DRAFT

9160
Wireless Gateway

User Manual

December 21, 2005 Part No. 8000009.A

ISO 9001 Certified
Quality Management System

PSION TEKLOGIX

© Copyright 2005 by Psion Teklogix Inc., Mississauga, Ontario

This document and the information it contains is the property of Psion Teklogix Inc., is issued in strict confidence, and is not to be reproduced or copied, in whole or in part, except for the sole purpose of promoting the sale of Psion Teklogix manufactured goods and services. Furthermore, this document is not to be used as a basis for design, manufacture, or sub-contract, or in any manner detrimental to the interests of Psion Teklogix Inc.

All trademarks are the property of their respective holders.

Return-To-Factory Warranty

Psion Teklogix warrants a return-to-factory warranty for a period of one year. Please contact your local Psion Teklogix office for details. For a list of offices, please refer to 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.

Service

When requesting service, please provide information concerning the nature of the failure and the manner in which the equipment was used when the failure occurred. Type, model, and serial number should also be provided. Before returning any products to the factory, call the Customer Services Group for a Return Authorization number.

Support Services

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”.

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: Session Monitoring

Chapter 9: Channel Management

Chapter 10: Wireless Neighborhood

Chapter 11: The Ethernet (Wired) Interface

Chapter 12: Setting the Wireless Interface

Chapter 13: Configuring Security

Chapter 14: Setting up Guest Access

Chapter 15: Configuring VLANs

Chapter 16: Configuring Radio Settings

Chapter 17: MAC Address Filtering

Chapter 18: Load Balancing

Chapter 19: Quality of Service (QoS)

Chapter 20: Wireless Distribution System

Chapter 21: Network Time Protocol Server

Chapter 22: The Administrator Password

Chapter 23: Maintenance And Monitoring

Chapter 24: Backing Up The Configuration

Chapter 25: Specifications

Appendices

Appendix A: Support Services And Worldwide Offices

Appendix B: Port Pinouts And Cable Diagrams

Appendix C: Configuring Security Settings On Wireless Clients

Appendix D: Troubleshooting

Appendix E: Glossary

Approvals and Safety Summary

Declaration Of Conformity

Product:	**9160 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 Wireless Gateway**

Year of Manufacture: 2005

Standard(s) to which Conformity is Declared:

The **9160 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 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.

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 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 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 must be installed by a qualified Psion Teklogix installer—failure to have the 9160 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, 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 with a damaged cord or plug. Replace immediately.
- Do not operate the 9160 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; 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 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 is designed for indoor use only; do not expose the 9160 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 is transmitting.

Connection to Outdoor Antenna

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

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 was first placed on the European Union market on or after August 13th, 2005, contact your local country representative for details on how to arrange recycling.

For a list of international subsidiaries, please go to *www.psionteklogix.com*.

INTRODUCTION 1

1.1 About This Manual

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

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

Chapter 2: Installation Requirements
explains the physical installation of the 9160 Wireless Gateway, and how to connect to the 9160 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 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: Session Monitoring
describes real-time session monitoring information, including client association, data rates, transmit/receive statistics, signal strength, and idle time.

Chapter 9: Channel Management
describes how the 9160 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 10: Wireless Neighborhood
provides a detailed view of neighborhood access points, including identifying information, cluster status, and statistical information.

Chapter 11: The Ethernet (Wired) Interface
describes how to configure the wired interface settings on the 9160 Wireless Gateway.

Chapter 12: Setting the Wireless Interface
describes how to configure the wireless address and related settings on the 9160 Wireless Gateway.

Chapter 13: 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 14: Setting up Guest Access
allows you to configure the 9160 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 Radio Settings
describes how to configure Radio Settings on the 9160 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 Wireless Gateway, enabling you to connect multiple access points which can then communicate with one another wirelessly in a standardized way.

Chapter 21: Network Time Protocol Server
describes how to configure the 9160 Wireless Gateway to use a specified Network Time Protocol (NTP) server to synchronize computer clock times on your network.

Chapter 22: The Administrator Password
controls access to the Administration Web pages for the 9160 Wireless Gateway. When the administration password is set and applied, the new password is updated and shared by all access points in the cluster.

Chapter 23: Maintenance And Monitoring
describes the maintenance and monitoring tasks for individual access points (not for cluster configurations).

Chapter 24: Backing Up The 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 Wireless Gateway.

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.

Appendix C: Configuring Security Settings On Wireless Clients
details how to configure security settings on the client to match the security mode being used by each network (AP) connection.

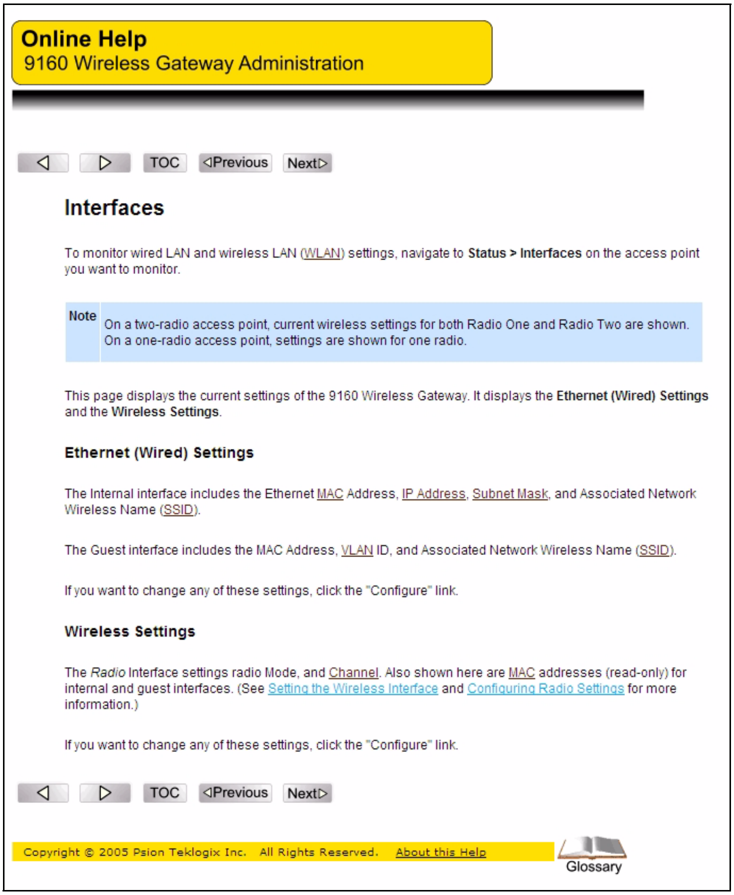
Appendix D: Troubleshooting
describes how to solve common problems possibly encountered while updating network configurations on networks served by multiple, clustered access points.

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 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 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 "Configure" link.

Wireless Settings

The *Radio* Interface settings radio Mode, and Channel. Also shown here are MAC addresses (read-only) for 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 "Configure" link.

Copyright © 2005 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 Wireless Gateway

The 9160 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 Wireless Gateway enables zero-administration wireless local area network (***WLAN***) deployment while providing state-of-the-art wireless networking features.

The 9160 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 Wireless Gateway is available as a single or dual-band access point with one or two radios.

The single band access point can broadcast in the following modes.

- IEEE ***802.11b***.
- IEEE ***802.11g***.
- Atheros Turbo 2.4 GHz.
- Atheros Dynamic Turbo 2.4 GHz.

The dual-band 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.

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

Given these capabilities, various hardware configurations for the end product are possible. For example, a two-radio access point with dual-band capabilities is capable of broadcasting in two different ***IEEE*** 802.11 modes simultaneously.

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

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*** and IEEE ***802.11a Turbo*** 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 IEEE ***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 and provides a seamless experience for roaming clients.
- 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 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.
- 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 multiple ***IEEE 802.11d*** Regulatory Domains (country codes for global operation).

1.5.3 Security Features

- Inhibit SSID Broadcast.
- Ignore SSID Broadcast.
- Weak IV avoidance.
- Wireless Equivalent Privacy (***WEP***).
- Wi-Fi Protected Access 2 (***WPA2***).
- Advanced Encryption Standard (***AES***).
- User-based access control with local authentication server.
- Local user database and user lifecycle management.
- MAC address filtering.

1.5.4 Out-of-the-Box Guest Interface

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

1.5.5 Clustering And Auto-Management

- Automatic setup with Kickstart.
- 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.
- Hardware watchdog.

1.5.6 Networking

- Dynamic Host Configuration Protocol (***DHCP***) support for dynamically assigning network configuration information to systems on the LAN.
- Virtual Local Area Network (VLAN) support.

1.5.7 SNMP Support

Release 1.1 of the 9160 Wireless Gateway ships with the following standard Simple Network Protocol (***SNMP***) Management Information Bases (***MIB***):

- SNMP v1 and v2 MIBs.
- IEEE802.11 MIB.
- Two proprietary MIBs, based on the upcoming IEEE 802.11k MIB, support the 9160 Wireless Gateway client association list and AP detection table, respectively.

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 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 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 9160s. 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 Wireless Gateway

The 9160 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'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 should be situated away from the path of vehicles and free from water or dust spray. The 9160 should only be mounted in the upright position, as shown in Figure 2.1 on page 16. This orientation minimizes the risk of water entering the 9160, should the unit accidentally be sprayed.

The 9160 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.

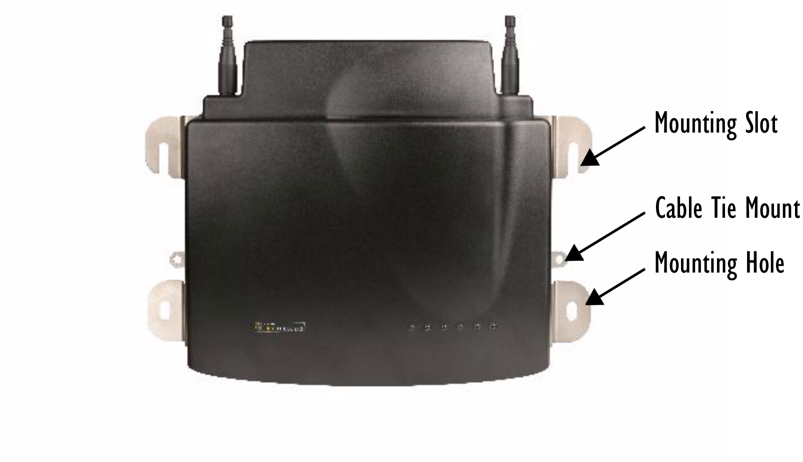


Figure 2.1 9160 Installation Position

2.1.2 Maintenance

The 9160 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

Mini-PCI 802.11g radio without integrated antenna (standard).

Mini-PCI 802.11a/g radio without integrated antenna (optional second radio).

2.1.4 Power And Antenna Cables

2.1.4.1 Power

To prevent accidental disconnection and stress on the 9160, 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 (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. The 9160 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 AC power supply has a universal input via a standard IEC320 connector.

To eliminate the need for AC wiring, the 9160 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 230.

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 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 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) 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 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 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 con-

nection 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 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.

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 to make disconnection easier.

2.2 Connecting To External Devices

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

2.2.1 Ports

Figure 2.2 on page 19 shows the locations of the port and power connectors on the base of the 9160. The port pinouts are described in Appendix B: “Port Pinouts And Cable Diagrams”.

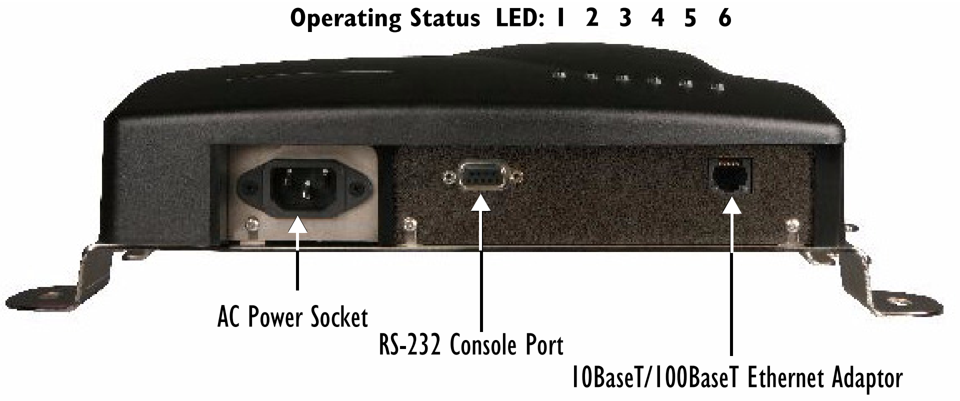

Operating Status LED: 1 2 3 4 5 6
AC Power Socket
RS-232 Console Port
10BaseT/100BaseT Ethernet Adaptor

Figure 2.2 9160 Port And LED Locations

2.2.2 LAN Installation: Overview

Because the 9160 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 is installed, connected and powered on, the system administrator can access the unit to check the configuration and to assign the 9160 its unique IP address. This may be done through the network (see “Changing The Configuration With A Web Browser” on page 20). Subsequent changes in the network, such as the addition of stations or users, would also require that the 9160 configuration be changed.

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

2.2.3 LAN Installation: Ethernet

The 9160 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 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 (10BaseT/100BaseT Ethernet cabling) is 100 m.

2.2.4 Status Indicators (LEDs)

The high-performance 9160 has six status indicators on the front of the enclosure, as shown in Figure 2.2 on page 19. 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	Radio 1 status	Radio 1 activity (Rx/Tx)	green
4	Radio 2 status	Radio 2 activity (Rx/Tx)	green
5	Not used	Always off (unused)	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 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 (see Figure 2.2 on page 19). 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 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 Wireless Gateway

The 9160 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 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 36.

