

CONFIGURING RADIO SETTINGS

16

16.1 Understanding Radio Settings	155
16.2 Navigating To Radio Settings	156
16.3 Configuring Radio Settings	157
16.4 Updating Settings.	160

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

16.1 Understanding Radio Settings

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

The 9160 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**

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

The IEEE mode, along with other radio settings, are configured as described in “Navigating To Radio Settings” on page 156 and “Configuring Radio Settings” on page 157.

16.2 Navigating To Radio Settings

To specify radio settings, navigate to *Advanced, Radio* tab, and update the fields as described in Table 16.1 on page 157.

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

Modify radio settings

Status ☒ On ☐ Off

Mode

IEEE 802.11g

Super AG ☐ Enabled ☒ Disabled

Channel

1

Beacon Interval

100

 (Msec, Range: 20 - 2000)

DTIM Period

2

 (Range: 1-255)

Fragmentation Threshold

2346

 (Range: 256-2346, even numbers only)

RTS Threshold

2347

 (Range: 0-2347)

Maximum Stations

2007

 (Range: 0-2007)

Transmit Power

100

 (Percent)

Rate Supported Basic

54 Mbps

☒

☐

48 Mbps

☒

☐

36 Mbps

☒

☐

24 Mbps

☒

☐

18 Mbps

☒

☐

12 Mbps

☒

☐

11 Mbps

☒

☒

9 Mbps

☒

☐

6 Mbps

☒

☐

5.5 Mbps

☒

☒

2 Mbps

☒

☒

1 Mbps

☒

☒

Rate Sets

11 Mbps

☒

☒

9 Mbps

☒

☐

6 Mbps

☒

☐

5.5 Mbps

☒

☒

2 Mbps

☒

☒

1 Mbps

☒

☒

Update

?

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

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

[More ...](#)

16.3 Configuring Radio Settings

Field	Description
<i>Radio</i>	The 9160 Wireless Gateway is available as a one-radio or two-radio access point. One-Radio AP: If you have a one-radio version of the 9160 Wireless Gateway, this field is not included on the Radio tab. Two-Radio AP: If you have a two-radio version of the 9160 Wireless Gateway, specify Radio One or Radio Two. On a two-radio AP, the rest of the settings on this tab apply to the radio selected in this field. Be sure to configure settings for both radios.
<i>Status (On/Off)</i>	Specify whether you want the radio on or off by clicking On or Off .
<i>Mode</i>	The <i>Mode</i> defines the <i>Physical Layer (PHY)</i> standard being used by the radio. The 9160 Wireless Gateway is available as a single or dual-band access point. Single-Band AP: For the Single-Band access point, select one of these modes: • IEEE 802.11b • IEEE 802.11g Dual-Band AP: For the Dual-Band access point, select one of these modes. • IEEE 802.11b • IEEE 802.11g • IEEE 802.11a Note: If you have a two-radio AP, different modes may available depending on whether <i>Radio One</i> or <i>Radio Two</i> is selected in the <i>Radio</i> field above.
<i>Super AG</i>	Enabling Super AG provides better performance by increasing radio throughput for a radio mode (IEEE 802.11b, g, a, and so on). Keep in mind that, with Super AG enabled, the access point transmissions will consume more bandwidth. • To enable Super AG click Enabled. • To disable Super AG click Disabled.
<i>Channel</i>	The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. For most Modes, the default is Auto. Auto is the recommended mode because it automatically detects the best channel choices based on signal strength, traffic loads, and so on.

Table 16.1 Radio Settings

Field	Description
<i>Beacon Interval</i>	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 <i>Beacon Interval</i> value is set in milliseconds. Enter a value from 20 to 2000.
<i>DTIM Period</i>	The <i>Delivery Traffic Information Map (DTIM)</i> message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up. The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup. Specify a DTIM period within the given range (1 - 255). The measurement is in beacons. For example, if you set this to 1, clients will check for buffered data on the AP at every beacon. If you set this to 2, clients will check on every other beacon. If you set this to 10, clients will check on every 10th beacon.
<i>Fragmentation Threshold</i>	Specify a number between 256 and 2,346 to set the frame size threshold in bytes. The <i>fragmentation threshold</i> is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation. Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help <i>improve</i> network performance and reliability if properly configured. Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems; for example, with microwave ovens. By default, fragmentation is off. We recommend not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.

Table 16.1 Radio Settings

Field	Description
<i>RTS Threshold</i>	Specify an RTS Threshold value between 0 and 2347. The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
<i>Maximum Stations</i>	Specify the maximum number of stations allowed to access this AP at any one time. You can enter a value between 0 and 2007.
<i>Transmit Power</i>	Provide a percentage value to set the transmit power for this access point. The default is to have the access point transmit using 100 percent of its power.  Recommendations: - For most cases, we recommend keeping the default and having the transmit power set to 100 percent. This is more cost-efficient as it gives the access point a maximum broadcast range, and reduces the number of APs needed. - To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This will help reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
<i>Rate Sets</i>	Check the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise. Rates are expressed in megabits per second. <i>Supported Rate Sets</i> indicate rates that the access point supports. You can check multiple rates (click a checkbox to select or de-select a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP. <i>Basic Rate Sets</i> indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.

Table 16.1 Radio Settings

16.4 Updating Settings

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



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

MAC ADDRESS FILTERING

17

17.1 Navigating To MAC Filtering Settings.	163
17.2 Using MAC Filtering.	164
17.3 Updating Settings.	164

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

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

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

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

17.1 Navigating To MAC Filtering Settings

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

The screenshot shows the 'Configure MAC Filtering of client stations' page. On the left is a navigation menu with sections: BASIC SETTINGS, CLUSTER, STATUS, and ADVANCED. The 'ADVANCED' section is expanded, showing options like Ethernet (Wired) Settings, Wireless Settings, Security, Guest Login, Radio, MAC Filtering (selected), Load Balancing, Quality of Service, Wireless Distribution System, Time Protocol, Reset Configuration, Upgrade, and Backup/Restore. The main content area is titled 'Configure MAC Filtering of client stations'. It features a 'Filter' section with two radio buttons: 'Allow only stations in list' and 'Allow any station unless in list' (which is selected). Below this is a 'Stations List' containing a text box with the MAC address 'FE:DA:BD:09:87:65' and a 'Remove' button. At the bottom of the list is an 'Add' button with a format guide: [] : [] : [] : [] : [] : []. An 'Update' button is located at the bottom right of the main area. On the far right, a help box with a question mark icon explains that MAC Filtering is used to exclude or allow only listed client stations to authenticate with the access point. It notes that these settings apply to both Internal and Guest networks. It defines a MAC address as a string of twelve (12) hexadecimal digits separated by colons, giving the example FE:DC:BA:09:87:65. A 'More ...' link is also present.

