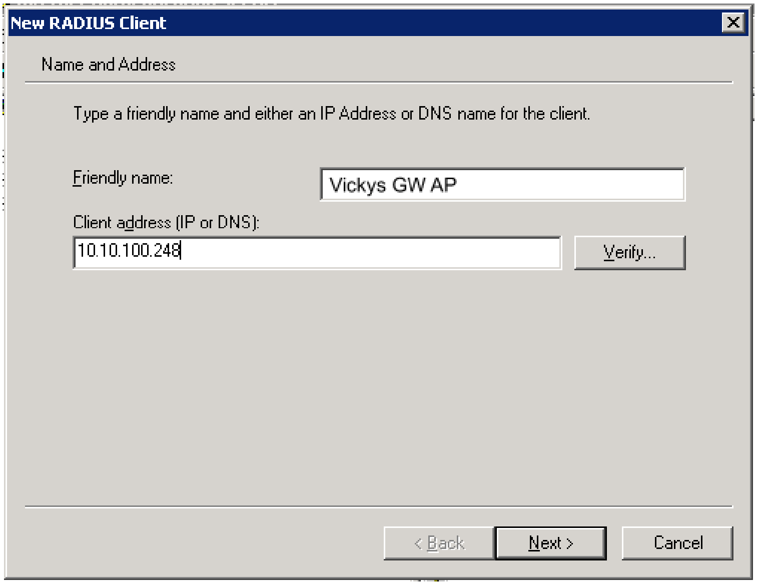
Friendly Name	Address	Protocol	Client-Vendor
JeffsAP	5.5.46.30	RADIUS	RADIUS Standard
SamsAP	7.6.13.2	RADIUS	RADIUS Standard

2. In the left panel, right click on **RADIUS Clients** node and choose **New > Radius Client** from the popup menu.

3. On the first screen of the *New RADIUS Client* wizard, provide information about the 9160 G2 Wireless Gateway to which you want your clients to connect:

   - A logical (friendly) name for the access point. (You might want to use DNS name or location.)

   - IP address for the access point. Click **Next**.

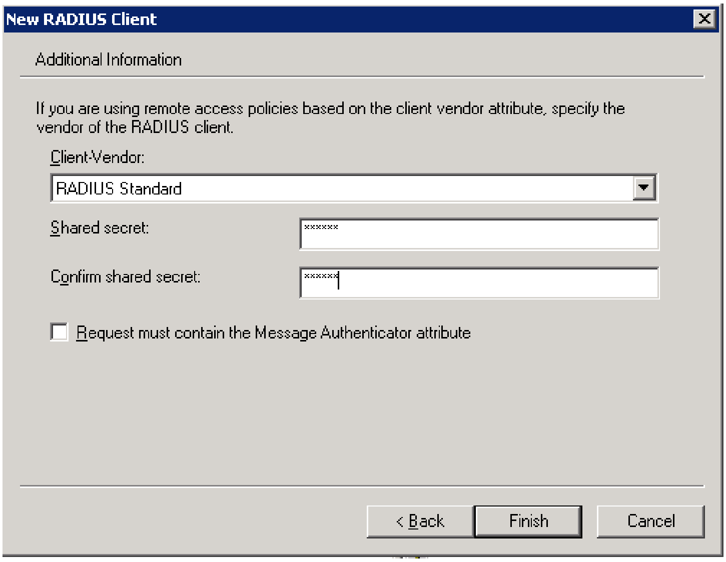


Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: Vickys GW AP

Client address (IP or DNS): 10.10.100.248

4. For the *Shared secret* enter the **RADIUS Key** you provided to the access point (on the *Security* page). Re-type the key to confirm.