3.1.1 Default Settings For The 9160 Wireless Gateway

Option	Default Settings	Related Information
System Name	9160PTX-Wireless-AP	“Setting The DNS Name” on page 100 in “The Ethernet (Wired) Interface” on page 97
User Name	admin The user name is read-only. It cannot be modified.	
Password	admin	“Provide Administrator Password And Wireless Network Name” on page 49 in “Configuring Basic Settings” on page 45 “Setting The Administrator Password” on page 203 in “The Administrator Password” on page 201

Table 3.1 9160 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 110 in "Setting the Wireless Interface" on page 105 "Configuring "Guest" Network Wireless Settings" on page 111 in "Setting the Wireless Interface" on page 105
Network Time Protocol (NTP)	None	"Network Time Protocol Server" on page 197
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 Wireless Gateway" on page 28
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 Wireless Gateway" on page 28 For information on how to re-configure the Connection Type, see "Configuring Internal Interface Ethernet Settings" on page 102.
Subnet Mask	None This is determined by your network setup and DHCP server configuration.	"The Ethernet (Wired) Interface" on page 97
Radio	On	"Configuring Radio Settings" on page 153

Table 3.1 9160 Default Settings

Option	Default Settings	Related Information
IEEE 802.11 Mode	802.11g or 802.11a+g	"Configuring Radio Settings" on page 153
802.11g Channel	Auto	"Configuring Radio Settings" on page 153
Beacon Interval	100	"Configuring Radio Settings" on page 153
DTIM Period	2	"Configuring Radio Settings" on page 153
Fragmentation Threshold	2346	"Configuring Radio Settings" on page 153
RTS Threshold	2347	"Configuring Radio Settings" on page 153
MAX Stations	2007	"Configuring Radio Settings" on page 153
Transmit Power	100 percent	"Configuring Radio Settings" on page 153
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 Radio Settings" on page 153
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 Radio Settings" on page 153
Broadcast SSID	Allow	"Configuring Security Settings: Broadcast SSID, Station Isolation, and Security Mode" on page 124.
Security Mode	None (plain-text)	"Configuring Security Settings: Broadcast SSID, Station Isolation, and Security Mode" on page 124.
Authentication Type	None	
MAC Filtering	Allow any station unless in list	"MAC Address Filtering" on page 161
Guest Login and Management	Disabled	"Setting up Guest Access" on page 141
Load Balancing	Disabled	"Load Balancing" on page 165
WDS Settings	None	"Wireless Distribution System" on page 185

Table 3.1 9160 Default Settings

3.1.2 What The Access Point Does Not Provide

The 9160 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 Wireless Gateway is accomplished with the KickStart utility (which you run from the CD) and 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 with KickStart 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 34 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 Wireless Gateway. For more details on Wi-Fi client setup, see "Wireless Client Computers" on page 27.

Table 3.2 Required AP Administrator Software And Hardware

Required Components	Description
Web Browser / Operating System	Configuration and administration of the 9160 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.
KickStart Wizard on CD-ROM	You can run the KickStart CD-ROM on any Windows laptop or computer that is connected to the access point (via Wired or Wireless connection). It detects 9160 Wireless Gateways on the network. The wizard steps you through initial configuration of new access points, and provides a link to the Administration Web pages where you finish up the basic setup process in a step-by-step mode and launch the network. For more about using KickStart, see “Run KickStart To Find Access Points On The Network” on page 37 in “Quick Steps For Setup And Launch” on page 31.
CD-ROM Drive	The administrator’s computer must have a CD-ROM drive to run the KickStart CD.
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 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 Component	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 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 113.

Table 3.3 Required AP Client Software And Hardware

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

9160 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.

When you run KickStart, it discovers the 9160 Wireless Gateways on the network and lists their IP addresses and MAC addresses. KickStart also provides a link to the administration Web pages of each access point using the IP address in the URL. (For more information about the KickStart utility, see "Run KickStart To Find Access Points On The Network" on page 37.)

3.4.2 Dynamic IP Addressing

The 9160 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 is present 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 Wireless Gateway ships with a default ***Static IP Address*** of 192.168.1.10. (See “Default Settings For The 9160 Wireless Gateway” on page 23.) 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 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 Internal Interface Ethernet Settings” on page 102.)

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 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 The Configuration To Factory Defaults” on page 218), 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 Wireless Gateways is in effect creating and launching a *wireless network*. The KickStart Wizard and corresponding Basic Settings Administration Web page simplify this process. Here is a step-by-step guide to setting up your 9160 Wireless Gateways and the resulting wireless network. Have the KickStart CD handy, and familiarize yourself with the Chapter 3: "Pre-Launch Checklist" if you haven't already. The topics covered here are:

- Step 1: ***Unpack The 9160 Wireless Gateway***.
- Step 2: ***Connect The Access Point To Network And Power***.
- Step 3: ***Power On The Access Point***.
- Step 4: ***Run KickStart To Find Access Points On The Network***.
- 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 Wireless Gateway

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

4.1.1 9160 Wireless Gateway Hardware And Ports

The 9160 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 Wireless Gateway?

The 9160 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 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 219.)

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 35.)

   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 36.)

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).

It is possible to detect access points on the network (using Kickstart) with a wireless connection. However, we strongly advise against using this method. In most environments you may have no way of knowing whether you are actually connecting to the intended AP and also because many of the initial configuration changes required will cause you to lose connectivity with the AP over a wireless connection.

ETHERNET CONNECTIONS WHEN USING DHCP FOR INITIAL CONFIGURATION

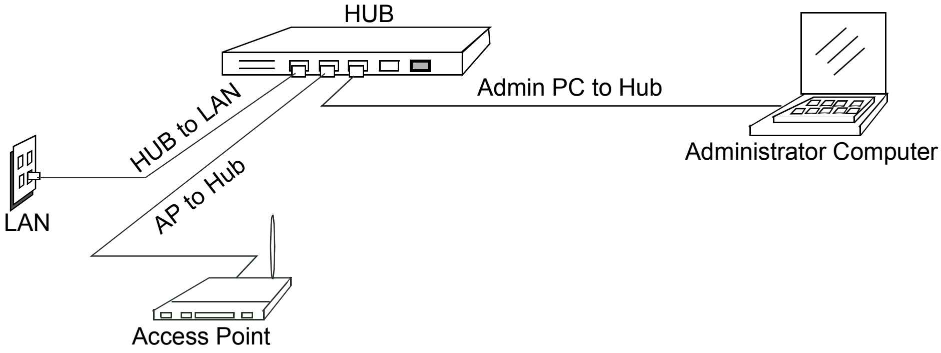


Figure 4.1 Ethernet Connections Using DHCP

ETHERNET CONNECTIONS WHEN USING STATIC IP FOR INITIAL CONFIGURATION

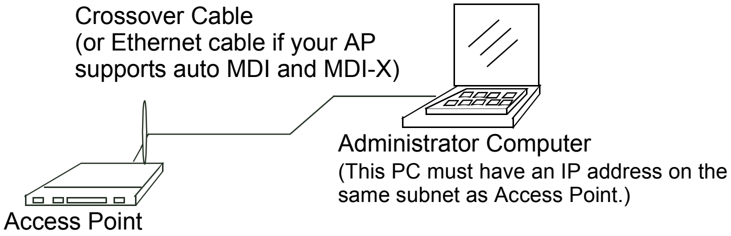

Crossover Cable
(or Ethernet cable if your AP
supports auto MDI and MDI-X)
Administrator Computer
(This PC must have an IP address on the
same subnet as Access Point.)
Access Point

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

4.4 Run KickStart To Find Access Points On The Network

KickStart is an easy-to-use utility for discovering and identifying new 9160 Wireless Gateways. KickStart scans the network looking for access points, and displays ID details on those it finds.

Notes: *Keep in mind that KickStart (and the other Administration tools) recognizes and configures only 9160 Wireless Gateways. KickStart will not find or configure non Psion Teklogix Inc. access points. Kickstart will not find any other devices.*

Run Kickstart only in the subnet of the "Internal" network (SSID). Do not run Kickstart on the guest subnetwork.

Kickstart will find only those access points that have IP addresses. IP addresses are dynamically assigned to APs if you have a DHCP server running on the network. Keep in mind that if you deploy the AP on a network with no DHCP server, the default static IP address (192.168.1.10) will be used.

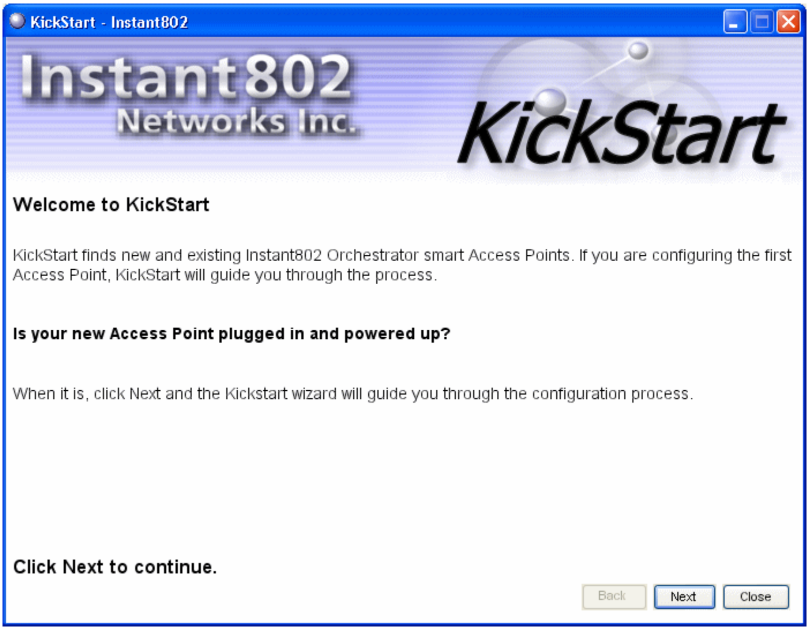
Important: ***Use caution with non-DHCP enabled networks: Do not deploy more than one new AP on a non-DHCP network because they will use the same default static IP addresses and conflict with each other. (For more information, see "Understanding Dynamic And Static IP Addressing On The 9160 Wireless Gateway" on page 28 and "How Does The Access Point Obtain An IP Address At Startup?" on page 29.)***

Run the KickStart CD-ROM on a laptop or computer that is connected to the same network as your access points and use it to step through the discovery process as follows:

1. Insert the KickStart Wizard CD into the CD-ROM drive on your computer.

   The Kickstart window should display automatically. If not, navigate to the CD-ROM drive and run the CD using AutoPlay or the ks.jar executable.

   The KickStart Welcome screen is displayed.



Welcome to KickStart

KickStart finds new and existing Instant802 Orchestrator smart Access Points. If you are configuring the first Access Point, KickStart will guide you through the process.

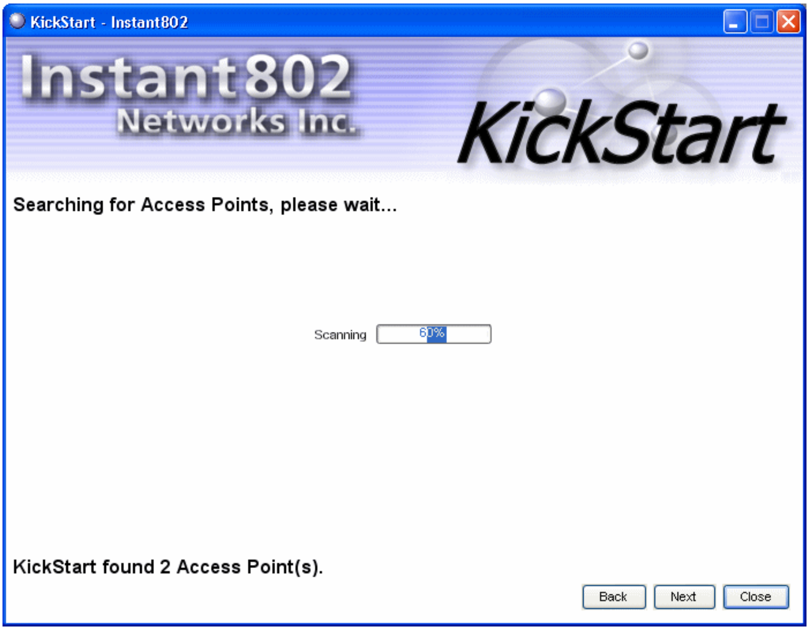
Is your new Access Point plugged in and powered up?

When it is, click Next and the Kickstart wizard will guide you through the configuration process.

Click Next to continue.

Click **Next** to search for access points.

2. Wait for the search to complete, or until KickStart has found your new access points.



Searching for Access Points, please wait...

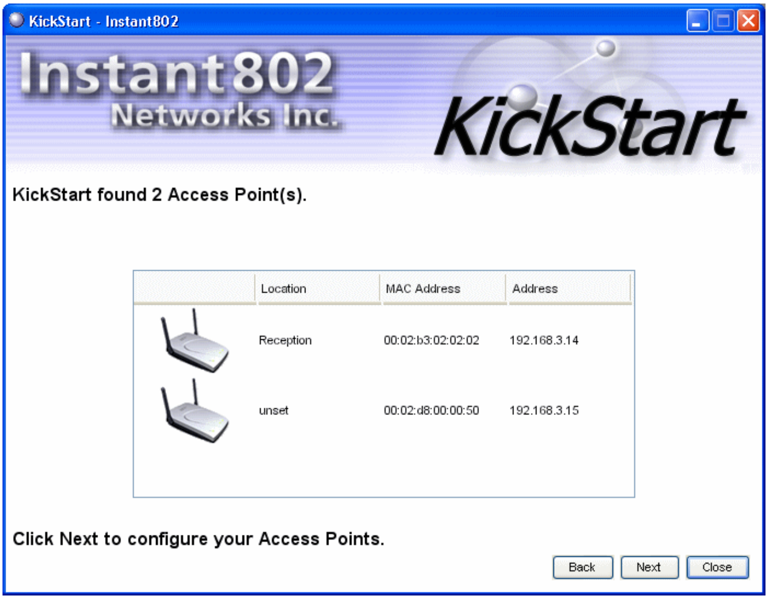
KickStart found 2 Access Point(s).

Note: *If no access points are found, Kickstart indicate this and presents some troubleshooting information about your LAN and power connections. Once you have checked hardware power and Ethernet connections, you can click the Kickstart Back button to search again for access points.*

3. Review the list of access points found.

KickStart will detect the IP addresses of 9160 Wireless Gateways. Access points are listed with their locations, Media Access Control (***MAC***) addresses, and ***IP Addresses***. If you are installing the first access point on a single-access-point network, only one entry will be displayed on this screen

Verify the ***MAC*** addresses shown here against the hardware labels for each access point. This will be especially helpful later in providing or modifying the descriptive “Location” name for each access point.



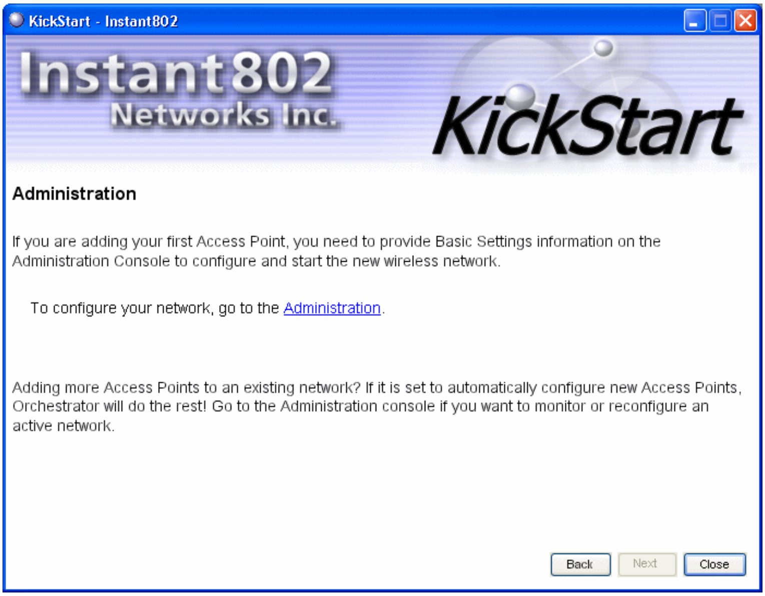
KickStart found 2 Access Point(s).