17.2 Using MAC Filtering

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

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

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

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

Table 17.1 MAC Filtering Settings

17.3 Updating Settings

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

18.1 Understanding Load Balancing	167
18.1.1 Identifying Imbalance: Overworked Or Under-utilized Access Points	167
18.1.2 Specifying Limits For Utilization And Client Associations	167
18.1.3 Load Balancing And QoS	168
18.2 Navigating To Load Balancing Settings	168
18.3 Configuring Load Balancing	169
18.4 Updating Settings	170

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

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

18.1 Understanding Load Balancing

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



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

18.1.1 Identifying Imbalance: Overworked Or Under-utilized Access Points

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

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

18.1.2 Specifying Limits For Utilization And Client Associations

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

18.1.3 Load Balancing And QoS

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

18.2 Navigating To Load Balancing Settings

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

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

Modify load balancing settings

Load Balancing

Enabled

Disabled

Utilization for No New Associations

0

(Percent, 0 disables)

Utilization for Disassociation

0

(Percent, 0 disables)

Station Threshold for Disassociation

0

(Range: 1-2007, 0 disables)

Update

?

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

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

With load balancing, you can ensure that all access points on the network handle a proportionate share of wireless traffic, and that no single access point gets overloaded.

[More ...](#)

18.3 Configuring Load Balancing

To configure load balancing, *enable* **Load Balancing** and set limits and behaviour to be triggered by a specified utilization rate of the access point.



Notes: To view the current Utilization Rates for access points, click **Cluster, Sessions** on the Administration Web pages. (See Chapter 8: “Session Monitoring”.)

Even when clients are disassociated from an AP, the network will still provide continuous service to client stations if another access point is within range so that clients can re-connect to the network. Clients should automatically retry the AP they were originally connected to and other APs on the subnet. Clients who are disassociated from one AP should experience a seamless transition to another AP on the same subnet.

Load Balancing settings apply to the AP load as a whole. When Guest access is enabled, the settings apply to both Internal and Guest networks together.

On a two-radio access point, Load Balancing settings apply to both radios but the load of each radio is calculated independently and includes both the Internal and Guest network (when Guest access is enabled).

Field	Description
<i>Load Balancing</i>	To enable load balancing on this access point, click Enable. To disable load balancing on this access point, click Disable.
<i>Utilization for No New Associations</i>	Utilization rate limits relate to wireless bandwidth utilization. Provide a bandwidth utilization rate percentage limit for this access point to indicate when to stop accepting new client associations. When the utilization rate for this access point exceeds the specified limit, no new client associations will be allowed on this access point. If you specify 0 in this field, all new associations will be allowed regardless of the utilization rate.

Table 18.1 Load Balancing Settings

Field	Description
<i>Utilization for Disassociation</i>	Utilization rate limits relate to wireless bandwidth utilization. Provide a bandwidth utilization rate percentage limit for this access point to indicate when to disassociate current clients. When the utilization rate exceeds the specified limit, a client currently associated with this access point will be disconnected. If you specify 0 in this field, current clients will never be disconnected regardless of the utilization rate.
<i>Stations Threshold for Disassociation</i>	Specify the number of client stations you want as a "stations threshold" for disassociation. If the number of client stations associated with the AP at any one time is equal to or less than the number you specify here, no stations will be disassociated regardless of the <i>Utilization for Disassociation</i> value. Theoretically, the maximum number of client stations allowed is 2007.  We recommend setting the maximum to between 30 and 50 client stations. This allows for a workable load on the access point, given that bandwidth is shared among the AP clients.

Table 18.1 Load Balancing Settings

18.4 Updating Settings

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

QUALITY OF SERVICE (QoS)

19

19.1 Understanding QoS.	173
19.1.1 QoS And Load Balancing	173
19.1.2 802.11e And WMM Standards Support	173
19.1.3 QoS Queues And Parameters To Coordinate Traffic Flow	174
19.2 Configuring QoS Queues.	178
19.2.1 Configuring AP EDCA Parameters	180
19.2.2 Enabling/Disabling Wi-Fi Multimedia.	182
19.2.3 Configuring Station EDCA Parameters	183
19.3 Updating Settings.	184

Quality of Service (**QoS**) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), other types of audio, video, and streaming media, as well as traditional IP data over the 9160 Wireless Gateway.

The following sections describe how to configure Quality of Service queues on the 9160 Wireless Gateway.

19.1 Understanding QoS

A primary factor that affects QoS is network congestion due to an increased number of clients attempting to access the air waves and higher traffic volume competing for bandwidth during a busy time of day. The most noticeable degradation in service on a busy, overloaded network will be evident in time-sensitive applications like Video, *Voice-over-IP* (VoIP), and streaming media.

Unlike typical data files which are less affected by variability in QoS, Video, VoIP and streaming media must be sent in a specific order at a consistent rate and with minimum delay between **Packet** transmission. If the quality of service is compromised, the audio or video will be distorted.

19.1.1 QoS And Load Balancing

By using a combination of load balancing (see Chapter 18: “Load Balancing”) and QoS techniques, you can provide a high quality of service for time-sensitive applications even on a busy network. Load balancing is a way of better distributing the traffic volume across access points. QoS is a means of allocating bandwidth and network access based on transmission priorities for different types of wireless traffic within a single access point.

19.1.2 802.11e And WMM Standards Support

QoS describes a range of technologies for controlling data streams on shared network connections. The **IEEE 802.11e** task group is in the process of defining a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion; limiting **Jitter**, **Latency**, and **Packet Loss**; supporting dedicated bandwidth for time-sensitive or mission critical applications, and prioritizing wireless traffic for channel access.

QoS Queues And Parameters To Coordinate Traffic Flow

As with all IEEE **802.11** working group standards, the goal is to provide a standard way of implementing QoS features so that components from different companies are interoperable.

The 9160 Wireless Gateway provides QoS based on the *Wireless Multimedia (WMM)* specification and *Wireless Multimedia* (WMM) standards, which are implementations of a subset of **802.11e** features.

Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled.

19.1.3 QoS Queues And Parameters To Coordinate Traffic Flow

Configuring QoS options on the 9160 Wireless Gateway consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

For example, time-sensitive Voice, Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

The 9160 Wireless Gateway implements QoS based on the IEEE Wireless Multimedia (WMM) standard. A Linux-based queuing class is used to tag packets and establish multiple queues. The queues provided offer built-in prioritization and routing based on the type of data being transmitted.

The Administration UI provides a way for you to configure parameters on the queues.

19.1.3.1 QoS Queues And Type Of Service (ToS) On Packets

QoS on the 9160 Wireless Gateway leverages **WMM** information in the **IP** packet header related to Type of Service (**ToS**). Every IP packet sent over the network includes a ToS field in the header that indicates how the data should be prioritized and transmitted over the network. The ToS field consists of a 3 to 7 bit value with each bit representing a different aspect or degree of priority for this data as well as other meta-information (low delay, high throughput, high reliability, low cost, and so on).

For example, the ToS for FTP data packets is likely to be set for maximum throughput since the critical consideration for FTP is the ability to transmit relatively large amounts of data in one go. Interactive feedback is a nice-to-have in this situation but certainly less critical. VoIP data packets are set for minimum delay because that is a critical factor in quality and performance for that type of data.

The access point examines the ToS field in the headers of all packets that pass through the AP. Based on the value in a packet's ToS field, the AP prioritizes the packet for transmission by assigning it to one of the queues. This process occurs automatically, regardless of whether you deliberately configure QoS or not.