If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

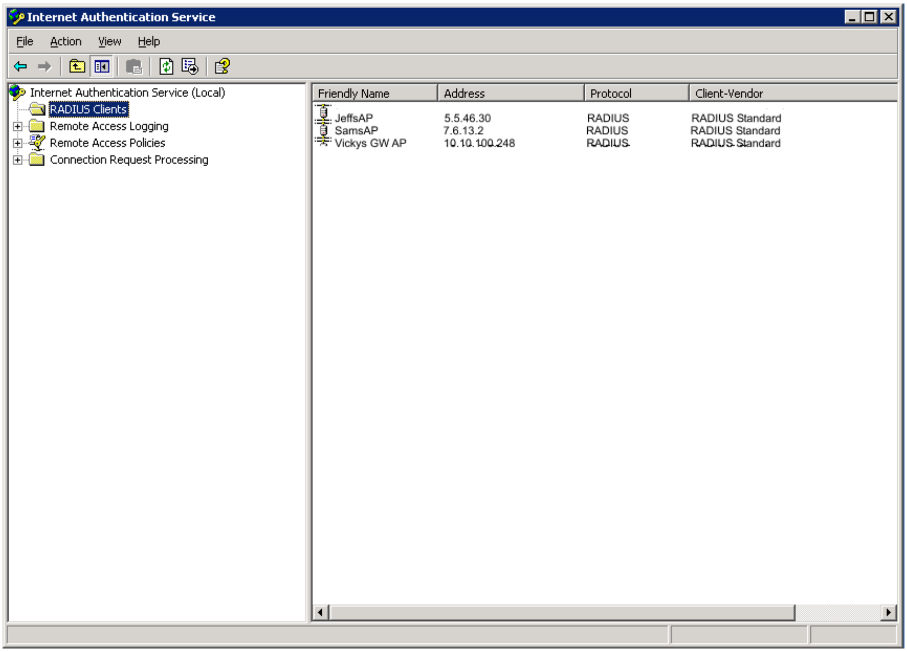
Client-Vendor: RADIUS Standard

Shared secret: ******

Confirm shared secret: ******

☐ Request must contain the Message Authenticator attribute

5. Click **Finish**. The access point is now displayed as a client of the Authentication Server.


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

Friendly Name	Address	Protocol	Client-Vendor
JeffsAP	5.5.46.30	RADIUS	RADIUS Standard
SamsAP	7.6.13.2	RADIUS	RADIUS Standard
Vickys GW AP	10.10.100.248	RADIUS	RADIUS Standard

C.10 Obtaining A TLS-EAP Certificate For A Client

Note: *If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA) server, configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.*

Some good starting points available on the Web for the Microsoft Windows PKI software are:

“How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881 , and

“How to Configure a Certificate Server” at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

Wireless clients configured to use either “WPA/WPA2 Enterprise (RADIUS)” or “IEEE 802.1x” security modes with an external RADIUS server that supports TLS-EAP certificates must obtain a TLS certificate from the RADIUS server.

This is an initial one-time step that must be completed on each client that uses either of these modes with certificates. In this procedure, we use the Microsoft Certificate Server as an example.

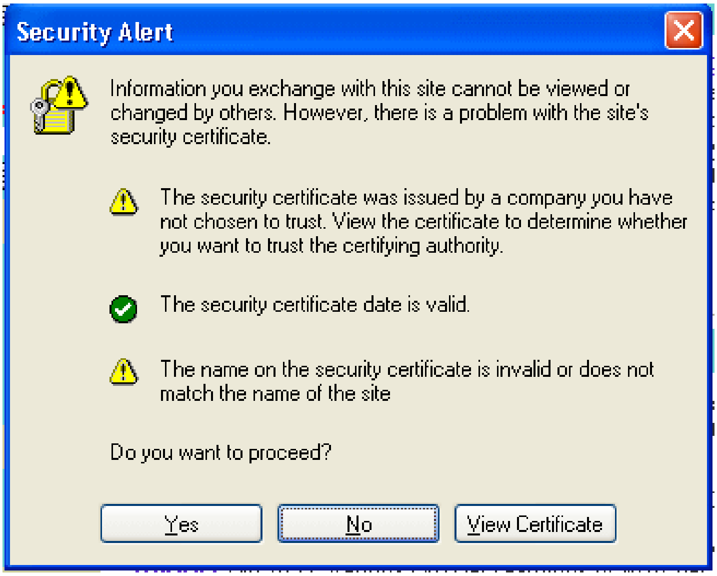
To obtain a certificate for a client, follow these steps.

1. Go to the following URL in a Web browser:

   https://IPAddressOfServer/certsrv/

   Where *IPAddressOfServer* is the IP address of your external RADIUS server, or of the *Certificate Authority* (CA), depending on the configuration of your infrastructure.

2. Click **Yes** to proceed to the secure Web page for the server.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

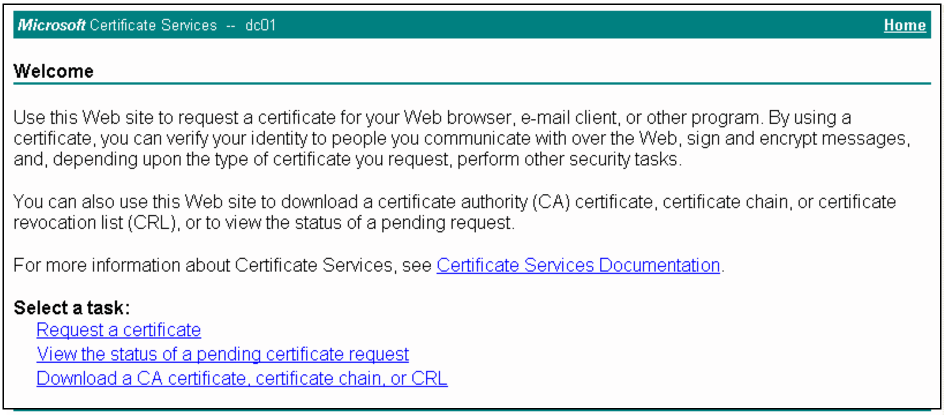
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

The Welcome screen for the Certificate Server is displayed in the browser.



Microsoft Certificate Services -- dc01 **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

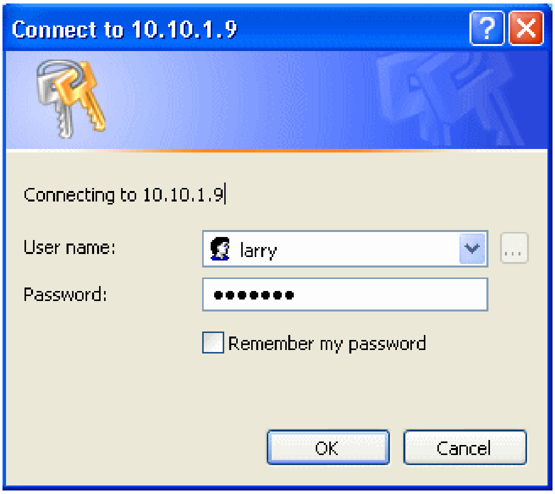
For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. Click **Request a certificate** to get the logon prompt for the RADIUS server.