	Location	MAC Address	Address
	Reception	00:02:b3:02:02:02	192.168.3.14
	unset	00:02:d8:00:00:50	192.168.3.15

Click Next to configure your Access Points.

Click **Next**.

4. Go to the Access Point Administration Web pages by taking the link provided on the KickStart page.



Administration

If you are adding your first Access Point, you need to provide Basic Settings information on the Administration Console to configure and start the new wireless network.

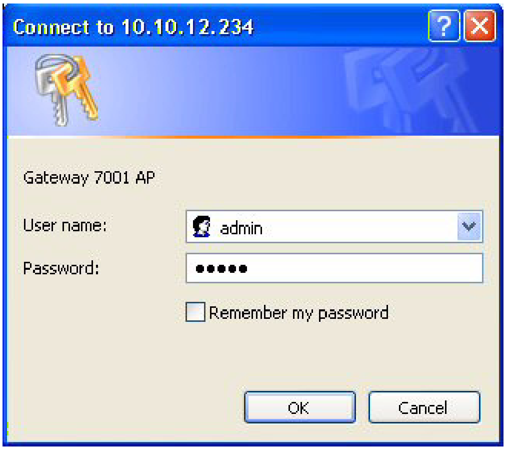
To configure your network, go to the Administration.

Adding more Access Points to an existing network? If it is set to automatically configure new Access Points, Orchestrator will do the rest! Go to the Administration console if you want to monitor or reconfigure an active network.

Note: *KickStart provides a link to the Administration Web pages via the IP address of the first access point of each model. (For more information about model types and clustering see "What Kinds Of APs Can Cluster Together?" on page 56.) The Administration Web pages are a centralized management tool that you can access via the IP address for any access point in a cluster. Once your other access points are configured, you can also link to the Administration Web pages by using the IP address for any of the other 9160 Wireless Gateways in a URL (*http://IPAddressOfAccessPoint*).*

4.5 Log On To The Administration Web Pages

When you follow the link from KickStart to the 9160 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.

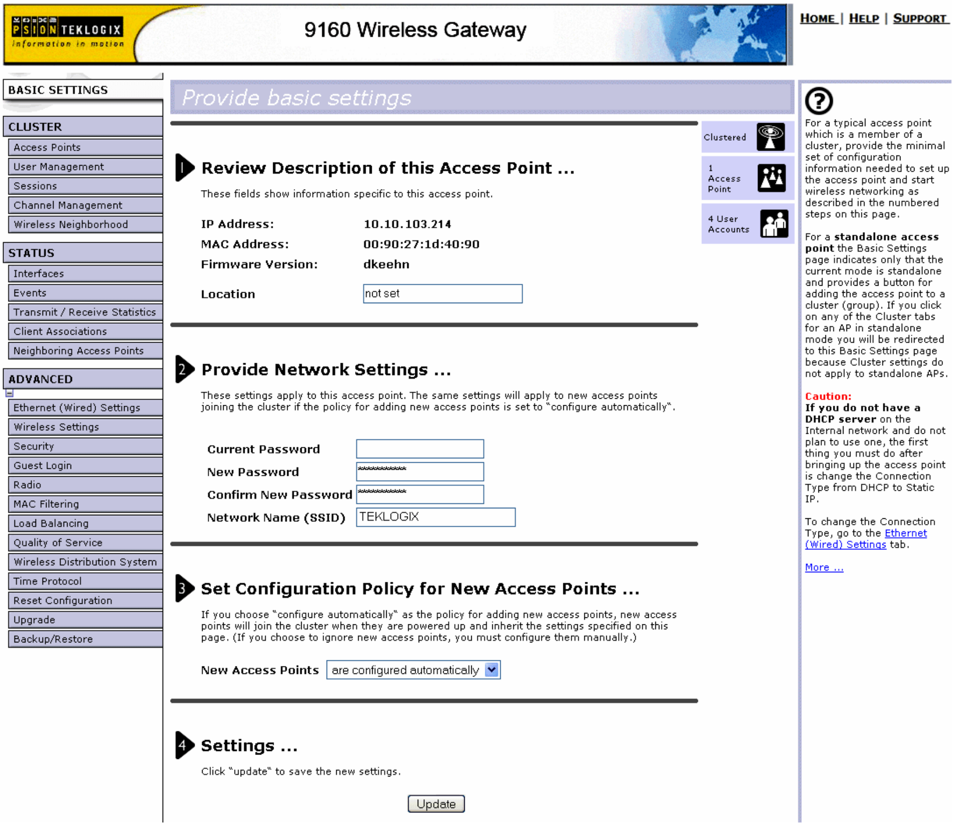
Field	Default Setting
Username	admin
Password	admin The user name is read-only. It cannot be modified.

Table 4.3 Username And Password

Enter the username and password and click **OK**.

4.5.1 Viewing Basic Settings For Access Points

When you first log in, the *Basic Settings* page for 9160 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.



Provide basic settings

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

These fields show information specific to this access point.

IP Address: 10.10.103.214
MAC Address: 00:90:27:1d:40:90
Firmware Version: dkeehn
Location not set

2 **Provide Network Settings ...**

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password
New Password ************
Confirm New Password ************
Network Name (SSID) TEKLOGIX

3 **Set Configuration Policy for New Access Points ...**

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points are configured automatically

4 **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.

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 ...

4.6 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 1-4 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 Administrator Password And Wireless Network Name" on page 49.

3. Set Configuration Policy for New Access Points.

   Choose to configure new access points automatically (as new members of the cluster) or ignore new access points.

   If you set a configuration policy to *configure new access points automatically*, new access points added to this network will join the cluster and be configured automatically based on the settings you defined here. Updates to the Network settings on any cluster member will be shared with all other access points in the group.

   If you chose to *ignore new access points*, then as you add new access points they will run in standalone mode. In standalone mode, an access point does not share the cluster configuration with other access points; it must be configured manually.

   You can always update the settings on a standalone access point to have it join the cluster. You can also remove an access point from a cluster thereby switching it to run in standalone mode.

   For more information, see "Set Configuration Policy For New Access Points" on page 50.

4. Start Wireless Networking.

   Click the **Update** button to activate the wireless network with these new settings. For more information, see "Update Basic Settings" on page 51.

4.6.1 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 Wireless Gateway” on page 23.

4.7 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.

4.7.1 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.

4.7.2 Test LAN Connectivity With Wireless Clients

Test the 9160 Wireless Gateway by trying to detect it and associate with it from some wireless client devices. (See “Wireless Client Computers” on page 27 in the ***PreLaunch Checklist*** for information on requirements for these clients.)

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

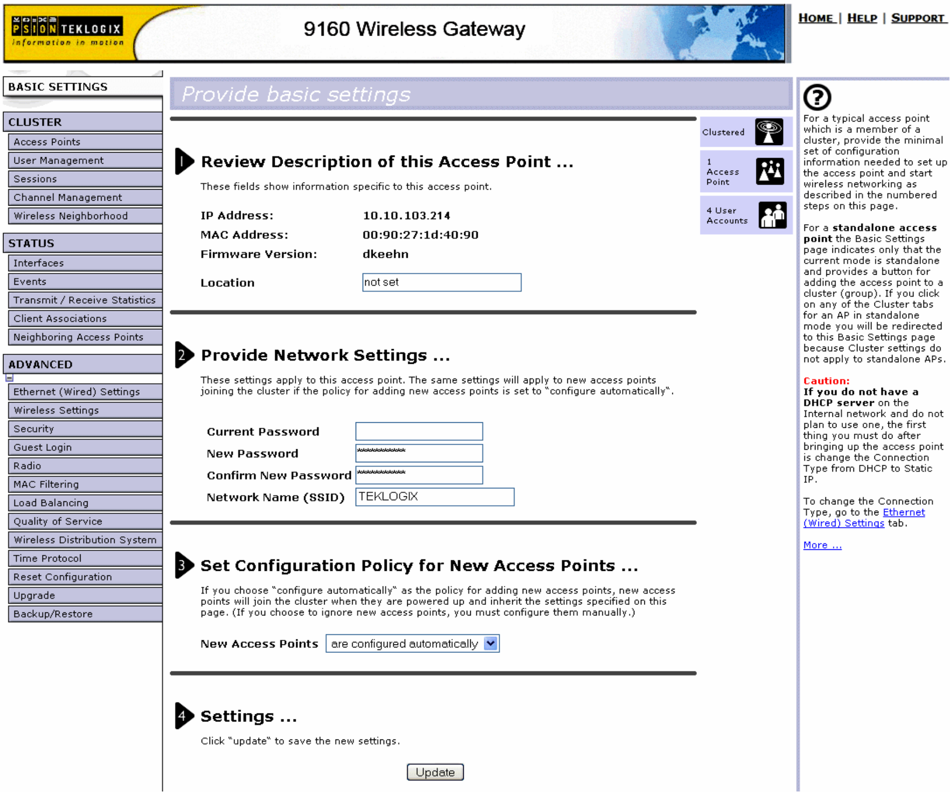
Once you have the wireless network up and running and have tested against the access point with some wireless clients, you can add in more layers of security, add users, configure a Guest interface, and fine-tune performance settings.

CONFIGURING BASIC SETTINGS 5

5.1 Navigating To Basic Settings

To configure initial settings, click *Basic Settings*.

If you use Kickstart to link to the Administration Web pages, the *Basic Settings* page is displayed by default.



Provide basic settings

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

These fields show information specific to this access point.

IP Address: 10.10.103.214
MAC Address: 00:90:27:1d:40:90
Firmware Version: dkeehn
Location: not set

2 **Provide Network Settings ...**

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password:
New Password: ***********
Confirm New Password: ***********
Network Name (SSID): TEKLOGIX

3 **Set Configuration Policy for New Access Points ...**

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points: are configured automatically

4 **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.

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.

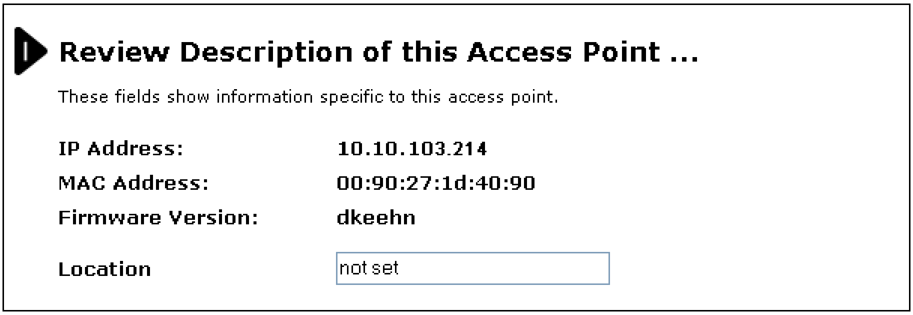
Caution:
If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

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

More ...

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: 10.10.103.214

MAC Address: 00:90:27:1d:40:90

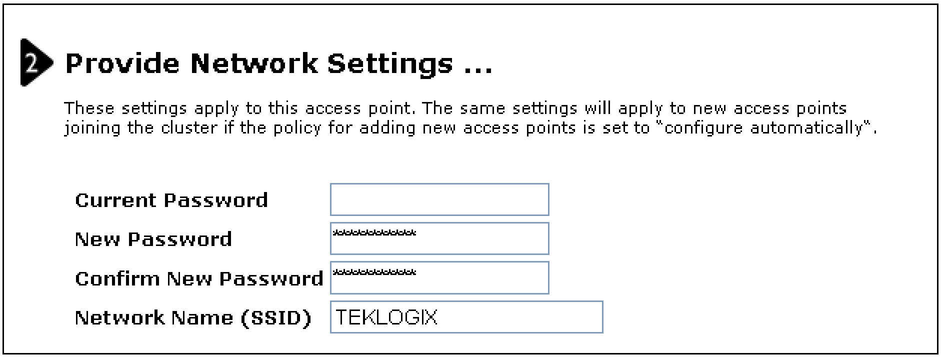
Firmware Version: dkeehn

Location: not set

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 104).
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 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 219.
Location	Specify a location description for this access point.

Table 5.1 Basic Settings Screen Options

5.3 Provide Administrator Password And Wireless Network Name



Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

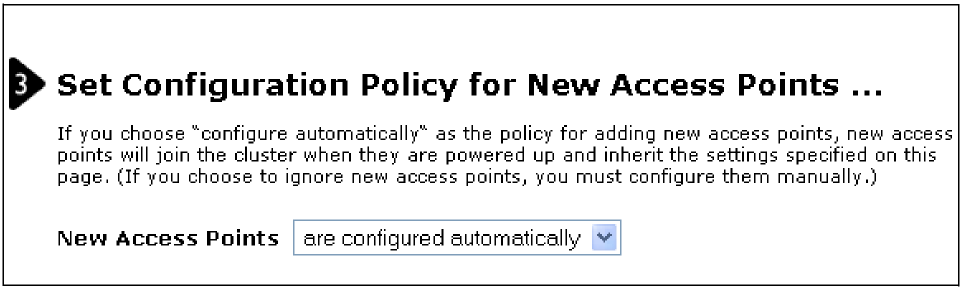
Current Password	
New Password	************
Confirm New Password	************
Network Name (SSID)	TEKLOGIX

Field	Description
Administrator 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.
Administrator Password (again)	Re-enter the new administrator password to confirm that you typed it as intended.
Wireless 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 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 synch but there is no guarantee that all configuration changes specified by multiple users will be applied.*

5.4 Set Configuration Policy For New Access Points



Set Configuration Policy for New Access Points ...