A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

- Data 0 (Voice). Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.
- Data 1 (Video). High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.
- Data 2 (Best Effort). Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Data 3 (Background). Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Packets in a higher priority queue will be transmitted before packets in a lower priority queue. Interactive data in the queues labelled "Data 0" and "Data 1" is always sent first, best effort data in "Data 2" is sent next, and Background (bulk) data in "Data 3" is sent last. Each lower priority queue (class of traffic) gets bandwidth that is left over after the higher classes of traffic have been sent. At an extreme end if you have enough interactive data to keep the access point busy all the time, low priority traffic would never get sent.

Using the QoS settings on the Administration UI, you can configure *Enhanced Distributed Channel Access* (EDCA) parameters that determine how each queue is treated when it is sent by the access point to the client or by the client to the access point.



Note: *Wireless traffic travels:*

- *Downstream from the access point to the client station.*
- *Upstream from client station to access point.*
- *Upstream from access point to network.*
- *Downstream from network to access point.*

With WMM enabled, QoS settings on the 9160 Wireless Gateway affect the first two of these; downstream traffic flowing from the access point to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the access point (station EDCA parameters).

With WMM disabled, you can still set some parameters on the downstream traffic flowing from the AP to the client station (AP EDCA parameters).

The other phases of the traffic flow (to and from the network) are not under control of the QoS settings on the AP.

19.1.3.2 EDCF Control Of Data Frames And Arbitration Interframe Spaces

Data is transmitted over 802.11 wireless networks in *frames*. A **Frame** consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network.



Note: *A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).*

Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection.

The 802.11 standard defines various *frame* types for management and control of the wireless infrastructure, and for data transmission. 802.11 frame types are: (1) *management frames*, (2) *control frames*, and (3) *data frames*. Management and control frames (which manage and control the availability of the wireless infrastructure) automatically have higher priority for transmission.

802.11e uses *interframe spaces* to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data.

Management and control frames wait a minimum amount of time for transmission; they wait a *short interframe space* (SIF). These wait times are built-in to 802.11 as infrastructure support and are not configurable.

The 9160 Wireless Gateway supports the *Enhanced Distribution Coordination Function (EDCF)* as defined by the **802.11e** standard. EDCF, which is an enhancement to the **DCF** standard and is based on **CSMA/CA** protocol, defines the interframe space (IFS) between *data frames*. Data frames wait for an amount of time defined as the *arbitration interframe space* (AIFs) before transmitting.

This parameter is configurable.

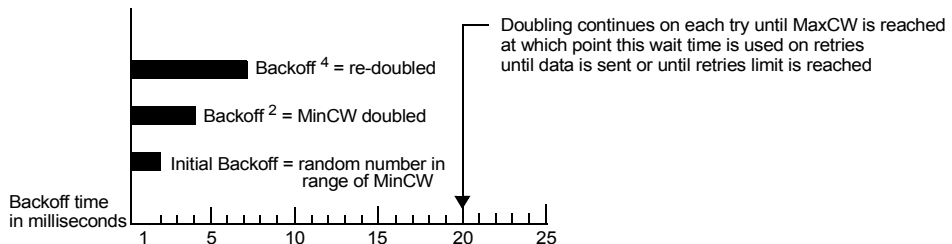


Note: *Sending data frames in AIFs allows higher priority management and control frames to be sent in SIFs first.*

The AIFs ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free.

19.1.3.3 Random Backoff And Minimum/Maximum Contention Windows

If an access point detects that the medium is in use (busy), it uses the DCF *random backoff* timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum Contention Window*) increases exponentially up to a specified limit (*Maximum Contention Window*). The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.



Configuring QoS Queues

The random backoff used by the access point is a configurable parameter. To describe the random delay, a “Minimum Contention Window” (MinCW) and a “Maximum Contention Window” (MaxCW) is defined.

- The value specified for the *Minimum Contention Window* is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the *Maximum Contention Window* is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

19.1.3.4 Packet Bursting For Better Performance

The 9160 Wireless Gateway includes 802.11e based *packet bursting* technology that increases data throughput and speed of transmission over the wireless network. Packet bursting enables the transmission of multiple packets without the extra overhead of header information. The effect of this is to increase network speed and data throughput. The size of packet bursts allowed (maximum burst length) is a configurable parameter.

19.1.3.5 Transmission Opportunity (TXOP) Interval For Client Stations

The *Transmission Opportunity* (TXOP) is an interval of time when a Wi-Fi Multimedia (WMM) client station has the right to initiate transmissions onto the wireless medium (WM).

19.2 Configuring QoS Queues

To set up queues for QoS, navigate to the *Advanced, Quality of Service* tab, and configure settings as described below.

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

Modify QoS queue parameters

AP EDCA parameters

Queue	ATFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	15
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Wi-Fi Multimedia (WMM)
☒ Enabled
☐ Disabled

Station EDCA parameters

Queue	ATFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

Update

?

Quality of Service (QoS) allows you to specify different queue parameters for different types of wireless traffic.

These settings apply to the AP load as a whole, and Internal and Guest network traffic is queued together.

QoS specifically relates to providing minimum delay service for Voice over IP (VoIP) and other time-sensitive types of data.

You do not need to modify these parameters to activate QoS. Queuing for Quality of Service (with the default parameters) automatically occurs whenever an AP is in service.

[More ...](#)

Configuring Quality of Service (**QoS**) on the 9160 Wireless Gateway consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (via *Contention Windows*) for transmission. The settings described here apply to data transmission behaviour on the access point only, not to that of the client stations.



Notes: For the Guest interface, QoS queue settings apply to the access point load as a whole (both BSSes together).

On a two-radio access point these settings apply to both radios but the traffic for each radio is queued independently. (The exception to this is guest traffic as noted below.)

Internal and Guest network traffic is always queued together within each radio. This is the case on both one-radio and two-radio APs.

Configuring Quality of Service includes:

- “Configuring AP EDCA Parameters” on page 180.
- “Enabling/Disabling Wi-Fi Multimedia” on page 182.
- “Updating Settings” on page 184.

19.2.1 Configuring AP EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station.

Field	Description
<i>Queue</i>	Queues are defined for different types of data transmitted from AP-to-station: Data 0 (Voice) High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. Data 1 (Video) High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. Data 2 (best effort) Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. Data 3 (Background) Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For more information, see "QoS Queues And Parameters To Coordinate Traffic Flow" on page 174.
<i>AIFs (Inter-Frame Space)</i>	The <i>Arbitration Inter-Frame Spacing</i> (AIFs) specifies a wait time (in milliseconds) for data frames. Valid values for AIFs are 1 through 255. For more information, see "EDCF Control Of Data Frames And Arbitration Interframe Spaces" on page 176.

Table 19.1 AP EDCA Parameters

Field	Description
<i>cwMin</i> (<i>Minimum Contention Window</i>)	This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the <i>Minimum Contention Window</i> is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for the "cwmin" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmin" must be lower than the value for "cwmax". For more information, see "Random Backoff And Minimum/Maximum Contention Windows" on page 177.
<i>cwMax</i> (<i>Maximum Contention Window</i>)	The value specified here in the <i>Maximum Contention Window</i> is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin". For more information, see "Random Backoff And Minimum/Maximum Contention Windows" on page 177.
<i>Max. Burst Length</i>	AP EDCA Parameter Only (The Max. Burst Length applies only to traffic flowing from the access point to the client station.) This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A <i>packet burst</i> is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999.9. For more information, see "Packet Bursting For Better Performance" on page 178.