4. Provide a valid **user name** and **password** to access the RADIUS server.



Connect to 10.10.1.9

Connecting to 10.10.1.9

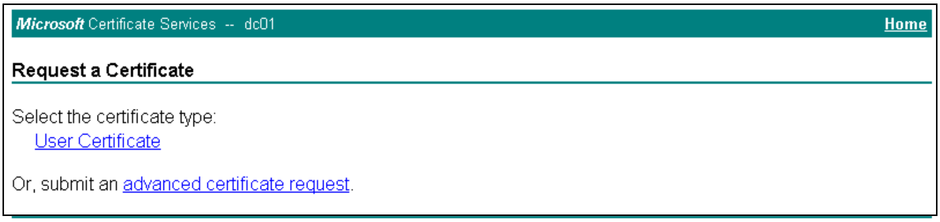
User name: larry

Password: ●●●●●●●

☐ Remember my password

Note: *The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Please consult the documentation for your RADIUS server for these procedures.*

5. Click **User Certificate** on the next page displayed.

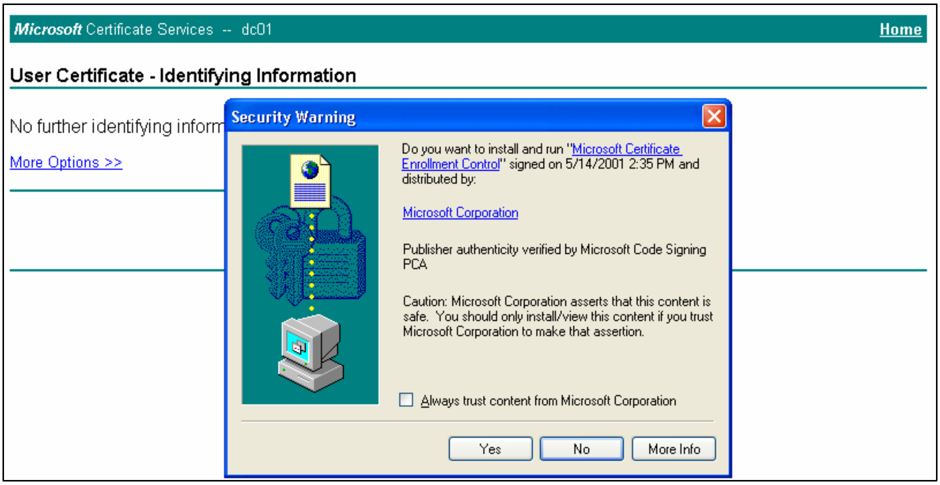


Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

6. Click **Yes** on the dialog displayed to install the certificate.



User Certificate - Identifying Information

No further identifying inform

Do you want to install and run "Microsoft Certificate Enrollment Control" signed on 5/14/2001 2:35 PM and distributed by:

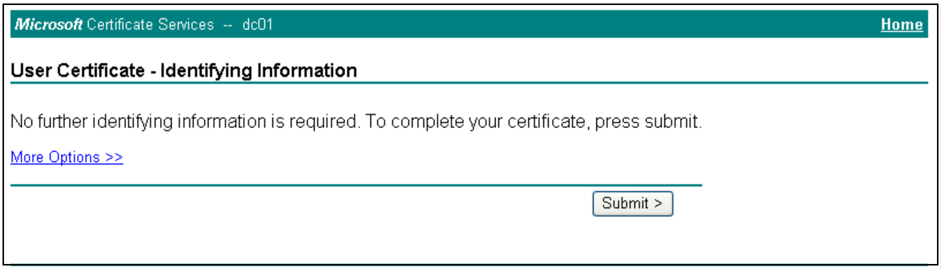
Microsoft Corporation

Publisher authenticity verified by Microsoft Code Signing PCA

Caution: Microsoft Corporation asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation to make that assertion.

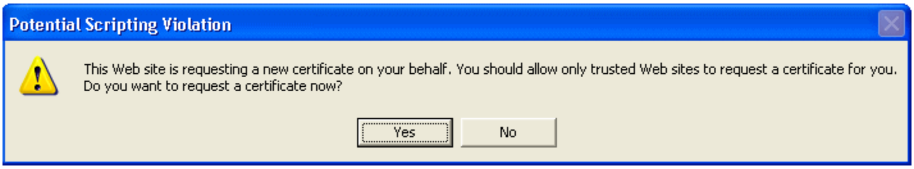
□ Always trust content from Microsoft Corporation

7. Click **Submit** to complete and click **Yes** to confirm the submittal on the popup dialog.



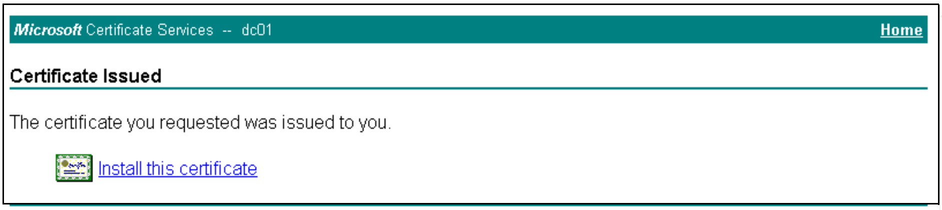
User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit.