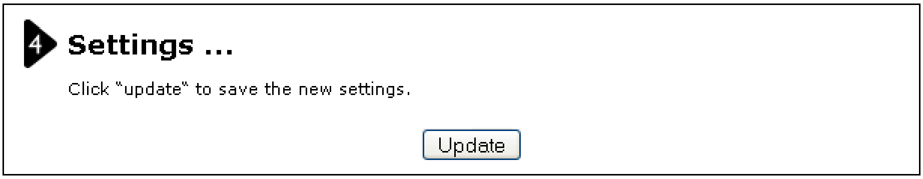
If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points: are configured automatically

Field	Description
New Access Points	Choose the policy you want to put in effect for adding *New Access Points* to the network. • If you choose "are configured automatically", then when a new access point is added to the network it automatically joins the existing *cluster*. The cluster configuration is copied to the new access point, and no manual configuration is required to deploy it. • If you choose "are ignored", new access points will not join the cluster; they will be considered *standalone*. You need to configure standalone access points manually via KickStart and the Administration Web pages residing on the standalone access points. (To get to the Web page for a standalone access point, use its IP address in a URL as follows: *http://IPAddressOfAccessPoint.*) ***Note:*** *If you change the policy so that new access points "are ignored", then any new access points you add to the network will not join the cluster. Existing clustered access points will not be aware of these standalone APs. Therefore, if you are viewing the Administration Web pages via the IP address of a clustered access point, the new standalone APs will not show up in the list of access points on the* Cluster, Access Points *tab. The only way to see a standalone AP is to browse to it directly by using its IP address in the URL.* *If you later change the policy back to the default so that new access points "are configured automatically", all subsequent new APs will automatically join the cluster. Standalone APs, however, will stay in standalone mode until you explicitly add them to the cluster.* *For information on how to add standalone APs to the cluster, see "Adding An Access Point To A Cluster" on page 62.*

Table 5.3 Configuration Policy For New Access Points

5.5 Update Basic Settings



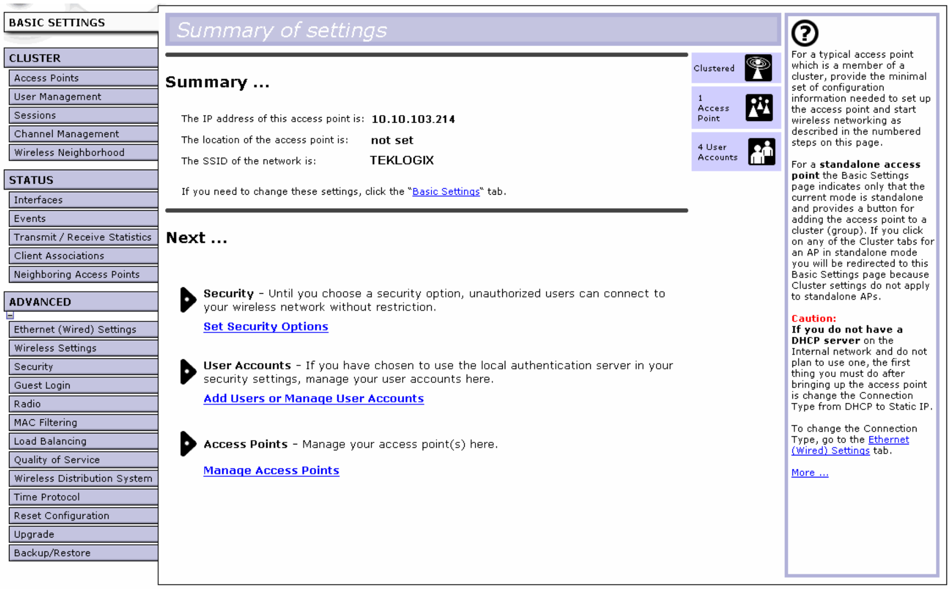
Settings ...

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.

5.6 Summary Of Settings

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



Summary of settings

Summary ...

The IP address of this access point is: 10.10.103.214

The location of the access point is: not set

The SSID of the network is: TEKLOGIX

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 13: "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.

5.7 Basic Settings For A Standalone Access Point

The *Basic Settings* tab for a standalone access point 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 on the Administration pages for an access point in standalone mode, you will be re-directed to the *Basic Settings* page because Cluster settings do not apply to standalone APs.

For more information see "Standalone Mode" on page 58 and "Adding An Access Point To A Cluster" on page 62.

5.8 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.

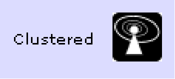
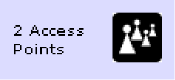
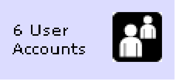
Icon	Description
	When one or more APs on your network are available for service, the "Wireless Network Available" icon is shown. The clustering icon indicates whether the current access point is "Clustered" or "Not Clustered" (that is, standalone). For information about clustering, see "Understanding Clustering" on page 56.
	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".
	Then 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 131 and "WPA/WPA2 Enterprise (RADIUS)" on page 136, which are the two security modes that offer the option of using the built-in authentication server.

Table 5.4 Indicator Icons

MANAGING ACCESS POINTS & CLUSTERS 6

6.1 Overview

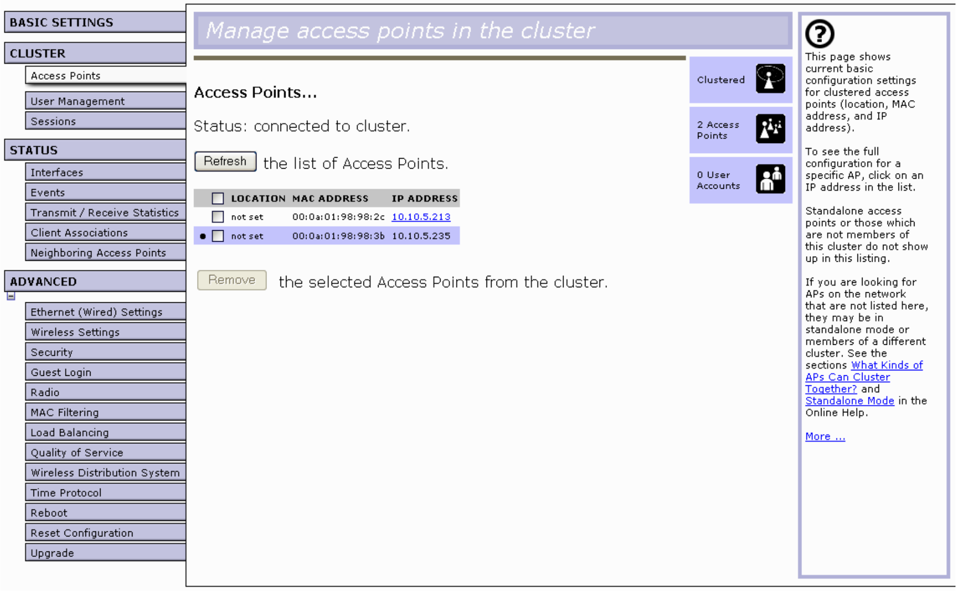
The 9160 Wireless Gateway shows current basic configuration settings for clustered access points (location, IP address, MAC address, status, and availability) and provides a way of navigating to the full configuration for specific APs if they are cluster members.

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 discover it via Kickstart, or know the IP address of the access point and use it in a URL (*http://IPAddressOfAccessPoint*).

Note: *The 9160 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 synch 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: connected to cluster.

Refresh the list of Access Points.

	LOCATION	MAC ADDRESS	IP ADDRESS
□	not set	00:0a:01:98:98:2c	10.10.5.213
● □	not set	00:0a:01:98:98:3b	10.10.5.235

Remove the selected Access Points from the 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 Wireless Gateway is the ability to form a dynamic, configuration-aware group (called a *cluster*) with other 9160 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 Wireless Gateway administration. You cannot create multiple clusters on a single wireless network (***SSID***). Only one cluster per wireless network is supported.

6.3.2 How Many APs Can A Cluster Support?

Up to eight access points are supported in a cluster at any one time. If a new AP is added to a network with a cluster that is already at full capacity, the new AP is added in *standalone mode*. Note that when the cluster is full, extra APs are added in standalone mode regardless of the configuration policy in effect for new access points.

For related information, see “Cluster Mode” on page 58, “Standalone Mode” on page 58, and “Set Configuration Policy For New Access Points” on page 50.

6.3.3 What Kinds Of APs Can Cluster Together?

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

- 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 Wireless Gateway clustering in any way. However, it is helpful to understand the clustering behaviour for administration purposes:

- Access points of the same model will form a cluster.
- 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 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.
- Configuration policy.
- 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 synched across the cluster. See "Stopping/Starting Automatic Channel Assignment" on page 84*

- 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 Mode

When an access point is a cluster member, it is considered to be in cluster mode. You define whether you want new access points to join the cluster or not via the configuration policy you set in the *Basic Settings*. (See “Set Configuration Policy For New Access Points” on page 50.) You can re-set an access point in cluster mode to standalone mode. (See “Removing An Access Point From The Cluster” on page 61.)

Note: *When the cluster is full (eight APs is the limit), extra APs are added in standalone mode regardless of the configuration policy in effect for new access points. See “How Many APs Can A Cluster Support?” on page 56.*

6.3.6 Standalone Mode

The 9160 Wireless Gateway can be configured in *standalone* mode. In standalone mode, an access point is not a member of the cluster and does not share the cluster configuration, but rather requires manual configuration that is not shared with other access points. (See “Set Configuration Policy For New Access Points” on page 50 and “Removing An Access Point From The Cluster” on page 61.)

Standalone access points are not listed on the *Cluster, Access Points* tab in the Administration UIs of APs that are cluster members. You need to know the IP addresses for standalone access points in order to configure and manage them directly. (See “Navigating To An AP By Using Its IP Address In A URL” on page 63.)

The *Basic Settings* tab for a standalone access point 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 on the Administration pages for an access point in standalone mode, you will be redirected to the *Basic Settings* page because Cluster settings do not apply to standalone APs.

Note: *When the cluster is full (eight APs is the limit), extra APs are added in standalone mode regardless of the configuration policy in effect for new access points. See “How Many APs Can A Cluster Support?” on page 56.*

You can re-enable cluster mode on a standalone access point. (See “Adding An Access Point To A Cluster” on page 62.)

6.3.7 Cluster Formation

A cluster is formed when the first 9160 Wireless Gateway is configured. (See Chapter 4: “Quick Steps For Setup And Launch” and Chapter 5: “Configuring Basic Settings”.)

If a cluster configuration policy is in place, when a new access point is deployed, it attempts to rendezvous with an existing cluster.

If it is unable to locate a cluster, then it establishes a new cluster on its own.

If it locates a cluster but is rejected because the cluster is full, or the clustering policy is to ignore new access points, then the access point will deploy in standalone mode.

6.3.8 Cluster Size And Membership

The upper limit of a cluster is eight access points. The “Cluster” Web administration pages provides a real-time, visual indicator of the number of access points in the current cluster and warn when the cluster has reached capacity. (See “Configure ‘Basic Settings’ And Start The Wireless Network” on page 42.)

If a cluster is present but is already full, new access points will deploy in standalone mode.

6.3.9 Intra-Cluster Security

To ensure that the security of the cluster as a whole is equivalent to the security of a single access point, communication of certain data between access points in a cluster is done using Secure Sockets Layer (typically referred to as SSL) with private key encryption.

Both the cluster configuration file and the user database are transmitted among access points using SSL.

6.3.10 Auto-Synch Of Cluster Configuration

If you are making changes to the AP configuration that require a relatively large amount of processing (such as adding several new users), you may encounter a synchronization progress bar after clicking "Update" on any of the Administration pages. The progress bar indicates that the system is busy performing an auto-synch of the updated configuration to all APs in the cluster. The Administration Web pages are not editable during the auto-synch.

Note that auto-synchronization always occurs during configuration updates that affect the cluster, but the processing time is usually negligible. The auto-synch progress bar is displayed only for longer-than-usual wait times.

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, 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.

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

6.5 Modifying The Location Description

To make modifications to the location description:

1. Navigate to the *Basic Settings* tab.
2. Update the Location description in section 1 under “Review Description of this Access Point.”
3. Click **Update** button to apply the changes.

6.6 Removing An Access Point From The Cluster

To remove an access point from the cluster, do the following.

1. Click the checkbox next to the access point so that the box is checked.

2. Click **Remove from 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 shows the deleted AP or shows an incomplete display; refer to the information on Cluster Recovery in Appendix D: "Troubleshooting" .*

6.7 Adding An Access Point To A Cluster

To add an access point that is currently in standalone mode back into 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 63.)

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

2. Click the **Basic Settings** tab in the Administration pages for the standalone access point.

   The *Basic Settings* tab for a standalone access point indicates that the current mode is standalone and provides a button for adding the access point to a cluster (group).

Note: *If you click on any of the Cluster tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.*

3. Click the **Join Cluster** button.

   The access point is now a cluster member. Its Status (Mode) on the *Cluster, Access Points* tab now indicates "cluster" instead of "standalone".

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; refer to the information on Cluster Recovery in Appendix D: "Troubleshooting" .*

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

In general, the 9160 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.

6.8.1 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.

If you do not know the IP address for a standalone access point, use Kickstart to find all the APs on the network and you should be able to derive which ones are standalone by comparing KickStart findings with access points listed on the *Cluster, Access Points* tab. The APs that Kickstart finds that are not shown on the this tab are probably standalone APs. (For more information on using Kickstart, see "Run KickStart To Find Access Points On The Network" on page 37.)

MANAGING USER ACCOUNTS 7

7.1 Overview

The 9160 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 131 in Chapter 13: “Configuring Security”).
- WPA with RADIUS mode (see “WPA/WPA2 Enterprise (RADIUS)” on page 136 in Chapter 13: “Configuring Security”).

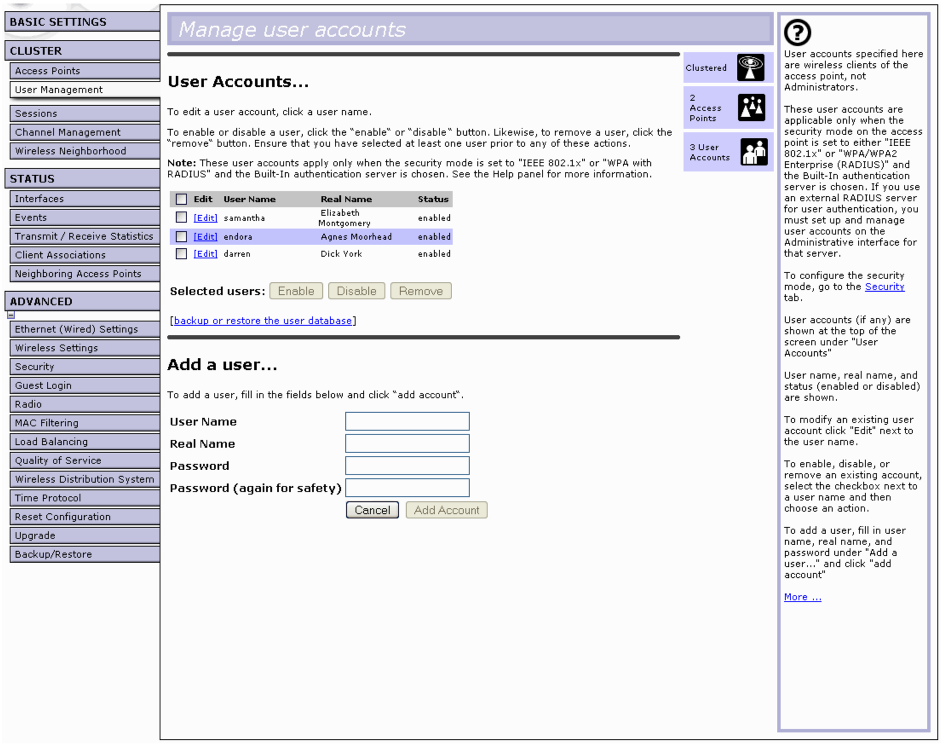
You have the option of using either the internal RADIUS server embedded in the 9160 Wireless Gateway or an external RADIUS server that you provide. If you use the embedded RADIUS server, use the Administration Web page on the access point to set up and manage user accounts. If you are using an external 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 edit a user account, click a user name.

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	User Name	Real Name	Status
□	[Edit]	samantha	Elizabeth Montgomery	enabled
□	[Edit]	endora	Agnes Moorhead	enabled
□	[Edit]	darren	Dick York	enabled

[backup or restore the user database]

Add a user...