Table 19.1 AP EDCA Parameters

19.2.2 Enabling/Disabling Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the 9160 Wireless Gateway control *downstream* traffic flowing from the access point to client station (AP EDCA parameters) and the *upstream* traffic flowing from the station to the access point (station EDCA parameters).

Disabling WMM will deactivate QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the access point

With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters).

- To disable WMM extensions, click **Disabled**.
- To enable WMM extensions, click **Enabled**.

19.2.3 Configuring Station EDCA Parameters

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

Field	Description
<i>Queue</i>	Queues are defined for different types of data transmitted from station-to-AP: Data 0 (Voice) Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. Data 1 (Video) Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. Data 2 (best effort) Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. Data 3 (Background) Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). For more information, see “QoS Queues And Parameters To Coordinate Traffic Flow” on page 174.
<i>AIFs (Inter-Frame Space)</i>	The <i>Arbitration Inter-Frame Spacing</i> (AIFs) specifies a wait time (in milliseconds) for <i>data frames</i>. For more information, see “EDCF Control Of Data Frames And Arbitration Interframe Spaces” on page 176.

Table 19.2 Station EDCA Parameters

Field	Description
<i>cwMin</i> (<i>Minimum Contention Window</i>)	This parameter is input to the algorithm that determines the initial random backoff wait time (“window”) for retry of a transmission. The value specified here in the <i>Minimum Contention Window</i> is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. For more information, see “Random Backoff And Minimum/Maximum Contention Windows” on page 177.
<i>cwMax</i> (<i>Maximum Contention Window</i>)	The value specified here in the <i>Maximum Contention Window</i> is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. For more information, see “Random Backoff And Minimum/Maximum Contention Windows” on page 177.
<i>TXOP Limit</i>	Station EDCA Parameter Only (The TXOP Limit applies only to traffic flowing from the client station to the access point.) The <i>Transmission Opportunity</i> (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the <i>Transmission Opportunity</i> (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

Table 19.2 Station EDCA Parameters

19.3 Updating Settings

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

WIRELESS DISTRIBUTION SYSTEM 20

20.1 Understanding The Wireless Distribution System	187
20.1.1 Using WDS To Bridge Distant Wired LANs	187
20.1.2 Using WDS To Extend Network Beyond The Wired Coverage Area	188
20.1.3 Backup Links and Unwanted Loops In WDS Bridges	189
20.1.4 Security Considerations Related To WDS Bridges	190
20.2 Configuring WDS Settings	190
20.2.1 Example Of Configuring A WDS Link.	194
20.3 Updating Settings	195

The 9160 Wireless Gateway lets you connect multiple access points using a Wireless Distribution System (**WDS**). WDS allows access points to communicate with one another wirelessly in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

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

20.1 Understanding The Wireless Distribution System

A *Wireless Distribution System (WDS)* is an **802.11f** technology that wirelessly connects access points, known as Basic Service Sets (**BSS**), to form what is known as an *Extended Service Set (ESS)*.



Note: *A BSS generally equates to an access point (deployed as a single-AP wireless “network”), except in cases where multi-BSSID features make a single access point look like two or more access points to the network. In such cases, the access point has multiple unique BSSIDs.*

20.1.1 Using WDS To Bridge Distant Wired LANs

In an **ESS**, a network of multiple access points, each access point serves part of an area which is too large for a single access point to cover. You can use WDS to bridge distant Ethernets to create a single **LAN**. For example, suppose you have one access point which is connected to the network by Ethernet and serving multiple client stations in the Conference Room (LAN Segment 1), and another Ethernet-wired access point serving stations in the West Wing offices (LAN Segment 2). You can bridge the Conference Room and West Wing access points with a WDS link to create a single network for clients in both areas (see Figure 20.1 on page 188).

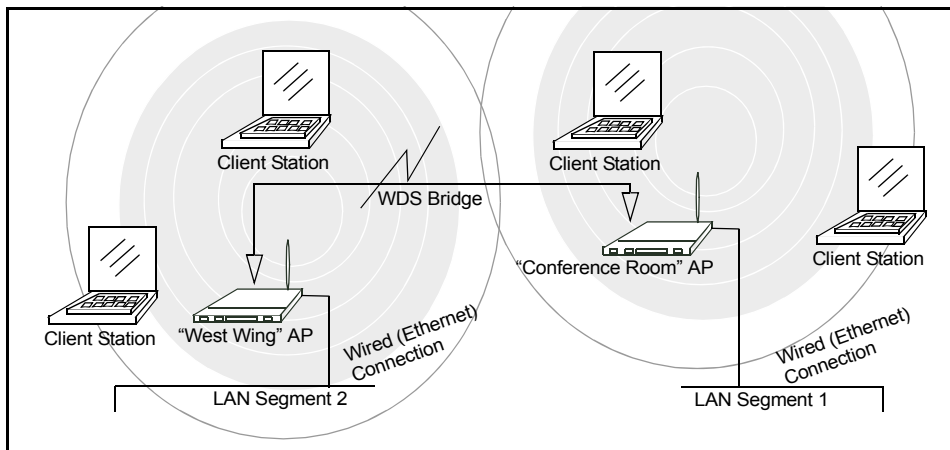


Figure 20.1 Bridged Distant Wired LANs

20.1.2 Using WDS To Extend Network Beyond The Wired Coverage Area

An **ESS** can extend the reach of the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have an access point which is connected to the network by Ethernet and serving multiple client stations in one area (“East Wing” in our example), but cannot reach others which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with Ethernet cabling. You can solve this problem by placing a second access point closer to second group of stations (“Poolside” in our example) and bridge the two APs with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations (see Figure 20.2 on page 189).

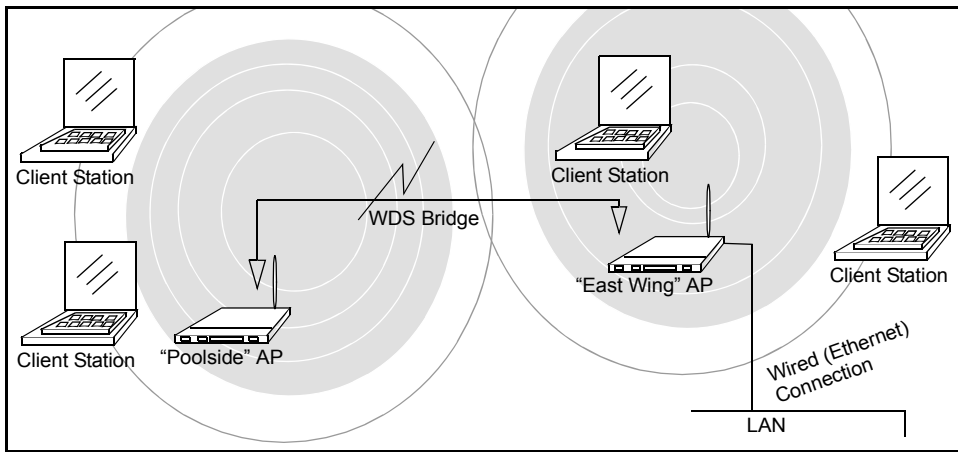


Figure 20.2 Extended Network Beyond The Wired Coverage Area

20.1.3 Backup Links and Unwanted Loops In WDS Bridges

Another use for WDS bridging, the creation of backup links, is not supported in this release of the 9160 Wireless Gateway. The topic is included here to emphasize that you should not try to use WDS in this way; backup links will result in unwanted, endless loops of data traffic

If an access point provides *Spanning Tree Protocol (STP)*, WDS can be used to configure backup paths between access points across the network. For example, between two access points you could have both a primary path via Ethernet and a secondary (backup) wireless path via a WDS link. If the Ethernet connection goes down, STP would reconfigure its map of the network and effectively fix the down network segment by activating the backup wireless path.