This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

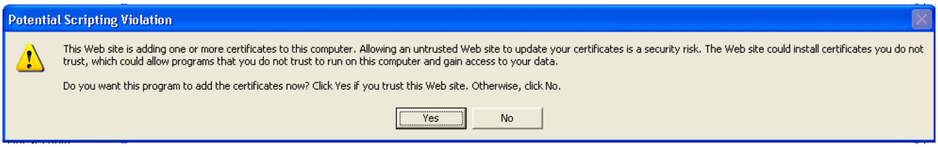
8. Click **Install this certificate** to install the newly issued certificate on your client station. (Also, click **Yes** on the popup windows to confirm the install and to add the certificate to the Root Store.)



Microsoft Certificate Services -- dc01

Certificate Issued

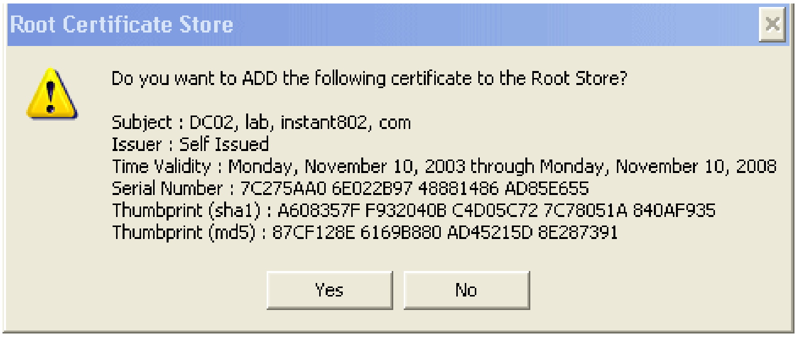
The certificate you requested was issued to you.



Potential Scripting Violation

This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

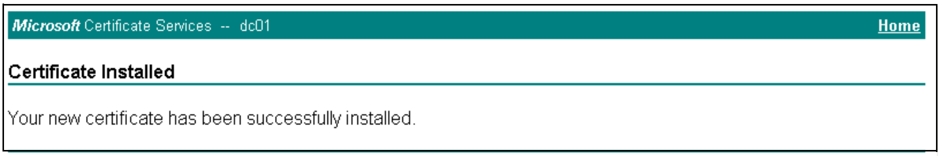


Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : DC02, lab, instant802, com
Issuer : Self Issued
Time Validity : Monday, November 10, 2003 through Monday, November 10, 2008
Serial Number : 7C275AA0 6E022B97 48881486 AD85E655
Thumbprint (sha1) : A608357F F932040B C4D05C72 7C78051A 840AF935
Thumbprint (md5) : 87CF128E 6169B880 AD45215D 8E287391

A success message is displayed indicating the certificate is now installed on the client.



Microsoft Certificate Services -- dc01

Certificate Installed

Your new certificate has been successfully installed.

C.11 Configuring RADIUS Server For VLAN tags

A VLAN is a grouping of ports on a switch or a grouping of ports on different switches. Dynamic VLANs allow you to assign a user to a VLAN, and switches dynamically use this information to configure the port on the switch automatically.

Selection of the VLAN is usually based on the identity of the user. The RADIUS server informs the NAS (for example the access point) of the selected VLAN as part of the authentication. This setup enables users of Dynamic VLANs to move from one location to another without intervention and without having to make any changes to the switches.

In the case of the 9160 G2 Wireless Gateway, if the user has selected to use an external RADIUS server (configured on the *Security* page), then an External RADIUS server will try to authenticate the user. A user's authentication credentials are passed to a RADIUS server. If these credentials are found to be valid, the NAS configures the port to the VLAN indicated by the RADIUS authentication server.

C.11.1 Configuring A RADIUS Server

A RADIUS server needs to be configured to use Tunnel attributes in Access-Accept messages, in order to inform the access point about the selected VLAN. These attributes are defined in RFC 2868 and their use for dynamic VLAN is specified in RFC 3580.

In the case of FreeRADIUS server, the following options may be set in the users file to add the necessary attributes.

```
example-userAuth-Type :=EAP, User-Password =="password"
   Tunnel-Type = 13,
   Tunnel-Medium-Type = 6,
   Tunnel-Private-Group-ID = 7
```

Tunnel-Type and Tunnel-Medium-Type use the same values for all stations. Tunnel-Private-Group-ID is the selected VLAN ID, however it can be different for each user.

APPENDIX D

TROUBLESHOOTING

This section provides information about how to solve common problems you might encounter in the course of updating network configurations on networks served by multiple, clustered access points.

D.1 Wireless Distribution System (WDS) Problems And Solutions

If you are having trouble configuring a WDS link, be sure you have read the notes and cautions in "Configuring WDS Settings" on page 203. These notes are reprinted here for your convenience. The most common problem Administrators encounter with WDS setups is forgetting to set both access points in the link to the same radio channel and IEEE 802.11 mode. That prerequisite, as well as others, is listed in the notes below.