To add a user, fill in the fields below and click "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...* . User name, real name, and status (enabled or disabled) 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 70.)

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 user name. User names 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

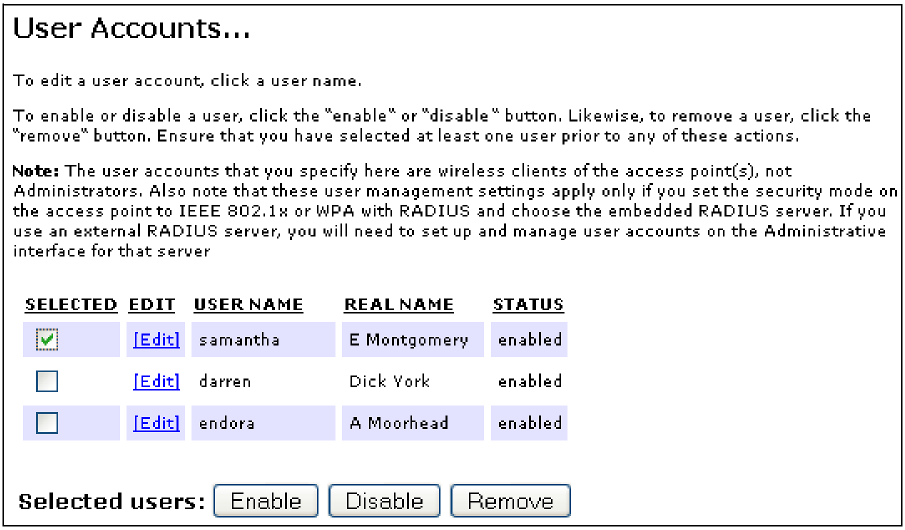
2. When you have filled in the fields, click **Add Account** to add the account.

   The new user is then displayed in the *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 user name so that the box is checked.



User Accounts...

To edit a user account, click a user name.

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: The user accounts that you specify here are wireless clients of the access point(s), not Administrators. Also note that these user management settings apply only if you set the security mode on the access point to IEEE 802.1x or WPA with RADIUS and choose the embedded RADIUS server. If you use an external RADIUS server, you will need to set up and manage user accounts on the Administrative interface for that server

SELECTED	EDIT	USER NAME	REAL NAME	STATUS
☑	[Edit]	samantha	E Montgomery	enabled
□	[Edit]	darren	Dick York	enabled
□	[Edit]	endora	A Moorhead	enabled

Selected users:

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 user name 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 user name 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 user name 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.)

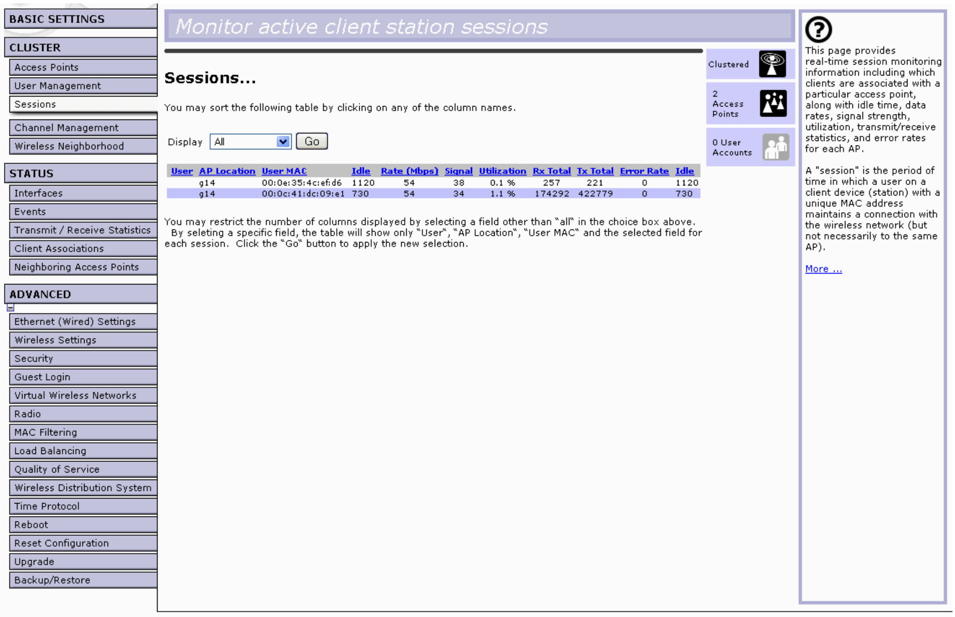
   Click the **Cluster, User Management** tab to see the restored user accounts.

SESSION MONITORING 8

The 9160 Wireless Gateway provides real-time session monitoring information, including which clients are associated with a particular access point, data rates, transmit/receive statistics, signal strength, and idle time.

8.1 Navigating To Session Monitoring

To view session monitoring information, click the **Cluster, Sessions** tab.



Monitor active client station sessions

Sessions...

You may sort the following table by clicking on any of the column names.

User	AP Location	User MAC	Idle	Rate (Mbps)	Signal	Utilization	Rx Total	Tx Total	Error Rate	Idle
	g14	00:0e:35:4c:ef:d6	1120	54	38	0.1 %	257	221	0	1120
	g14	00:0c:41:dc:09:e1	730	54	34	1.1 %	174292	422779	0	730

You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By seleting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

This page provides real-time session monitoring information including which clients are associated with a particular access point, along with idle time, data rates, signal strength, utilization, transmit/receive statistics, and error rates for each AP.

A "session" is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network (but not necessarily to the same AP).

8.2 Understanding Session Monitoring Information

The *Sessions* page shows information on client stations associated with access points in the cluster. Each client is identified by user name and user ***MAC*** address, along with the AP (location) to which it is currently connected.

To view a particular statistic for client sessions, select an item from the *Display* drop-down list and click **Go**. You can view information on Idle Time, Data Rate, Signal, Utilization, and so on; all of which are described in detail in Table 8.1.

A "session" in this context is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the client logs on to the network, and the session ends when the client either logs off intentionally or loses the connection for some other reason.

Notes: *A session is not the same as an association, which describes a client connection to a particular access point. A client network connection can shift from one clustered AP to another within the context of the same session. A client station can roam between APs and maintain the session.*

For information about monitoring associations and link integrity monitoring, see "Associated Wireless Clients" on page 214.

Details about the session information shown is described below.

Field	Description
User Name	Indicates the client user name of IEEE 802.1x clients. ***Note:*** *This field is relevant only for clients that are connected to APs using IEEE 802.1x security mode and local authentication server. (For more information about this mode, see "IEEE 802.1x" on page 131.) For clients of APs using IEEE 802.1x with RADIUS server or other security modes, no user name will be shown here.*
AP Location	Indicates the location of the access point. This is derived from the location description specified on the *Basic Settings* tab.
User MAC Address	Indicates the MAC address of the user's client device (station). A ***MAC*** address is a hardware address that uniquely identifies each node of a network.

Table 8.1 Client Session Statistics

Field	Description
Idle Time	Indicates the amount of time this station has remained inactive. A station is considered to be “idle” when it is not receiving or transmitting data.
Data Rate	The speed at which this access point is transferring data to the specified client. The data transmission rate is measured in *megabits per second* (Mbps). This value should fall within the range of the advertised rate set for the ***IEEE 802.1x*** mode in use on the access point. For example, 6 to 54Mbps for 802.11a,
Signal	Indicates the strength of the radio frequency (RF) signal the client receives from the access point. The measure used for this is an ***IEEE 802.1x*** value known as *Received Signal Strength Indication* (RSSI), and will be a value between 0 and 100. RSSI is determined by a an IEEE 802.1x mechanism implemented on the network interface card (***NIC***) of the client station.
Utilization	Utilization rate for this station. For example, if the station is “active” (transmitting and receiving data) 90% of the time, and inactive 10% of the time, its “utilization rate” is 90%.
Receive Total	Indicates number of total packets received by the client during the current session.
Transmit Total	Indicates number of total packets transmitted to the client during this session.
Error Rate	Indicates the percentage of time frames are dropped during transmission on this access point.

Table 8.1 Client Session Statistics

8.3 Viewing Session Information For Access Points

You can view session information for all access points on the network at the same time, or set the display to show session information for a specified access point chosen from the drop-down menu at the top of the screen.

To view information on all access points, select the **Show all access points** radio button at the top of the page.

To view session information on a particular access point, select the **Show only this access point** radio button and choose the access point name from the drop-down menu.

8.4 Sorting Session Information

To order (sort) the information shown in the tables by a particular indicator, click on the column label by which you want to order things. For example, if you want to see the table rows ordered by Utilization rate, click on the **Utilization** column label. The entries will be sorted by Utilization rate.

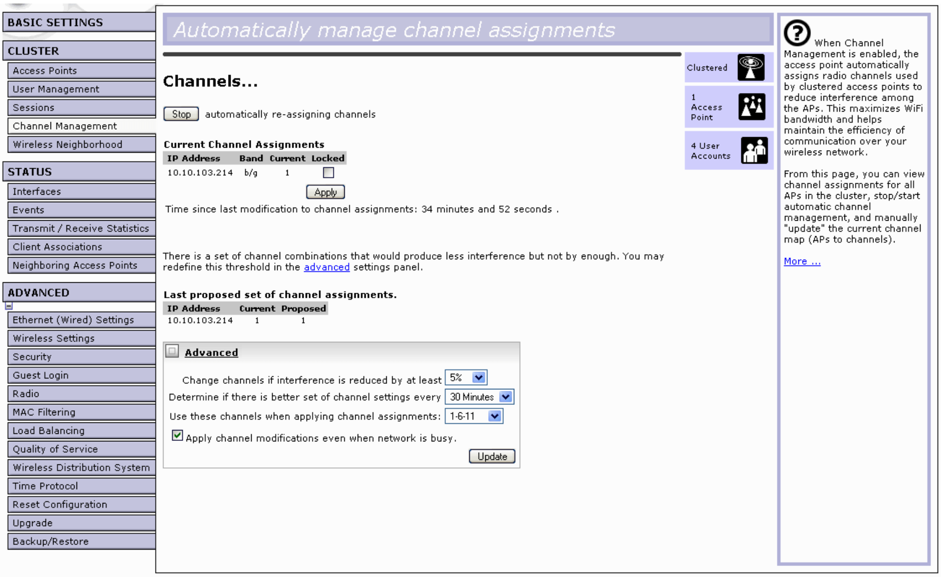
8.5 Refreshing Session Information

You can force an update of the information displayed on the *Session Monitoring* page by clicking the **Refresh** button.

CHANNEL MANAGEMENT 9

9.1 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	Band	Current	Locked
10.10.103.214	b/g	1	□

Apply

Time since last modification to channel assignments: 34 minutes and 52 seconds .

There is a set of channel combinations that would produce less interference but not by enough. You may redefine this threshold in the advanced settings panel.

Last proposed set of channel assignments.

IP Address	Current	Proposed
10.10.103.214	1	1

□ **Advanced**

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

Determine if there is better set of channel settings every: 30 Minutes

Use these channels when applying channel assignments: 1-6-11

☑ Apply channel modifications even when network is busy.

Update

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 ...

9.2 Understanding Channel Management

When *Channel Management* is enabled, the 9160 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 84.)

9.2.1 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*).

9.2.2 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.

9.2.3 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 9.1 on page 83.

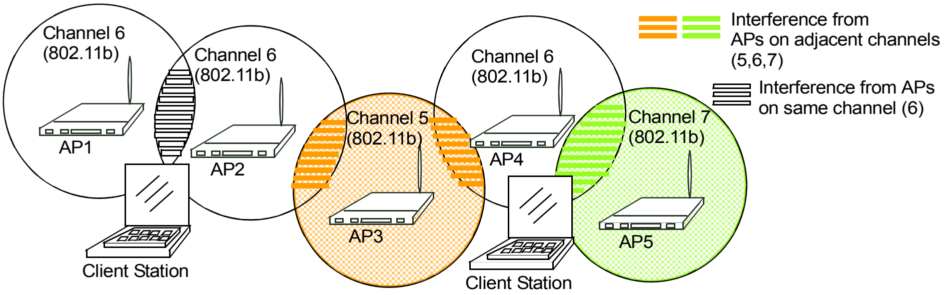


Figure 9.1 Without Automatic Channel Management

With automated channel management, APs in the cluster are automatically re-assigned to non-interfering channels as shown in Figure 9.2.

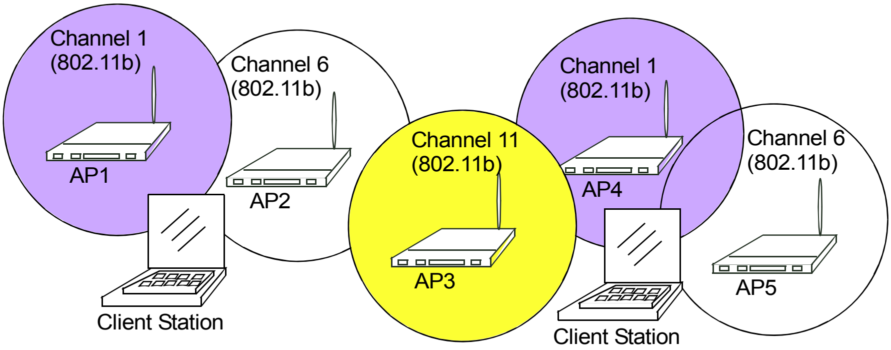


Figure 9.2 With Channel Management Enabled

9.3 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 84.
- “Viewing Current Channel Assignments And Setting Locks” on page 85.
- “Update Current Channel Settings (Manual)” on page 86.
- “Viewing Last Proposed Set Of Changes” on page 86.
- “Configuring Advanced Settings (Customizing And Scheduling Channel Plans)” on page 86.
- “Update Advanced Settings” on page 88.

9.3.1 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 synched 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.)

9.3.2 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 (a or b), 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.
Band	Indicates the band (b/g or a) on which the access point is broadcasting.
Current	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 9.3 Current Channel Settings

9.3.2.1 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.