The 9160 Wireless Gateway does not provide STP for this release. Without STP, it is possible that both connections (paths) may be active at the same time, and result in an endless loop of traffic on the LAN.

Therefore, be sure not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

For more information, see the “Do not create loops” note under “Configuring WDS Settings” on page 190.

20.1.4 Security Considerations Related To WDS Bridges

Static *Wired Equivalent Privacy* (**WEP**) is a data encryption protocol for 802.11 wireless networks. Both access points in a given WDS link must be configured with the same security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

You can enable Static **WEP** on the WDS link (bridge). When WEP is enabled, all data exchanged between the two access points in a WDS link is encrypted using a fixed WEP key that you provide.

Static WEP is the only security mode available for the WDS link, and it does not provide effective data protection to the level of other security modes available for service to client stations. If you use WDS on a **LAN** intended for secure wireless traffic you are putting your network at risk. Therefore, we recommend using WDS to bridge the Guest network only for this release. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.

For more information about the effectiveness of different security modes, see Chapter 13: “Configuring Security”. This topic also covers use of plain-text security mode for AP-to-station traffic on the Guest network, which is intended for less sensitive data traffic.

20.2 Configuring WDS Settings

To specify the details of traffic exchange from this access point to others, navigate to the *Advanced, Wireless Distribution System* tab, and update the fields as described below.



Note: *Figure 20.3 on page 191 shows the WDS settings page for the two-radio AP. The Administration Web page for the one-radio AP will look slightly different.*

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

Configure WDS bridges to other access points

Local Address 00:0C:41:0A:33:7E

Remote Address

Bridge with Internal Network

WEP Enabled Disabled

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required

WEP Key

Remote Address

Bridge with Internal Network

WEP Enabled Disabled

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required

WEP Key

Remote Address

Bridge with Internal Network

WEP Enabled Disabled

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required

WEP Key

Remote Address

Bridge with Internal Network

WEP Enabled Disabled

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required

WEP Key

Update

?

The Wireless Distribution System (WDS) allows you to bridge wireless traffic between access points.

By wirelessly connecting APs to one another in an Extended Service Set, you can bridge distant Ethernet into a single LAN with each AP serving part of an area too large for a single AP to cover. WDS can extend the reach of your network into areas where cabling might be too difficult.

Caution:
Do not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

Loops created by WDS bridges with the intention of establishing backup links or extended service sets (ESS) with two WDS bridges on one AP will not work; they will result in endless loop data traffic on the network because Spanning Tree Protocol (STP) is not on the AP to prevent it.

[More ...](#)

Figure 20.3 Wireless Distribution System Settings

The following notes summarize some critical guidelines regarding **WDS** configuration. Please read all the notes before proceeding with WDS configuration.



Notes:

- The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, we recommend using WDS to bridge the Guest network only for this release. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.*

Configuring WDS Settings

- *When using WDS, be sure to configure WDS settings on both access points participating in the WDS link.*
- *You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.*
- *Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See Chapter 16: “Configuring Radio Settings” for information on configuring the Radio mode and channel.)*
- ***Do not create loops*** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. Spanning Tree Protocol (STP), which manages path redundancy and prevent unwanted loops, is not enabled for this release. Keep these rules in mind when working with WDS on this release of the 9160 Wireless Gateway:

Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.

Do not create “backup” links.

If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.

You can only extend or bridge either the Internal or Guest network but not both.

To configure WDS on this access point, describe each AP intended to receive hand-offs and send information to this AP. Each destination AP needs the following description, as shown in Table 20.4 on page 193.

Field	Description
<i>Radio</i>	The 9160 Wireless Gateway is available as a one-radio or two-radio access point. One-Radio AP: On the one-radio version of the 9160 Wireless Gateway, this field is not included on the <i>WDS</i> tab. Two-Radio AP: For each WDS link on a two-radio AP, select Radio One or Radio Two. The rest of the settings for the link apply to the radio selected in this field. The read-only “Local Address” will change depending on which Radio you select here.
<i>Local Address</i>	Indicates the Media Access Control (MAC) addresses for this access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point or interface. One-Radio AP: On a one-radio access point, a single MAC address is shown at the top of the <i>WDS</i> settings page. The address shown for the one-radio AP is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks. Two-Radio AP: For each WDS link on a two-radio AP, the <i>Local Address</i> reflects the MAC address for the Internal interface on the selected radio (Radio One on WLAN0 or Radio Two WLAN1).
<i>Remote Address</i>	Specify the MAC address of the destination access point; that is, the access point to which data will be sent or “handed-off” and from which data will be received.
<i>Bridge with</i>	The 9160 Wireless Gateway provides the capability of setting up guest and internal networks on the same access point. (See Chapter 14: “Setting up Guest Access”.) The guest network typically provides internet access but isolates guest clients from more sensitive areas of your internal network. It is common to have security disabled on the guest network to provide open access. Alternatively, the <i>internal</i> network provides full access to protected information behind a firewall and requires secure logins or certificates for access. When using WDS to link up one access point to another, you need to identify within which of these networks you want the data exchange to occur. Specify the network to which you want to bridge this access point: • Internal Network • Guest Network

Table 20.4 Destination Access Point Settings

Field	Description
WEP	Specify whether you want <i>Wired Equivalent Privacy (WEP)</i> encryption enabled for the WDS link. - Enabled - Disabled <i>Wired Equivalent Privacy (WEP)</i> is a data encryption protocol for 802.11 wireless networks. Both access points on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.
Key Length	If WEP is enabled, specify the length of the WEP key: 64 bits 128 bits
Key Type	If WEP is enabled, specify the WEP key type: - ASCII - Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
WEP Key	Enter a string of characters. If you selected ASCII, enter any combination of 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). These are the RC4 encryption keys shared with the stations using the access point.

Table 20.4 Destination Access Point Settings

20.2.1 Example Of Configuring A WDS Link

When using WDS, be sure to configure *WDS* settings on both access points on the WDS link. For example, to create a WDS link between a pair of access points “**MyAP1**” and “**MyAP2**” do the following:

1. Open the Administration Web pages for MyAP1, by entering the IP address for MyAP1 as a URL in the Web browser address bar in the following form:

http://IPAddressOfAccessPoint

where *IPAddressOfAccessPoint* is the address of MyAP1.