Notes:

- *When using WDS, be sure to configure WDS settings on* **both** *access points participating in the WDS link.*
- *You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.*
- *Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See "Configuring Radio Settings" on page 165 for information on configuring the Radio mode and channel.) For more information on IEEE 802.11h, see "802.11h Regulatory Domain Control" on page 142.*
- *Ensure Spanning Tree Protocol (STP) is enabled to prevent endless loops and path redundancy with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. If STP is enabled, you can use WDS to create backup links. If STP is disabled, keep these rules in mind:*
    - *Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.*
    - *Do not create "backup" links.*
    - *If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.*
    - *You can only extend or bridge either the Internal or Guest network, but not both.*

D.2 Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

D.2.1 Reboot Or Reset Access Point

These recovery methods are given in the order you should try them. In all but the last case (stop clustering), you only need to reset or reboot the particular access point whose configuration is out of sync with other cluster members or cannot remove/join the cluster.

- Physically reboot the access point by cycling the power (pressing the Power button Off, then On).
- Reset the access point from its Administration UI. To do this, go to *http://IPAddressOfAccessPoint*, navigate to *Reset Configuration*, and click the **Reset** button. (IP addresses for APs are on the *Cluster > Access Points* page for any cluster member.)

APPENDIX E

GLOSSARY

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0-9

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a ***LAN***. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of ***LAN***.

Included in the 802 family of ***IEEE*** standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing ***EAP*** packets over an ***802.11*** wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the ***LLC*** layer for the ***802*** family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the ***MAC*** layer for networks that use ***CSMA/CA***. ***Ethernet*** is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (***MAC***) and physical layer (***PHY***) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by ***802.11b***.

IEEE 802.11 is also used generically to refer to the family of ***IEEE*** standards for wireless local area networks.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) is a ***PHY*** standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.

802.11a Turbo

IEEE 802.11a Turbo is a proprietary variant of the ***802.11a*** standard from Atheros Communications. It supports accelerated data rates ranging from 6 to 108Mbps. Atheros Turbo 5 GHz is IEEE 802.11a Turbo mode. Atheros Turbo 2.4 GHz is IEEE 802.11g Turbo mode.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial ***802.11 PHY*** to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11d

IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. PHY requirements such as provides frequency hopping tables, acceptable channels, and power levels for each country are provided. Enabling support for IEEE 802.11d on the access point causes the AP to broadcast which country it is operating in as a part of its beacons. Client stations then use this information. This is particularly important for AP operation in the 5GHz IEEE 802.11a bands because use of these frequencies varies a great deal from one country to another.

802.11e

IEEE 802.11e is a developing ***IEEE*** standard for ***MAC*** enhancements to support ***QoS***. It provides a mechanism to prioritize traffic within ***802.11***. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in kµsec) of a burst of data.

IEEE 802.11e is still a draft ***IEEE*** standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (***WMM***) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (***IAPP***) for access points (wireless hubs) in an extended service set (***ESS***). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the ***802.11b PHY***, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11h

IEEE 802.11h is a standard used is to resolve the issue of interference which was prevalent in 802.11a. The two schemes used to minimize interference in 802.11h are

Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). DFS detects other APs on the same frequency and redirects these to another channel. TCP reduces the network frequency output power of the AP, thus reducing the chance of any interference. This is a required standard in Europe, Japan, and the U.S.

802.11i

IEEE 802.11i is a comprehensive ***IEEE*** standard for security in a wireless local area network (***WLAN***) that describes ***Wi-Fi*** *Protected Access 2* (***WPA2***). It defines enhancements to the ***MAC*** Layer to counter the some of the weaknesses of ***WEP***. It incorporates stronger encryption techniques than the original ***Wi-Fi*** *Protected Access* (***WPA***), such as Advanced Encryption Standard (***AES***).

The original ***WPA***, which can be considered a subset of 802.11i, uses *Temporal Key Integrity Protocol* (***TKIP***) for encryption. WPA2 is backwards-compatible with products that support the original WPA

IEEE 802.11i / ***WPA2*** was finalized and ratified in June of 2004.

802.11j

EEE 802.11j standardizes chipsets that can use both the 4.9 and 5 GHz radio bands according to rules specified by the Japanese government to open both bands to indoor, outdoor and mobile wireless LAN applications. The regulations require companies to adjust the width of those channels. IEEE 802.11j allows wireless devices to reach some previously unavailable channels by taking advantage of new frequencies and operating modes. This is partially an attempt to mitigate the crowding on the airwaves, and has tangential relationships to IEEE 802.11h.

802.11k

IEEE 802.11k is a developing ***IEEE*** standard for wireless networks (***WLAN***s) that helps auto-manage network ***Channel*** selection, client ***Roaming***, and ***Access Point*** (AP) utilization. 802.11k capable networks will automatically load balance network traffic across APs to improve network performance and prevent under or over-utilization of any one AP. 802.11k will eventually complement the ***802.11e*** quality of service (***QoS***) standard by ensuring QoS for multimedia over a wireless link.

802.1p

802.1p is an extension of the IEEE 802 standard and is responsible for QoS provision. The primary purpose of 802.1p is to prioritize network traffic at the data link/ MAC layer. 802.1p offers the ability to filter multicast traffic to ensure it doesn’t increase over layer 2 switched networks. It uses tag frames for the prioritization scheme.