9.3.3 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 9.4 AP’s Channel Plan

9.3.4 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 re-configure 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 channels 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 9.5 Advanced Settings

9.3.4.1 Update Advanced Settings

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

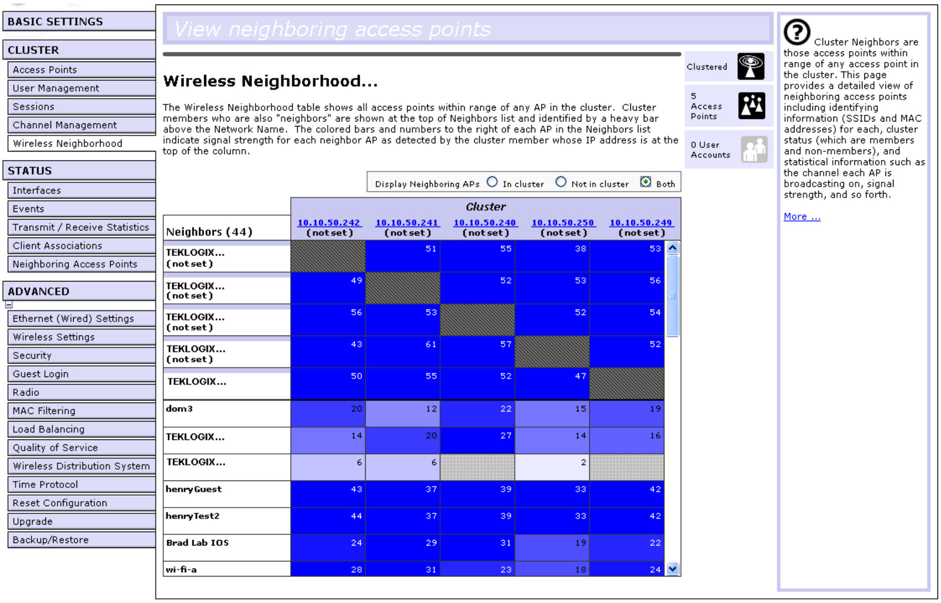
Advanced Settings will take effect when they are applied, and influence how automatic channel management is performed. (The new interference reduction minimum, scheduled tuning interval, channel set, and network busy settings will be taken into account for automated and manual updates.)

WIRELESS NEIGHBORHOOD 10

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.

10.1 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 neighbor AP as 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 (44)	10.10.50.242 (not set)	10.10.50.241 (not set)	10.10.50.240 (not set)	10.10.50.250 (not set)	10.10.50.249 (not set)
TEKLOGIX... (not set)	▨	51	55	38	53
TEKLOGIX... (not set)	49	▨	52	53	56
TEKLOGIX... (not set)	56	53	▨	52	54
TEKLOGIX... (not set)	43	61	57	▨	52
TEKLOGIX...	50	55	52	47	▨
dom3	20	12	22	15	19
TEKLOGIX...	14	20	27	14	16
TEKLOGIX...	6	6	░	2	░
henryGuest	43	37	39	33	42
henryTest2	44	37	39	33	42
Brad Lab IOS	24	29	31	19	22
wi-fi-a	28	31	23	18	24

Cluster Neighbors are 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 10.1 Neighbor APs Both In Cluster And Not In Cluster

10.2 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.

10.3 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 10.3 on page 94.

Table 10.2 Wireless Neighborhood Statistics

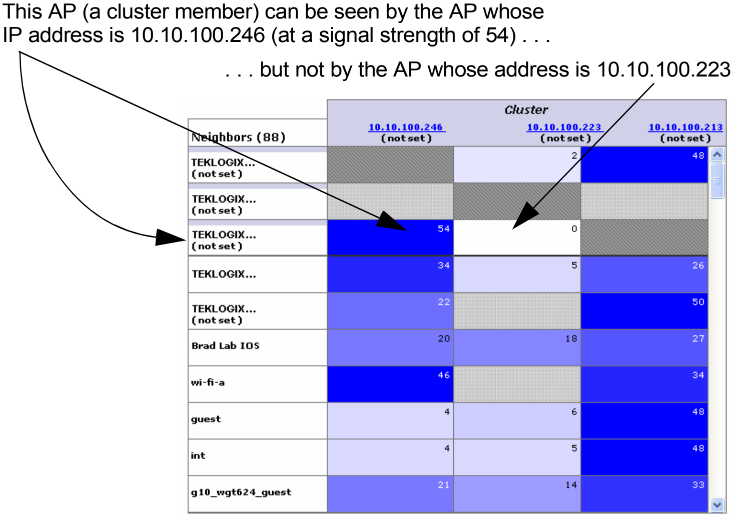
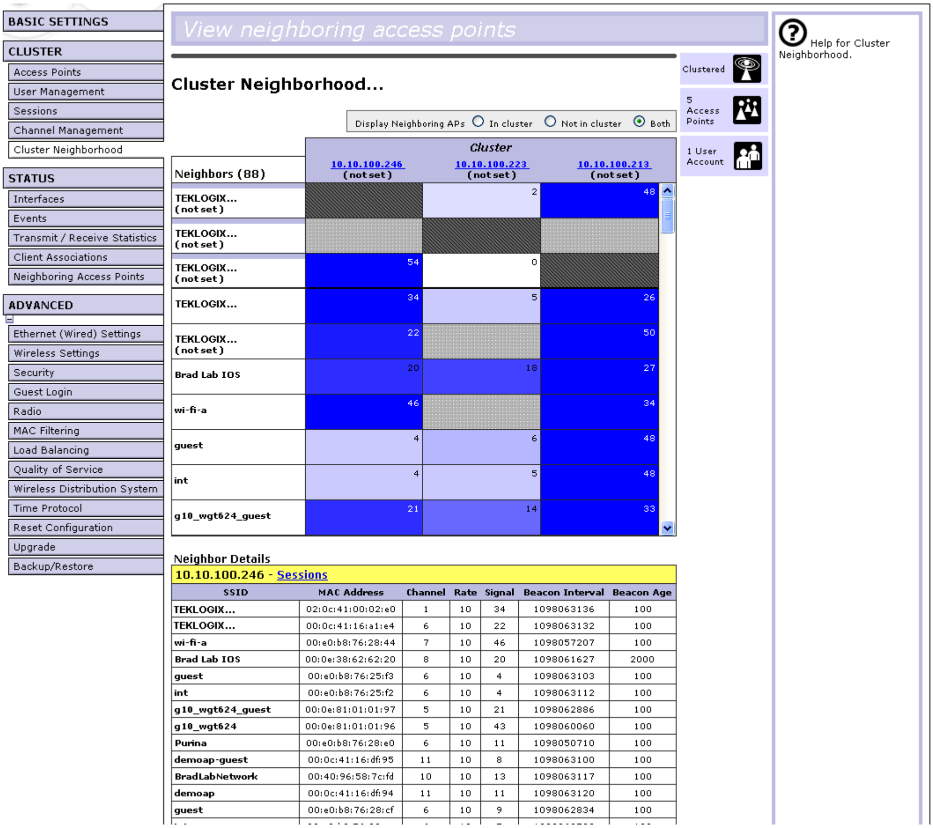
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><em>Neighbors</em></td><td>
Access points which are neighbors of one or more of the clustered APs are listed in the left column by SSID (Network Name). An access point which is detected as a neighbor of a cluster member can also be a cluster 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...</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><strong>Dark Blue Bar</strong> - 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><strong>Lighter Blue Bar -</strong> 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><strong>White Bar</strong> - 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><strong>Light Gray Bar -</strong> 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><strong>Dark Gray Bar</strong> - A dark gray bar and no signal strength number indicates this <em>is</em> 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 10.2 Wireless Neighborhood Statistics

10.4 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.



Cluster Neighborhood...

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

	Cluster		
Neighbors (88)	10.10.100.246 (not set)	10.10.100.223 (not set)	10.10.100.213 (not set)
TEKLOGIX... (not set)	▨	2	48
TEKLOGIX... (not set)	▒	▨	▒
TEKLOGIX... (not set)	54	0	▨
TEKLOGIX...	34	5	26
TEKLOGIX... (not set)	22	▒	50
Brad Lab IOS	20	18	27
wi-fi-a	46	▒	34
guest	4	6	48
int	4	5	48
g10_wgt624_guest	21	14	33

Neighbor Details

10.10.100.246 - Sessions

SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
TEKLOGIX...	02:0c:41:00:02:e0	1	10	34	1098063136	100
TEKLOGIX...	00:0c:41:16:a1:e4	6	10	22	1098063132	100
wi-fi-a	00:e0:b8:76:28:44	7	10	46	1098057207	100
Brad Lab IOS	00:0e:38:62:62:20	8	10	20	1098061627	2000
guest	00:e0:b8:76:25:f3	6	10	4	1098063103	100
int	00:e0:b8:76:25:f2	6	10	4	1098063112	100
g10_wgt624_guest	00:0e:81:01:01:97	5	10	21	1098062886	100
g10_wgt624	00:0e:81:01:01:96	5	10	43	1098060060	100
Purina	00:e0:b8:76:28:e0	6	10	11	1098050710	100
demoap-guest	00:0c:41:16:df:95	11	10	8	1098063100	100
BradLabNetwork	00:40:96:58:7c:fd	10	10	13	1098063117	100
demoap	00:0c:41:16:df:94	11	10	11	1098063120	100
guest	00:e0:b8:76:28:cf	6	10	9	1098062834	100

Figure 10.3 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 12: “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 Settings*. (See Chapter 16: “Configuring 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 Settings*. (See Chapter 16: “Configuring Radio Settings”.)
Last Beacon (Beacon Age)	Shows the date and time of the most recent beacon was transmitted from the access point.

Table 10.4 Access Point Statistics

THE ETHERNET (WIRED) INTERFACE 11

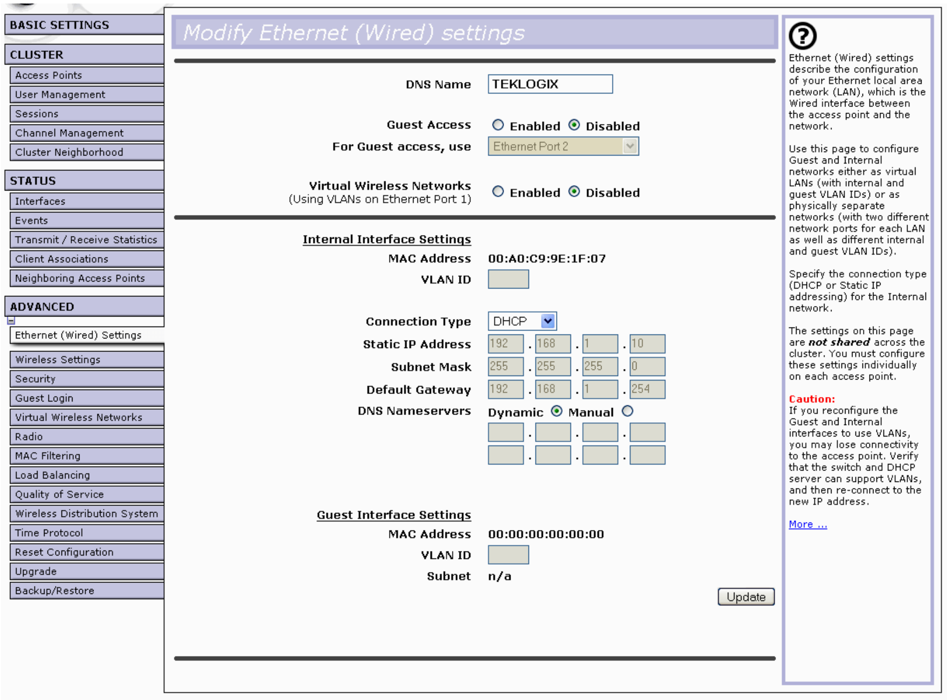
Ethernet (Wired) Settings describe the configuration of your ***Ethernet*** local area network (***LAN***).

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 Wireless Gateway:

11.1 Navigating To Ethernet (Wired) Settings

To set the wired address for an access point, navigate to the *Advanced, Ethernet (Wired) Settings* tab, and update the fields as described below.



Modify Ethernet (Wired) settings

DNS Name: TEKLOGIX

Guest Access: ○ Enabled ● Disabled

For Guest access, use: Ethernet Port 2

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

Internal Interface Settings

MAC Address: 00:A0:C9:9E:1F:07

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.

More ...

11.1.1 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 11.1 Setting DNS Name

11.1.2 Enabling Or Disabling Guest Access

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

11.1.2.1 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 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 12: “Setting the Wireless Interface”. For an overview of how to set up the Guest interface, see Chapter 14: “Setting up Guest Access”.)

11.1.2.2 Enabling Or Disabling Guest Access

The 9160 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 Wireless Gateway ships with Guest Access **disabled**. • To enable Guest Access, click **Enabled**. • To disable Guest Access, click **Disabled**.

Table 11.2 Enabling/Disabling Guest Access

11.1.2.3 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 11.3.

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, use	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 104. ***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*** Advanced, Ethernet (Wired) Settings ***page, 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.)***

Table 11.3 Specifying A Virtual Guest Network

11.1.3 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 149.

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 149.) • Select **Disabled** to disable the VLAN for the Internal network, and for any additional virtual networks on this access point.

11.1.4 Configuring Internal Interface Ethernet Settings

To configure Ethernet (wired) settings for the Internal LAN, fill in the fields as described in Table 11.4.

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 ***802.1Q*** frames. The access point must be able to reach the DHCP server. Check with the Administrator regarding the VLAN and DHCP configurations.

Table 11.4 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 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 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 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 The Configuration To Factory Defaults” on page 218.
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 11.4 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 **Manual**, you should assign static IP addresses manually. • 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.)

Table 11.4 Ethernet Settings For Internal LAN

11.1.5 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 11.5 Configuring Guest Interface Ethernet Settings

11.1.6 Updating Settings

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

SETTING THE WIRELESS INTERFACE 12

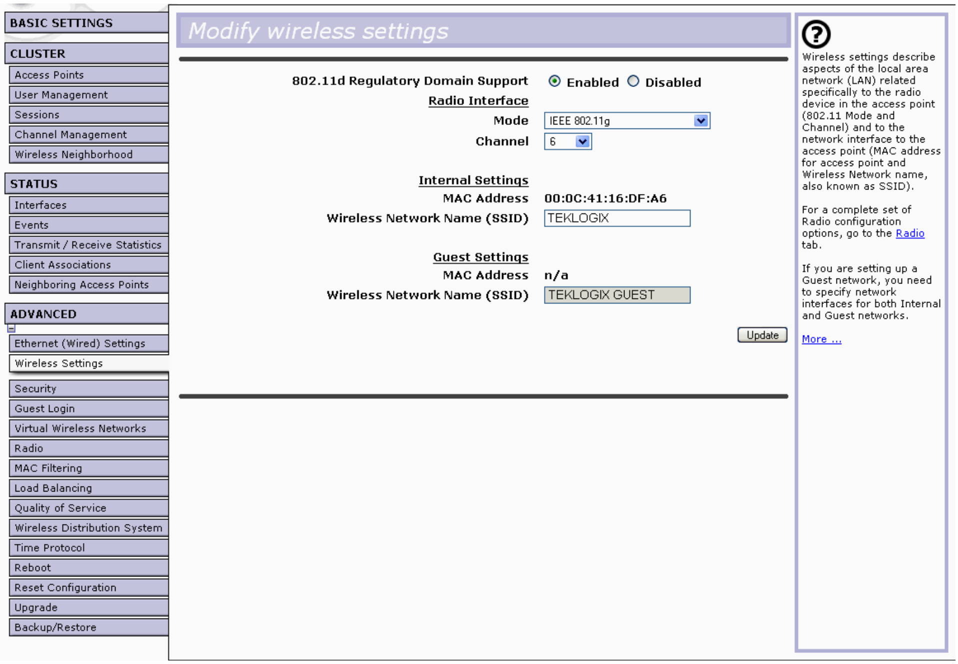
Wireless Settings describes aspects of the local area network (***LAN***) related specifically to the radio device in the access point (***802.11*** Mode and ***Channel***) and to the network interface to the access point (***MAC*** address for access point and Wireless Network name, also known as ***SSID***).