2. Navigate to the WDS tab on MyAP1 Administration Web pages.
The MAC address for MyAP1 (the access point you are currently viewing) will show as the “Local Address” at the top of the page.
3. Configure a WDS interface for data exchange with MyAP2.
Start by entering the MAC address for MyAP2 as the “Remote Address” and fill in the rest of the fields to specify the network (guest or internal), security, and so on. Save the settings (click **Update**).
4. Navigate to the radio settings on the Administration Web pages (*Advanced, Radio*) to verify or set the mode and the radio channel on which you want MyAP1 to broadcast.
Remember that the two access points participating in the link, MyAP1 and MyAP2, must be set to the same Mode and be transmitting on the same channel.
For our example, let’s say we’re using IEEE 802.11b Mode and broadcasting on Channel 6. (We’d choose Mode and Channel from the drop-down menus on the Radio tab.)
5. Now repeat the same steps for MyAP2:
 - Open Administration Web pages for MyAP2 by using MyAP2’s IP address in a URL.
 - Navigate to the WDS tab on MyAP2 Administration Web pages. (MyAP2’s MAC address will show as the “Local Address”.)
 - Configure a WDS interface for data exchange with MyAP1, starting with the MAC address for MyAP1.
 - Navigate to the radio settings for MyAP2 to verify that it is using the same mode and broadcasting on the same channel as MyAP1. (For our example Mode is 802.11b and the channel is 6.)
 - Be sure to save the settings by clicking **Update**.

20.3 Updating Settings

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

NETWORK TIME PROTOCOL SERVER 21

21.1 Navigating To Time Protocol Settings	199
21.2 Enabling Or Disabling A Network Time Protocol (NTP) Server	200
21.3 Updating Settings.	200

The *Network Time Protocol (NTP)* is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time (UTC)*, also known as *Greenwich Mean Time* to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

The timestamp will be used to indicate the date and time of each event in log messages.

See <http://www.ntp.org> for more general information on NTP.

The following sections describe how to configure the 9160 Wireless Gateway to use a specified NTP server.

21.1 Navigating To Time Protocol Settings

To enable an *NTP* server, navigate to the *Advanced, Time Protocol* tab, and update the fields as described below.

The screenshot shows the configuration interface for the Network Time Protocol (NTP) server. On the left is a navigation menu with categories: BASIC SETTINGS, CLUSTER, STATUS, and ADVANCED. The ADVANCED section is expanded, showing options like Ethernet (Wired) Settings, Wireless Settings, Security, Guest Login, Radio, MAC Filtering, Load Balancing, Quality of Service, Wireless Distribution System, Time Protocol, Reset Configuration, Upgrade, and Backup/Restore. The main content area is titled 'Modify how the access point discovers the time'. It contains a toggle for 'Network Time Protocol (NTP)' set to 'Disabled', an empty 'NTP Server' text field, and an 'Update' button. A help sidebar on the right explains that NTP is an Internet standard protocol for synchronizing clock times and provides a link to <http://www.ntp.org> for more information.

BASIC SETTINGS	Modify how the access point discovers the time		? Use this page to configure the access point to use a specified Network Time Protocol (NTP) server. "NTP" is an Internet standard protocol that synchronizes computer clock times on a network. NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. See http://www.ntp.org for more information on NTP. More ...
CLUSTER	Network Time Protocol (NTP) ☐ Enabled ☒ Disabled		
Access Points	NTP Server		
User Management	Update		
Sessions			
Channel Management			
Wireless Neighborhood			
STATUS			
Interfaces			
Events			
Transmit / Receive Statistics			
Client Associations			
Neighboring Access Points			
ADVANCED			
Ethernet (Wired) Settings			
Wireless Settings			
Security			
Guest Login			
Radio			
MAC Filtering			
Load Balancing			
Quality of Service			
Wireless Distribution System			
Time Protocol			
Reset Configuration			
Upgrade			
Backup/Restore			

21.2 Enabling Or Disabling A Network Time Protocol (NTP) Server

To configure your access point to use a network time protocol (*NTP*) server, first **enable** the use of NTP, and then select the NTP server you want to use. (To shut down NTP service on the network, disable NTP on the access point.)

Field	Description
<i>Network Time Protocol</i>	NTP provides a way for the access point to obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information. See http://www.ntp.org for more general information on NTP. Choose to either enable or disable the use of a network time protocol (NTP) server: • Enabled • Disabled
<i>NTP Server</i>	If NTP is enabled, select the NTP server you want to use. You can specify the NTP server by host name or IP address, although using the IP address is not recommended as these can change more readily.

Table 21.1 NTP Settings

21.3 Updating Settings

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

THE ADMINISTRATOR PASSWORD 22

22.1 Navigating To Administrator Password Setting	203
22.2 Setting The Administrator Password.	203
22.3 Updating Settings.	204

The administrator password controls access to the Administration Web pages for the 9160 Wireless Gateway. This setting is also available on the *Basic Settings* administration page. When you set the administration password in either place and apply the change, the new password is updated and shared by all access points in the cluster.

The following sections describe how to configure the Administrator password on the 9160 Wireless Gateway.

22.1 Navigating To Administrator Password Setting

To set the administrator password, navigate to the *Advanced, Password* tab, and update the fields as described below.

22.2 Setting The Administrator Password

To set a new administrator password, fill in the password and then re-confirm. The password setting requires that you know the existing password before you can change it. This is to prevent an unauthorized person from changing the password in a case where you leave an open browser unattended. See Table 22.1 on page 204.

Field	Description
Existing Password	Enter the current administrator password. (The factory default password is admin .) The text you enter will be displayed as “ * ” characters to prevent others from seeing your password as you type.
New Password	Enter a new administrator password. The Administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces. Re-enter the new administrator password to confirm that you typed it as intended.

Table 22.1 Administrator Password Settings

22.3 Updating Settings

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

MAINTENANCE AND MONITORING 23

23.1 Interfaces	207
23.1.1 Ethernet (Wired) Settings	208
23.1.2 Wireless Settings	208
23.2 Event Logs	208
23.2.1 Log Relay Host For Kernel Messages.	209
23.2.1.1 Understanding Remote Logging.	209
23.2.1.2 Setting Up The Log Relay Host	210
23.2.1.3 Enabling Or Disabling The Log Relay Host On The Status, Events Page	211
23.2.2 Events Log.	212
23.3 Transmit/Receive Statistics	212
23.4 Associated Wireless Clients.	214
23.4.1 Link Integrity Monitoring	214
23.4.2 What Is The Difference Between An Association And A Session? .215	
23.5 Neighboring Access Points	215
23.6 Rebooting The Access Point	218
23.7 Resetting The Configuration To Factory Defaults	218
23.8 Upgrading The Firmware	219
23.8.1 Update	221
23.8.2 Verifying The Firmware Upgrade	221



Important: *The maintenance and monitoring tasks described here all pertain to viewing and modifying settings on specific access points; not on a cluster configuration that is automatically shared by multiple access points. Therefore, it is important to ensure that you are accessing the Administration Web pages for the particular access point you want to configure. For information on this, see “Navigating To Configuration Information For A Specific AP And Managing Standalone APs” on page 63.*

23.1 Interfaces

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



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

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

View settings for network interfaces

Wired Settings

(Configure)

Internal Interface

MAC Address 00:0C:41:0A:33:7E

VLAN ID

IP Address 10.10.103.214

Subnet Mask 255.255.255.0

Guest Interface

MAC Address 00:00:00:00:00:00

VLAN ID

Subnet n/a

Wireless Settings

(Configure)

Radio

Mode IEEE 802.11g

Channel 6 (2437 MHz)

Internal Interface

MAC Address 00:0C:41:0A:33:7E

Network Name (SSID) TEKLOGIX

Guest Interface

MAC Address n/a

Network Name (SSID) TEKLOGIX GUEST

?