To be compliant with this standard, layer 2 switches must be capable of grouping incoming LAN packets into separate traffic classes.

802.1Q

IEEE 802.1Q is the ***IEEE*** standard for *Virtual Local Area Networks* (***VLAN***s) specific to wireless technologies. (See *http://www.ieee802.org/1/pages/802.1Q.html*.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.11Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

A

Access Point

An *access point* is the communication hub for the devices on a ***WLAN***, providing a connection or bridge between wireless and wired network devices. It supports a ***Wireless Networking Framework*** called ***Infrastructure Mode***.

When one access point is connected to a wired network and supports a set of wireless stations, it is referred to as a basic service set (***BSS***). An extended service set (***ESS***) is created by combining two or more BSSs.

Ad hoc Mode

Ad hoc mode is a ***Wireless Networking Framework*** in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (***IBSS***).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

Atheros XR (Extended Range)

Atheros Extended Range (XR) is a proprietary method for implementing low rate traffic over longer distances. It is meant to be transparent to XR enabled clients and access points and is designed to interoperate with the 802.11 standard in 802.11g and 802.11a modes. There is no support for Atheros XR in 802.11b, Atheros Turbo 5 GHz, or Atheros Dynamic Turbo 5 GHz.

B

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames provide the "heartbeat" of a ***WLAN***, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion. It carries the following information (some of which is optional):

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.
- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.

- The *Capability Information* lists requirements of stations that want to join the ***WLAN***. For example, it indicates that all stations must use ***WEP***.
- The *Service Set Identifier* (***SSID***).
- The ***Basic Rate Set*** is a bitmap that lists the rates that the ***WLAN*** supports.
- The optional *Parameter Sets* indicates features of the specific signalling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map* (TIM) identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (***LAN***s) using the same protocol, such as Ethernet or ***IEEE 802.1x***.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form of ***IEEE 802.1x Frame***s to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also ***Unicast*** and ***Multicast***.

Broadcast Address

See ***IP Address***.

BSS

A *basic service set* (BSS) is an ***Infrastructure Mode Wireless Networking Framework*** with a single access point. Also see extended service set (***ESS***) and independent basic service set (***IBSS***).

BSSID

In ***Infrastructure Mode***, the *Basic Service Set Identifier* (BSSID) is the 48-bit ***MAC*** address of the wireless interface of the ***Access Point***.

C

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for ***802.11h*** that uses ***AES***. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an ***HTTP*** server. It specifies how to pass arguments to the executing program as part of the ***HTTP*** request. It may also define a set of environment variables.

A CGI program is a common way for an ***HTTP*** server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each ***802.11*** standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (***DCF***). See also ***RTS*** and ***CTS***.

The CSMA/CA protocol used by ***802.11*** networks is a variation on CSMA/CD (used by ***Ethernet*** networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an ***IEEE 802.11*** client station in response to an *request to send* (***RTS***) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 ***CSMA/CA*** protocol. (See also ***RTS***.)

D

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows. See also ***EDCF***.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server “offers” a “lease” (for a pre-configured period of time—see ***Lease Time***) to the client system. The information supplied includes the client's IP addresses and netmask plus the address of its ***DNS*** servers and ***Gateway***.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, www is the host name of a Web server and *www.psionteklogix.com* is the fully-qualified name of that server. DNS translates the domain name *www.psionteklogix.com* to some IP address, for example 66.93.138.219.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which *top level domain* (TLD) it belongs to. Every country has its own top-level domain, for example .de for Germany, .fr for France, .jp for Japan, .tw for Taiwan, .uk for the United Kingdom, .us for the U.S.A., and so on. There are also .com for commercial bodies, .edu for educational institutions, .net for network operators, and .org for other organizations as well as .gov for the U. S. government and .mil for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, images, tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some ***Beacon*** frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the ***Access Point*** awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See ***IP Address***.

E

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

EDCF

Enhanced Distribution Control Function is an extension of ***DCF***. EDCF, a component of the IEEE Wireless Multimedia (WMM) standard, provides prioritized access to the wireless medium.

ESS

An *extended service set* (ESS) is an ***Infrastructure Mode Wireless Networking Framework*** with multiple access points, forming a single subnetwork that can support more clients than a basic service set (***BSS***). Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (***LAN***) architecture supporting data transfer rates of 10 Mbps to 1 Gbps. The Ethernet specification is the basis for the ***IEEE 802.3*** standard, which specifies the physical and lower software layers. It uses the ***CSMA/CA*** access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as “*X*base*Y*”, where *X* is the data rate in Mbps and *Y* is the category of cabling. The original cable was *10base5* (Thicknet or “Yellow Cable”). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by ***IEEE 802.11g*** stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the IEEE ***802.11g*** standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel.

Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations.

If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the access point and enable *request to send* (***RTS***) and *clear to send* (***CTS***) protection before sending data.

See also ***CSMA/CA*** protocol.

F

Frame

A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination ***MAC*** address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a ***Packet***, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the ***OSI*** model).

G

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a ***LAN*** can access the Internet, it needs to know the address of its *default gateway.*

H

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an <html> tag and ends with a </html> tag. A properly formatted document also contains a <head> ... </head> section, which contains the metadata to define the document, and a <body> ... </body> section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML).