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

12.1 Navigating To Wireless Settings

To set the wireless address for an access point, navigate to the *Advanced, Wireless Settings* tab, 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

Radio Interface
Mode: IEEE 802.11g
Channel: 6

Internal Settings
MAC Address: 00:0C:41:16:DF:A6
Wireless Network Name (SSID): TEKLOGIX

Guest Settings
MAC Address: n/a
Wireless Network Name (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.

12.2 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.

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**. ***Note:*** *The IEEE **802.11d** defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. IEEE 802.11d allows client stations to operate in any country without reconfiguration. The 9160 Wireless Gateway must be configured by the Manufacturer via the command line interface (CLI) country codes for operation in a particular country.*

Table 12.1 802.11d Regulatory Domain Support

12.3 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 12.2 Radio Interface Settings

Field	Description
Mode	The *Mode* defines the *Physical Layer* (***PHY***) standard being used by the radio. The 9160 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 12.2 Radio Interface Settings

12.4 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 12.3.

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 12.3 Wireless LAN Settings

12.5 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 12.4. Configuring an access point with two different network names (SSIDs) allows you to leverage the Guest interface feature on the 9160 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 12.4 Guest Network Wireless Settings

12.6 Updating Settings

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

CONFIGURING SECURITY 13

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

13.1 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 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: “Configuring Security Settings On Wireless Clients”.

13.1.1 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, plain-text mode (no security) 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 122)

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.

13.1.2 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 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 Plain-text" on page 117.
- "When To Use Static WEP" on page 117.
- "When To Use IEEE 802.1x" on page 118.
- "When To Use WPA/WPA2 Personal (PSK)" on page 119.
- "When To Use WPA/WPA2 Enterprise (RADIUS)" on page 120.

13.1.2.1 When To Use Plain-text

Plain-text mode 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

Plain-text mode is **not recommended** for regular use on the Internal network because it is not secure.

Plain-text mode 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, use plain-text mode 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 plain-text mode, see “Plain-text” on page 126.

13.1.2.2 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 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 13.1 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 126.

13.1.2.3 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 Wireless Gateway embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

Table 13.2 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/WPA2 Enterprise (RADIUS) mode instead and check the "Allow non-WPA IEEE 802.1x clients" checkbox** to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA and WPA2 clients.

See Also

For information on how to configure IEEE 802.1x security mode, see "IEEE 802.1x" on page 131.

13.1.2.4 When To Use WPA/WPA2 Personal (PSK)

Wi-Fi Protected Access 2 (***WPA2***) Personal *Pre-Shared Key* (***PSK***) is an implementation of the Wi-Fi Alliance IEEE ***802.11i*** 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/WPA2 Personal (PSK) 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 13.3 WPA/WPA2 Personal (PSK) Security Mode

Recommendations

WPA/WPA2 Personal (PSK) is not recommended for use with the 9160 Wireless Gateway when WPA/WPA2 Enterprise (RADIUS) is an option.

We recommend that you use WPA/WPA2 Enterprise (RADIUS) 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/WPA2 Personal (PSK).

See Also

For information on how to configure this security mode, see “WPA/WPA2 Personal (PSK)” on page 133.

13.1.2.5 When To Use WPA/WPA2 Enterprise (RADIUS)

Wi-Fi Protected Access 2 (***WPA2***) with *Remote Authentication Dial-In User Service* (***RADIUS***) is an implementation of the Wi-Fi Alliance IEEE ***802.11i*** 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/WPA2 Enterprise (RADIUS) 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/WPA2 Enterprise (RADIUS) 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 Wireless Gateway embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

Table 13.4 WPA/WPA2 Enterprise (RADIUS) Security Mode

Recommendations

WPA/WPA2 Enterprise (RADIUS) 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/WPA2 Personal (PSK) mode.

Use the following guidelines for choosing options within the WPA/WPA2 Enterprise (RADIUS) security mode:

1. The best security you can have to date on a wireless network is WPA/WPA2 Enterprise (RADIUS) 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/WPA2 Enterprise (RADIUS) with the encryption algorithm set to “Both” (that is, 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/WPA2 Enterprise (RADIUS) 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.

Notes: *If there are older client stations on your network that do not support WPA or WPA2, you can configure WPA/WPA2 Enterprise (RADIUS) with Both, CCMP, or TKIP and check the "Allow non-WPA IEEE 802.1x clients" checkbox to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.*

A typical scenario is that one is upgrading a current 802.1x network to use WPA. You might have a mix of clients; some new clients that support WPA or WPA2 and some older ones that do not support any flavours of WPA. You might even have other access points on the network that support only 802.1x and some that support WPA with RADIUS or WPA2 Enterprise (RADIUS). For as long as this mix persists, use the "Allow non-WPA IEEE 802.1x clients" option.

When all the stations have been upgraded to use WPA or better yet WPA2, you should disable the "Allow non-WPA IEEE 802.1x clients" option, and set "WPA Versions" option appropriately ("WPA", "WPA2," or "Both").

See Also

For information on how to configure this security mode, see "WPA/WPA2 Enterprise (RADIUS)" on page 136.

13.1.3 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 plain-text 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 126.)

13.1.4 How Does Station Isolation Protect The Network?

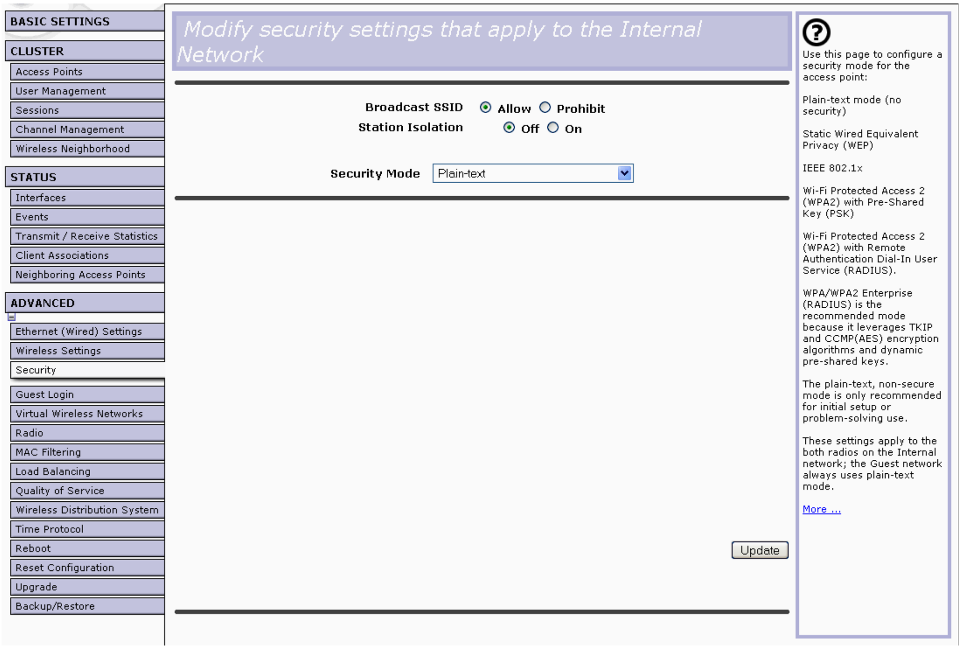
When *Station Isolation* is enabled, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients.

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.

13.2 Configuring Security Settings: Broadcast SSID, Station Isolation, and Security Mode

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



Modify security settings that apply to the Internal Network

Broadcast SSID ● Allow ○ Prohibit

Station Isolation ● Off ○ On

Security Mode: Plain-text

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.

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".)*

To configure security on the access point, select a security mode and fill in the related fields as described in Table 13.5.

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	Select the *Broadcast SSID* setting by clicking the **Allow** or **Prohibit** radio button. 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	Select **Off** to disable Station Isolation or **On** to enable it. • When Station Isolation is **Off**, wireless clients can communicate with one another normally by sending traffic through the access point. • When Station Isolation is **On**, 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: • "Plain-text" on page 126. • "Static WEP" on page 126. • "IEEE 802.1x" on page 131. • "WPA/WPA2 Personal (PSK)" on page 133. • "WPA/WPA2 Enterprise (RADIUS)" on page 136. For a Guest network, only the "Plain-text" setting can be used. (For more information, see Chapter 14: "Setting up Guest Access".) 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.

Table 13.5 Security Settings

13.2.1 Plain-text

Plain-text means any data transferred to and from the 9160 Wireless Gateway is not encrypted. There are no further options for “Plain-text” mode.

Plain-text 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.

13.2.1.1 Guest Network

Plain-text mode 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 122).

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

13.2.2 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.

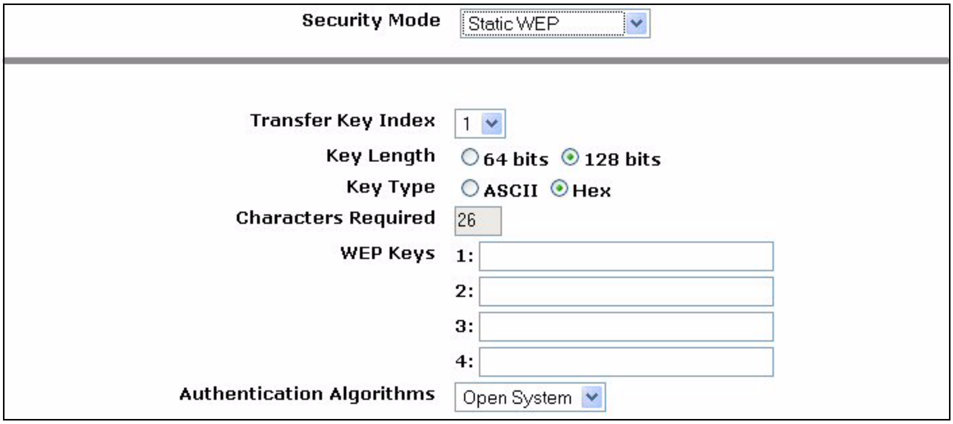
You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Static WEP is not the most secure mode available, but it offers more protection than plain-text mode 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 131, “WPA/WPA2 Personal (PSK)” on page 133.), or “WPA/WPA2 Enterprise (RADIUS)” on page 136.

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 following on the access point settings:



Security Mode: Static WEP

Transfer Key Index: 1

Key Length: ○ 64 bits ● 128 bits

Key Type: ○ ASCII ● Hex

Characters Required: 26

WEP Keys 1:
2:
3:
4:

Authentication Algorithms: Open System

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

Table 13.6 Static WEP Security Settings

Field	Description
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.
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 129.)
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 plain-text, 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.

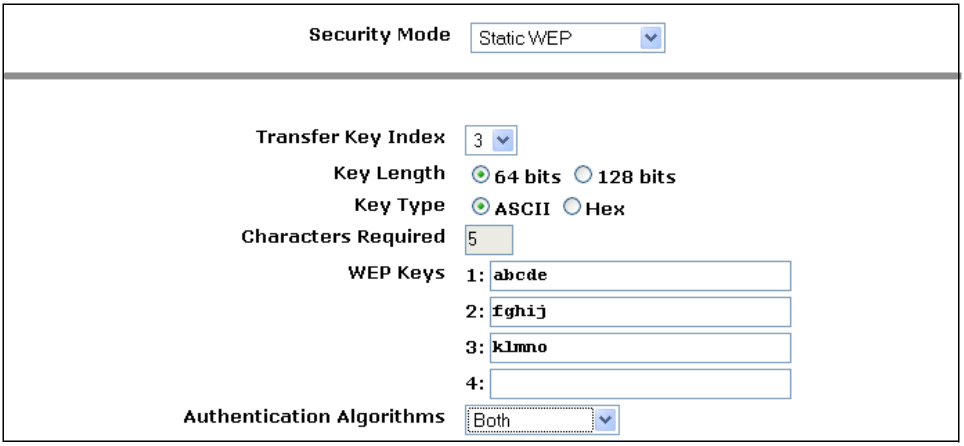
Table 13.6 Static WEP Security Settings

13.2.2.1 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.

13.2.2.2 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.



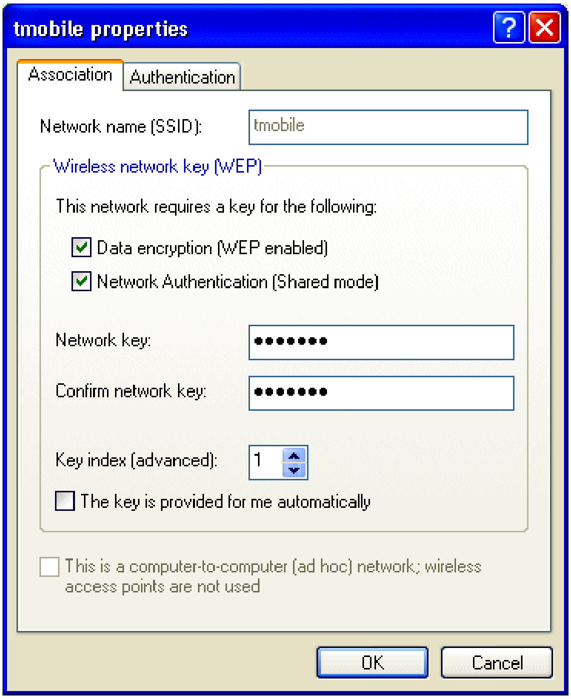
Security Mode: Static WEP

Transfer Key Index: 3
Key Length: ● 64 bits ○ 128 bits
Key Type: ● ASCII ○ Hex
Characters Required: 5
WEP Keys
1: abcde
2: fghij
3: klmno
4:
Authentication Algorithms: Both

Figure 13.7 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.



tmobile properties

Association | Authentication

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

OK | Cancel

Figure 13.8 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.

13.2.2.3 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.

The Figure 13.9 illustrates the dynamics of the AP and two client stations using multiple WEP keys and a transfer key index.

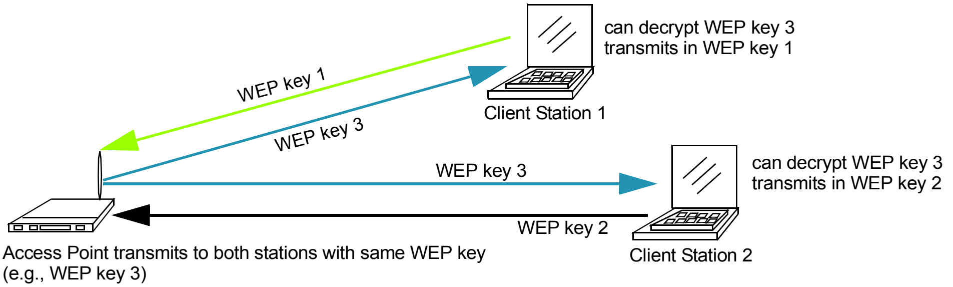


Figure 13.9 Example Of Using Multiple WEP Keys And Transfer Key Index On Client Stations

13.2.3 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.