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

To configure Ethernet Settings, go to the [Ethernet \(Wired\) Settings](#) tab.

To configure Wireless Settings, go to the [Wireless Settings](#) tab.

[More ...](#)

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

23.1.1 Ethernet (Wired) Settings

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

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

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

23.1.2 Wireless Settings

The *Radio* interface includes settings for radio **Mode**, and **Channel**. Also shown here are **MAC addresses** (read-only) for internal and guest interfaces. (See Chapter 12: “Setting the Wireless Interface” and Chapter 16: “Configuring Radio Settings” for more information.)

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

23.2 Event Logs

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

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

View events generated by this access point

Log Relay Host

Enabled

Disabled

Relay Host

Relay Port

514

Update

Events Log

Time	Severity	Service	Description
Oct 21 11:21:53	info	udhcpd	Lease of 10.10.103.214 obtained, lease time 300
Oct 21 11:21:53	debug	udhcpd	Sending renew...
Oct 21 11:19:23	info	udhcpd	Lease of 10.10.103.214 obtained, lease time 300
Oct 21 11:19:23	debug	udhcpd	Sending renew...
Oct 21 11:19:12	info	login[245]	root login on 'tty0'
Oct 21 11:16:53	info	udhcpd	Lease of 10.10.103.214 obtained, lease time 300
Oct 21 11:16:53	debug	udhcpd	Sending renew...
Oct 21 11:14:23	info	udhcpd	Lease of 10.10.103.214 obtained, lease time 300
Oct 21 11:14:23	debug	udhcpd	Sending select for 10.10.103.214...
Oct 21 11:14:22	debug	udhcpd	Sending discover...
Oct 21 11:14:12	debug	udhcpd	Sending discover...
Oct 21 11:14:08	debug	udhcpd	Sending discover...
Oct 21 11:14:07	info	dropbear[246]	Not forking
Oct 21 11:14:06	info	udhcpd	udhcp client (v0.9.8-pre) started

?

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

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

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

[More ...](#)

This page lists the most recent events generated by this access point (see “Events Log” on page 212).

This page also gives you the option of enabling a remote “log relay host” to capture all system events and errors in a Kernel Log. (This requires setting up a remote relay host first. See “Log Relay Host For Kernel Messages” on page 209).



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

For information on setting the network time protocol, see Chapter 21: “Network Time Protocol Server”.

23.2.1 Log Relay Host For Kernel Messages

- “Understanding Remote Logging” on page 209.
- “Setting Up The Log Relay Host” on page 210.
- “Enabling Or Disabling The Log Relay Host On The Status, Events Page” on page 211.

23.2.1.1 Understanding Remote Logging

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

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

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

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

23.2.1.2 Setting Up The Log Relay Host

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

Example Of Using Linux syslogd

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

Log Relay Host Enabled

☒ Enabled
 ☐ Disabled

Relay Host

10.10.100.107

Relay Port

514

Update

Field	Description
<i>Log Relay Host Enabled</i>	Choose to either enable or disable use of the Log Relay Host: Enabled Disabled If you select Enabled , the <i>Relay Host</i> and <i>Relay Port</i> fields are editable.
<i>Relay Host</i>	Specify the IP Address or DNS name of the Relay Host.
<i>Relay Port</i>	Specify the Port number for the syslog process on the Relay Host. The default port is 514 .

Table 23.1 Log Relay Host Settings

Update Settings

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

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

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

23.2.2 Events Log

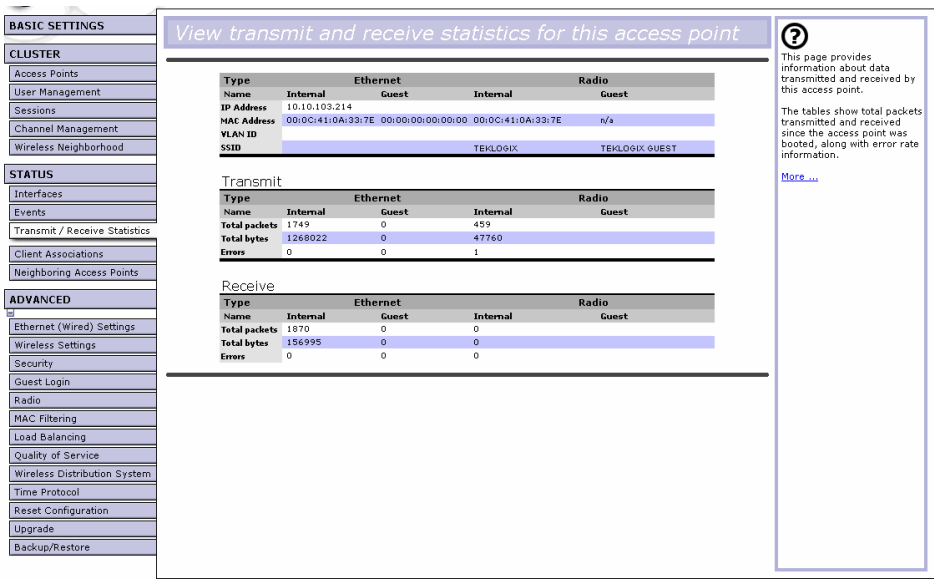
The Events Log shows system events on the access point such as stations associating, being authenticated, and other occurrences. The real-time Events Log is always shown on the *Status, Events* Administration Web UI page for the access point you are monitoring.

23.3 Transmit/Receive Statistics

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



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



This page provides some basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in Table 23.2 on page 213. All transmit and receive statistics shown are totals since the access point was last started. If the AP is rebooted, these figures indicate transmit/receive totals since the re-boot.

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

Table 23.2 Transmit/Receive Statistics

23.4 Associated Wireless Clients

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

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Virtual Wireless Networks

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reboot

Reset Configuration

Upgrade

Backup/Restore

View list of currently associated client stations

Radio	Network	Station	Status		From Station		To Station	
			Authenticated	Associated	Packets	Bytes	Packets	Bytes
One	Internal	00:0e:35:f4:c1:ef:d6	Yes	Yes	41	2344	19	2748
Two	Internal	00:0c:41:dc:09:e1	Yes	Yes	1992	277679	1760	681683

?

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

[More...](#)

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

23.4.1 Link Integrity Monitoring

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

23.4.2 What Is The Difference Between An Association And A Session?

An *association* describes a client connection to a particular access point. A *session* describes a client connection to the network. 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 on monitoring *sessions*, see “Understanding Session Monitoring Information” on page 76.