HTML documents are sent from server to browser via ***HTTP***. Also see ***XML***.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a ***URL*** and a command (GET, HEAD, POST, etc.), a request followed by a response.

HTTPS

The Secure Hypertext Transfer Protocol (HTTPS) is the secure version of HTTP, the communication protocol of the World Wide Web. HTTPS is built into the browser. If you are using HTTPS you will notice a closed lock icon at the bottom corner of your browser page.

All data sent via HTTPS is encrypted, thus ensuring secure transactions take place.

I

IAPP

The *Inter Access Point Protocol* (IAPP) is an ***IEEE*** standard (***802.11f***) that defines communication between the access points in a “distribution system”. This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an ***Ad hoc Mode Wireless Networking Framework*** in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See ***802***, ***802.1x***, ***802.11***, ***802.11a***, ***802.11b***, ***802.11e***, ***802.11f***, ***802.11g***, and ***802.11h***.)

For more information about IEEE task groups and standards, see *http://standards.ieee.org/*.

Infrastructure Mode

Infrastructure Mode is a ***Wireless Networking Framework*** in which wireless stations communicate with each other by first going through an ***Access Point***. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (***BSS***) or a number of access points (***ESS***).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly. It is combined with higher-level protocols, such as ***TCP*** or ***UDP***, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called IPv6 or IPng, is under development. IPv6 is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in form 192.168.2.254. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A ***Subnet Mask*** is used to define the portions. There are two special host numbers:

- The ***Network Address*** consists of a host number that is all zeroes (for example, 192.168.2.0).
- The ***Broadcast Address*** consists of a host number that is all ones (for example, 192.168.2.255).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

A ***Dynamic IP Address*** is an IP address that is automatically assigned to a host by a ***DHCP*** server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A ***Static IP Address*** is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the ***IP*** layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.
- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

J

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including ***Latency***), ***QoS*** for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. ***QoS*** is designed to reduce jitter along with other factors that can impact network performance.

L

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a ***Packet*** from sender to receiver. Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. ***QoS*** features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. ***Ethernet*** is the most common technology implementing a LAN.

Wireless Ethernet (***802.11***) is another very popular LAN technology (also see ***WLAN***).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the ***DHCP*** Server gives its clients an ***IP Address*** and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the ***PHY*** layer, working in conjunction with the ***MAC*** layer.

M

MAC

The *Media Access Control* (MAC) layer handles moving data packets between ***NIC***s across a shared channel. It is a higher level protocol over the ***PHY*** layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. ***IEEE 802*** network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

MDI and MDI-X

Medium Dependent Interface (MDI) and *MDI crossover* (MDIX) are twisted pair cabling technologies for Ethernet ports in hardware devices. Built-in twisted pair cabling and auto-sensing enable connection between like devices with the use of a standard Ethernet cable. (For example, if a wireless access point supports MDI/MDIX, one can successfully connect a PC and that access point with an Ethernet cable rather than having to use a crossover cable).

MIB

Management Information Base (MIB) is a virtual database of objects used for network management. ***SNMP*** agents along with other SNMP tools can be used to monitor any network device defined in the MIB.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for ***PPP*** connections between a Windows-based computer and an ***Access Point*** or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of ***IEEE 802.1x Frame***s to a specified set of client stations (***MAC*** addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also ***Unicast*** and ***Broadcast***.

N

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a ***LAN***. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See ***IP Address***.

NIC

A *Network Interface Card* is an adaptor or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, ***Ethernet*** or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

O

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a components of the physical layer.
- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as ***CSMA/CA*** and components like ***MAC*** addresses, and ***Frame***s are all defined and dealt with as a part of the Data-Link layer.
- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. ***Packet***s and logical ***IP Address***es operate on the network layer.
- Layer 4, the Transport layer, defines connection oriented protocols such as ***TCP*** and ***UDP***.
- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).

- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.
- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (***HTTP***), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

P

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. ***QoS*** features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see ***OSI***). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, ***NIC***s, and physical aspects.

Ethernet and the ***802.11*** family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the fork() system call. It can be used by wait() or kill() to perform actions on the given process.

Port Forwarding

Port Forwarding creates a ‘tunnel’ through a firewall, allowing users on the Internet access to a service running on one of the computers on your ***LAN***, for example, a Web server, an FTP or SSH server, or other services. From the outside user’s point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (***IP*** packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a ***LAN*** to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunnelling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (***VPN***) within the *Point-to-Point Protocol* (***PPP***). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see ***Shared Key***.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see ***Shared Key***.

Q

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize ***Latency***, ***Jitter***, ***Packet Loss***, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The ***IEEE*** standard for implementing QoS on wireless networks is currently in-work by the ***802.11e*** task group. A subset of ***802.11e*** features is described in the ***WMM*** specification.

R

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ***ISP***s.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Roaming

In ***IEEE 802.11*** parlance, *roaming clients* are mobile client stations or devices on a wireless network (***WLAN***) that require use of more than one ***Access Point*** (AP) as they move out of and into range of different base station service areas. IEEE ***802.11f*** defines a standard by which APs can communicate information about client associations and disassociations in support of roaming clients.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (***LAN***s) or between a ***LAN*** and a wide-area network (***WAN***), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an ***802.1x*** value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTP

Real-Time Transport Protocol (RTP) is an Internet protocol for transmitting real-time data like audio and video. It does not guarantee delivery but provides support mechanisms for the sending and receiving applications to enable streaming data. RTP typically runs on top of the ***UDP*** protocol, but can support other transport protocols as well.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the access point, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 ***CSMA/CA*** protocol. (See also ***RTS Threshold*** and ***CTS***.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (***RTS***) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

S

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see ***Public Key***.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the ***TCP/IP*** protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (***MIB***s) and return this data to the SNMP management system when requested.