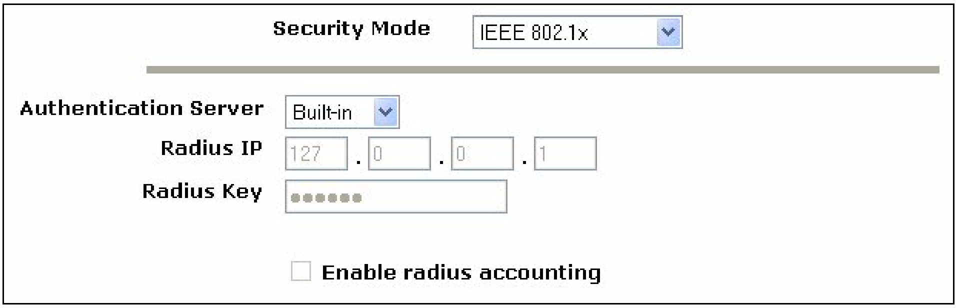
This mode requires the use of a ***RADIUS*** server to authenticate users, and configuration of user accounts via the Cluster, User Management tab.

The access point requires a RADIUS server capable of ***EAP***, such as the Microsoft Internet Authentication Server or the 9160 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 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

Field	Description
Authentication Server	Select one of the following from the drop-down menu: • *Built-in* - To use the authentication server provided with the 9160 Wireless Gateway. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • *External* - To use an external authentication server. If you choose this option 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 Wireless Gateway, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The 9160 Wireless Gateway is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.*

Table 13.10 IEEE 802.1x Security Settings

Field	Description
Radius IP	Enter the Radius IP in the text box. The *Radius IP* is the IP address of the ***RADIUS*** server. (The 9160 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 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 track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.

Table 13.10 IEEE 802.1x Security Settings

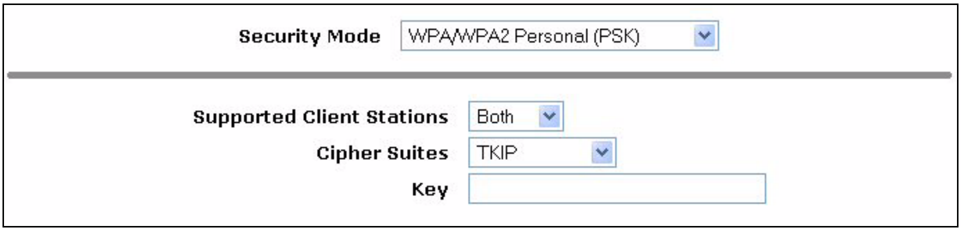
13.2.4 WPA/WPA2 Personal (PSK)

Wi-Fi Protected Access 2 (***WPA2***) with *Pre-Shared Key* (***PSK***) is a Wi-Fi Alliance IEEE ***802.11i*** standard, which includes *Advanced Encryption Algorithm* (***AES***), *Counter mode/CBC-MAC Protocol* (***CCMP***), and *Temporal Key Integrity Protocol* (***TKIP***) mechanisms.

The Personal version of WPA2 employs a pre-shared key (instead of using IEEE ***802.1x*** and ***EAP*** as is used in the Enterprise WPA2 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/WPA2 Personal (PSK)" *Security Mode*, complete the settings as described in Table 13.11.



Security Mode: WPA/WPA2 Personal (PSK)

Supported Client Stations: Both

Cipher Suites: TKIP

Key:

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.

Table 13.11 WPA/WPA2 Personal (PSK) Security Settings

Field	Description
Cipher Suites	Select the cipher you want to use from the drop-down menu: • 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 the authentication algorithm is set to "**Both**", 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***-PSK will not be able to associate with AP.
Key	The *Pre-shared Key* is the shared secret key for ***WPA***-PSK. Enter a string of at least 8 characters to a maximum of 63 characters.

Table 13.11 WPA/WPA2 Personal (PSK) Security Settings

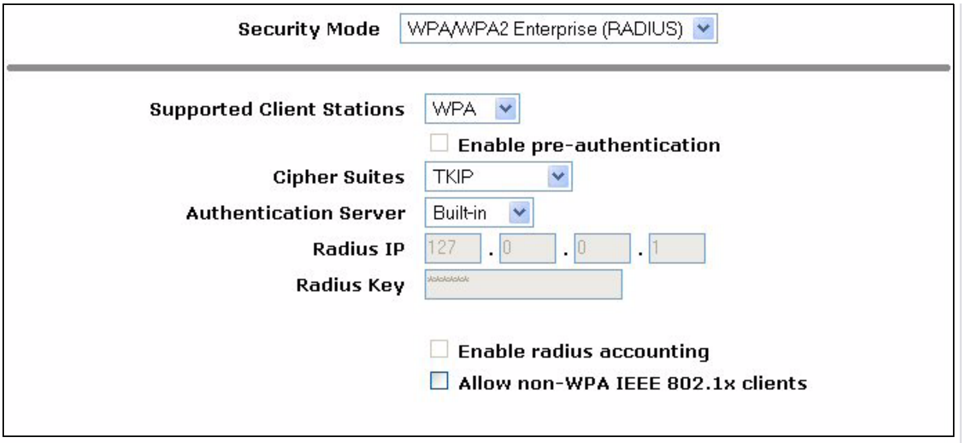
13.2.5 WPA/WPA2 Enterprise (RADIUS)

Wi-Fi Protected Access 2 (***WPA2***) with *Remote Authentication Dial-In User Service* (***RADIUS***) is an implementation of the Wi-Fi Alliance IEEE ***802.11i*** 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 WPA2 Enterprise (RADIUS) mode, you have a choice of whether to use the built-in RADIUS server or an external RADIUS server that you provide. The 9160 Wireless Gateway built-in RADIUS server supports Protected ***EAP*** (PEAP) and MSCHAP V2.

If you selected "WPA/WPA2 Enterprise (RADIUS)" *Security Mode*, complete the settings as described in Table 13.12 on page 137.



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

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.
Enable pre-authentication	If for WPA Versions you select "WPA2" or "Both", you can enable pre-authentication for ***WPA2*** clients. Click **Enable pre-authentication** if you want ***WPA2*** wireless clients to send a 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.

Table 13.12 WPA/WPA2 Enterprise (RADIUS) Security Settings

Field	Description
Cipher Suites	Select the cipher you want to use from the drop-down menu: • ***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 the authentication algorithm is set to "**Both**", 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. **Both** is the default. When the authentication algorithm is set to "Both", 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 13.12 WPA/WPA2 Enterprise (RADIUS) Security Settings

Field	Description
Authentication Server	Select one of the following from the drop-down menu: • *Built-in* - To use the authentication server provided with the 9160 Wireless Gateway. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • *External* - To use an external authentication server. If you choose this option 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 Wireless Gateway, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The 9160 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 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 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”.
Allow non-WPA Clients	Click the **Allow non-*WPA* clients** checkbox if you want to let non-WPA (***802.11***), un-authenticated client stations, use this access point.

Table 13.12 WPA/WPA2 Enterprise (RADIUS) Security Settings

13.3 Updating Settings

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

SETTING UP GUEST ACCESS 14

Out-of-the-box *Guest Interface* features allow you to configure the 9160 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 logins or certificates for access.

You can configure an 9160 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 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 144.

Notes: *This method leverages multiple **BSSID** and Virtual LAN (**VLAN**) technologies that are built-in to the 9160 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 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 145.

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 11: "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 101.)

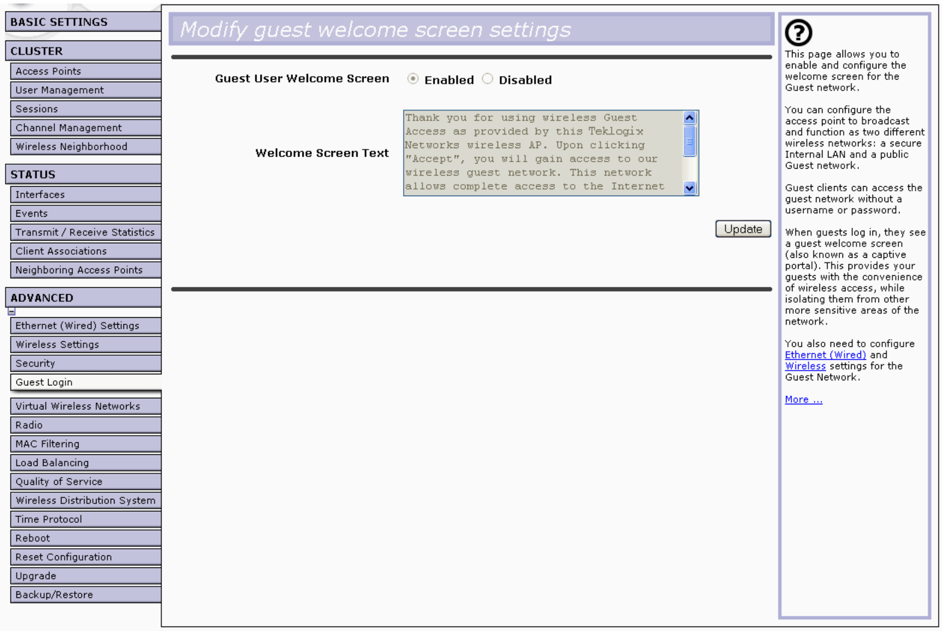
3. Provide the radio interface settings and network names (SSIDs) for both Internal and Guest networks as described in Chapter 12: "Setting the Wireless Interface".

4. Configure the guest splash screen as described in "Configuring The Welcome Screen (Captive Portal)" on page 145.

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 *Advanced, 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 Teklogix
Networks wireless AP. Upon clicking
"Accept", you will gain access to our
wireless guest network. This network
allows complete access to the Internet
```

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 on page 146, the dotted lines indicate dedicated guest connections. All access points and all connections (including guests) are administered from the same 9160 Wireless Gateway Administration Web pages.

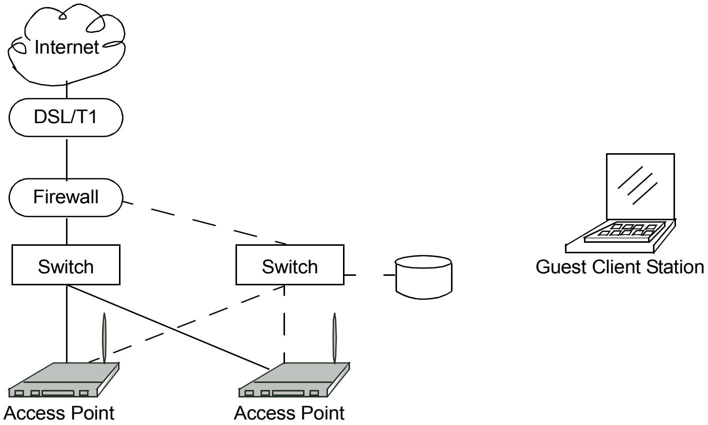


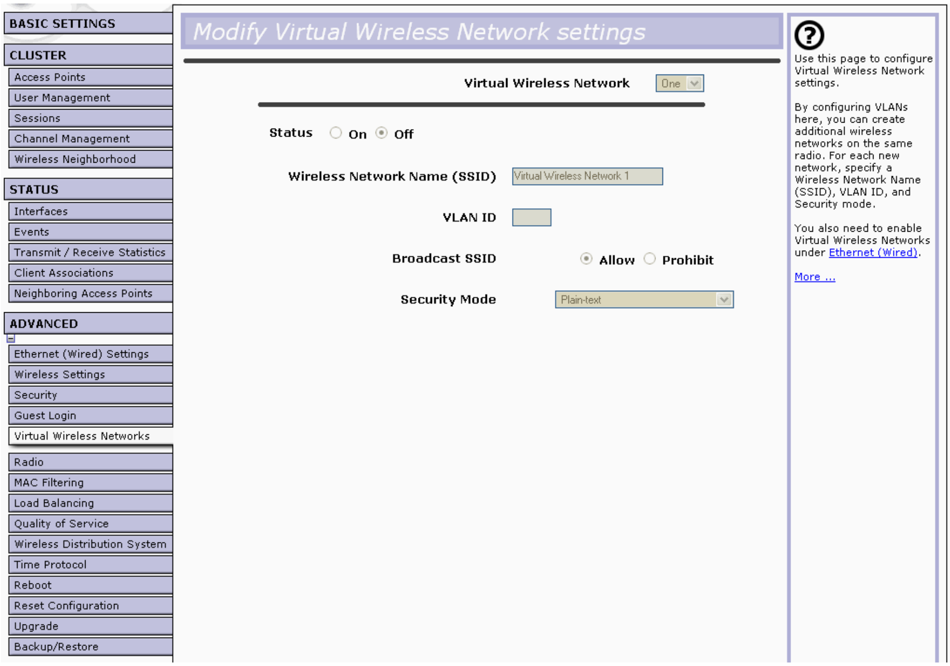
Figure 14.1 Dedicated Guest Connections

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 *Advanced, Virtual Wireless Networks* tab, and update the fields as described below.



Modify Virtual Wireless Network settings

Virtual Wireless Network: One

Status ○ On ● Off

Wireless Network Name (SSID): Virtual Wireless Network 1

VLAN ID:

Broadcast SSID ● Allow ○ Prohibit

Security Mode: Plain-text

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 a Wireless Network Name (SSID), VLAN ID, and Security mode.

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

More ...

15.2 Configuring VLANs

Note: *To configure additional networks on VLANs, you must first enable Virtual Wireless Networks on the Ethernet (wired) interface. See "Enabling / Disabling Virtual Wireless Networks On The AP" on page 102.*

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	Choose one of the following from the drop-down menu to identify an additional network to configure: • **One** • **Two**
Status	You can enable or disable a configured network. • To enable the specified network, click **On**. • To disable the specified network, click **Off**.
Wireless 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.*
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.

Table 15.1 Virtual Wireless Network Settings

Field	Description
Broadcast SSID	Select the *Broadcast SSID* setting by clicking the **Allow** or **Prohibit** radio button. 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 *Advanced, Ethernet [Wired]* tab) uses the Broadcast SSID set on *Advanced, Security*. • If a Guest network is configured, the Broadcast SSID is always allowed.
Security Mode	Select the *Security Mode* for this VLAN. Select one of the following: • ***Plain-text*** • ***Static WEP*** • ***IEEE 802.1x*** • ***WPA/WPA2 Personal (PSK)*** • ***WPA/WPA2 Enterprise (RADIUS)*** ***Note:*** *The Security mode 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 *Advanced, Ethernet [Wired]* tab) uses the Security mode set on *Advanced, Security*. • If a Guest network is configured, it always using **plain-text** security mode.

Table 15.1 Virtual Wireless Network Settings

15.3 Updating Settings

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