SNMP Traps

SNMP traps enable the asynchronous communication from network devices to managed agents. Setting SNMP traps saves on network resources and eliminates redundant SNMP requests.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See ***IP Address***.

STP

The *Spanning Tree Protocol* (STP) is an IEEE 802.1 standard protocol (related to network management) for ***MAC*** bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there are multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and re-establishes the link by activating the standby path. Without STP in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as 255.255.255.0) or as a number appended to the IP address (for example, 192.168.2.0/24).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is 192.168.2.128 and the netmask is 255.255.255.0, the resulting Network address is 192.168.2.0.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

IP address	192.168.2.128	11000000 10101000 00000010 10000000
Netmask	255.255.255.0	11111111 11111111 11111111 00000000
Resulting network address	192.168.2.0	11000000 10101000 00000010 00000000

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the ***Basic Rate Set***.

SVP

SpectraLink Voice Priority (SVP) is a QoS approach to Wi-Fi deployments. SVP is an open specification that is compliant with the IEEE 802.11b standard. SVP minimizes delay and prioritizes voice packets over data packets on the Wireless LAN, thus increasing the probability of better network performance.

T

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (***IP***). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although ***TCP*** and ***IP*** are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, ***UDP***, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called “Michael”), and a re-keying mechanism. It uses a ***RC4*** stream cipher to encrypt the frame body and CRC of each ***802.11*** frame before transmission. It is an important component of the ***WPA*** and ***802.11h*** security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit Type *of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way “best-effort” settings depending upon the requirements of the data. The ToS field is used by the 9160 G2 Wireless Gateway to provide configuration control over *Quality of Service* (***QoS***) queues for data transmitted from the AP to client stations.

U

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an ***IP*** packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of ***IEEE 802.1x Frame***s directly to a single client station ***MAC*** address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also ***Multicast*** and ***Broadcast***.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, ftp://ftp.devicescape.com/downloads/myfile.tar.gz specifies a file that should be fetched using the FTP protocol; *http://www.devicescape.com/index.html* specifies a Web page that should be fetched using the ***HTTP*** protocol.

V

VLAN

A *virtual **LAN*** (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The 9160 G2 Wireless Gateway supports the configuration of a wireless VLAN. This technology is leveraged on the access point for the “virtual” guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

W

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites.

The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an ***Access Point*** is connected to a wired ***LAN***. WDS allows access points to be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for ***802.11*** wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) ***Shared Key*** for data encryption. It uses a ***RC4*** stream cipher to encrypt the frame body and CRC of each ***802.11*** frame before transmission.

Wi-Fi

A test and certification of interoperability for ***WLAN*** products based on the ***IEEE 802.11*** standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an ***Ad hoc Mode*** network, also known as an independent basic service set (***IBSS***).
- Stations communicate through an ***Access Point*** in an ***Infrastructure Mode*** network. A single access point creates an infrastructure basic service set (***BSS***) whereas multiple access points are organized in an extended service set (***ESS***).

WLAN

Wireless Local Area Network (WLAN) is a ***LAN*** that uses high-frequency radio waves rather than wires to communicate between its nodes.

WMM

Wireless Multimedia (WMM) is a ***IEEE*** technology standard designed to improve the quality of audio, video and multimedia applications on a wireless network. Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled. WMM features are based on is a subset of the ***WLAN*** IEEE ***802.11e*** draft specification. Wireless products that are built to the standard and pass a set of quality tests can carry the “Wi-Fi certified for WMM” label to ensure interoperability with other such products. For more information, see the WMM page on the Wi-Fi Alliance Web site: *http://www.wi-fi.org/OpenSection/wmm.asp*.

WPA

Wi-Fi Protected Access (WPA) is a ***Wi-Fi*** Alliance version of the draft ***IEEE 802.11h*** standard. It provides more sophisticated data encryption than ***WEP*** and also provides user authentication. WPA includes ***TKIP*** and ***802.1x*** mechanisms.

WPA2

Wi-Fi Protected Access (WPA2) is an enhanced security standard, described in ***IEEE 802.11h***, that uses Advanced Encryption Standard (***AES***) for data encryption.

The original ***WPA*** uses Temporal Key Integrity Protocol (***TKIP***) for data encryption. WPA2 is backwards-compatible with products that support the original ***WPA***.

WPA2, like the original ***WPA***, supports an *Enterprise* and *Personal* version. The Enterprise version requires use of IEEE ***802.1x*** security features and *Extensible Authentication Protocol* (***EAP***) authentication with a ***RADIUS*** server.

The Personal version does not require IEEE ***802.1x*** or ***EAP***. It uses a *Pre-Shared Key* (***PSK***) password to generate the keys needed for authentication.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for ***802.11h*** that uses ***AES*** but another encryption mode (OCB) for encryption and integrity.

X

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), designed especially for electronic publishing.

INDEX