23.5 Neighboring Access Points

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

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

BASIC SETTINGS

CLUSTER

Access Points

User Management

Sessions

Channel Management

Wireless Neighborhood

STATUS

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

ADVANCED

Ethernet (Wired) Settings

Wireless Settings

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Time Protocol

Reset Configuration

Upgrade

Backup/Restore

View neighboring access points

AP Detection ☒ Enabled ☐ Disabled

Update

MAC Addr.	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	# of Beacons	Last Beacon	Rates
00:e0:b8:76:26:0a	100	AP	Virtual Wireless Network 1	On	On	2.4	6	10	33	1455	Thu Oct 21 11:23:47 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:e0:b8:76:17:a3	100	AP	TEKLOGIX GUEST	Off	Off	2.4	11	10	14	1	Thu Oct 21 11:20:17 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:e0:b8:76:28:cf	100	AP	kamesh-vwn1	Off	Off	2.4	6	10	50	891	Thu Oct 21 11:18:30 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:e0:b8:76:26:71	100	AP	kamesh-vwn1	Off	Off	2.4	6	10	45	837	Thu Oct 21 11:18:28 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:e0:b8:76:25:f3	100	AP	kamesh-vwn1	Off	Off	2.4	6	10	43	1184	Thu Oct 21 11:18:26 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:0a:38:e2:62:20	2000	AP	Brad Lab IOS	Off	Off	2.4	8	10	31	32	Thu Oct 21 11:23:37 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:0b:46:ca:5e:15	100	AP	ikm-leap	On	Off	5	64	60	22	1	Thu Oct 21 11:15:35 2004	6, 9, 12, 18, 24, 36, 48, 54
02:0c:41:00:00:82	100	AP	Virtual Wireless Network 1	Off	Off	2.4	6	10	11	1286	Thu Oct 21 11:23:41 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
00:e0:b8:76:1a:f6	100	AP	TEKLOGIX	Off	Off	2.4	6	10	21	2399	Thu Oct 21 11:23:47 2004	1.2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54

?

This page shows configuration information and statistics on neighboring access points.

"Neighboring access points" are those which are within range of detection, whether they are on the same wireless network or not.

More...

Information provided on neighboring access points is described in Table 23.3.

Field	Description
MAC Address	Shows the MAC address of the neighboring access point. A MAC address is a hardware address that uniquely identifies each node of a network.
Radio	Two-Radio APs If the access point that is “doing the detecting” of neighboring APs is a two-radio access point, the Radio field is included. The Radio field indicates which radio the neighboring AP was detected on: • wlan0 (Radio One) • wlan1 (Radio Two) One-Radio APs This field is not included on the <i>Neighboring Access Points</i> pages of one-radio access points.
Beacon Interval	Shows the Beacon interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on the <i>Advanced, Radio Settings</i> page. (See Chapter 16: “Configuring Radio Settings”.)
Type	Indicates the type of device: • AP indicates the neighboring device is an access point that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode. • Ad hoc indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional access point. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as “peer-to-peer” mode or an <i>Independent Basic Service Set (IBSS)</i>.
SSID	The <i>Service Set Identifier (SSID)</i> for the access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the “Network Name”. The SSID is set in Basic Settings. (See Chapter 5: “Configuring Basic Settings”) or in <i>Advanced, Wireless Settings</i> (see 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.

Table 23.3 Neighboring Access Point Statistics

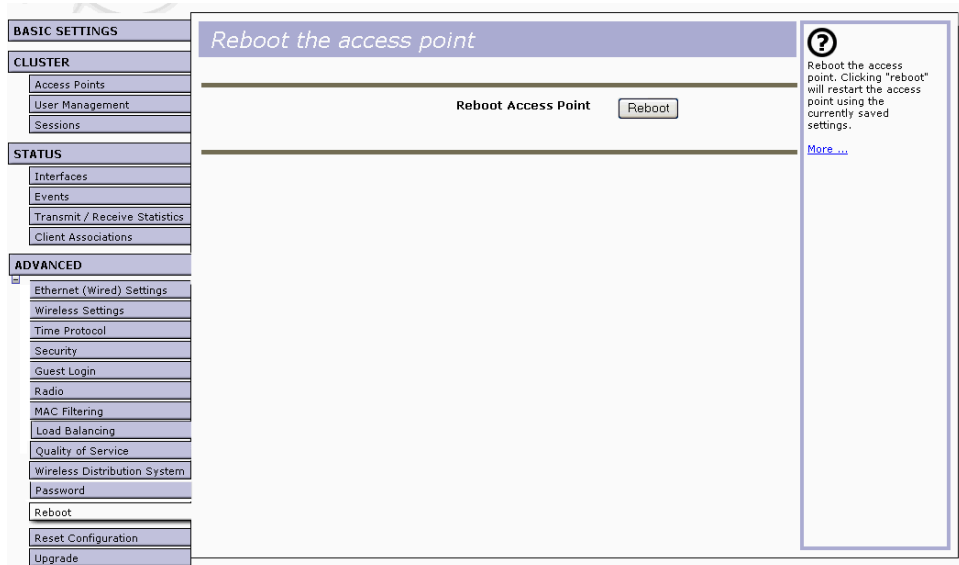
Field	Description
<i>Privacy</i>	Indicates whether there is any security on the neighboring device. • Off indicates that the Security mode on the neighboring device is set to “plain-text” mode (no security). • On indicates that the neighboring device has some security in place. Security is configured on the AP at <i>Advanced, Security</i>. For more information on security settings, see Chapter 13: “Configuring Security”.
<i>WPA</i>	Indicates whether WPA security is On or Off for this access point.
<i>Band</i>	This indicates the IEEE 802.11 mode being used on this access point. (For example, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.) The number shown indicates the mode according to the following map: • 2.4 indicates IEEE 802.11b mode or IEEE 802.11g mode. • 5 indicates IEEE 802.11a mode.
<i>Channel</i>	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 <i>Advanced, Radio Settings</i>. (See Chapter 16: “Configuring Radio Settings”.)
<i>Rate</i>	Shows the rate (in megabits per second) at which this access point is currently transmitting. The current rate will always be one of the supported rates shown in <i>Rates</i>.
<i>Signal</i>	Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).
<i># of Beacons</i>	Shows the total number of beacons transmitted by this access point since it was last booted.
<i>Last Beacon</i>	Shows the date and time that the most recent beacon was transmitted from the access point.
<i>Rates</i>	Shows supported and basic (advertised) rate sets for the neighboring access point. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on <i>Advanced, Radio Settings</i>. (See Chapter 16: “Configuring Radio Settings”.) The rates shown for an access point will always be the rates currently specified for that AP in its <i>Radio Settings</i>.

Table 23.3 Neighboring Access Point Statistics

23.6 Rebooting The Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the 9160 Wireless Gateway as follows.

1. Click the *Advanced, Reboot* tab.



2. Click the **Reboot** button.
The AP reboots.

23.7 Resetting The Configuration To Factory Defaults

If you are experiencing extreme problems with the 9160 Wireless Gateway and have tried all other troubleshooting measures, use the *Reset Configuration* function. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

1. Click the *Advanced, Reset Configuration* tab.

BASIC SETTINGS	Reset the access point back to factory settings	 Reset the access point back to factory settings. Clicking "reset" will restore factory defaults and clear all settings, including settings such as a new password or wireless settings. More ...
CLUSTER	Restore Factory Default Configuration Reset	
Access Points		
User Management		
Sessions		
Channel Management		
Wireless Neighborhood		
STATUS		
Interfaces		
Events		
Transmit / Receive Statistics		
Client Associations		
Neighboring Access Points		
ADVANCED		
Ethernet (Wired) Settings		
Wireless Settings		
Security		
Guest Login		
Radio		
MAC Filtering		
Load Balancing		
Quality of Service		
Wireless Distribution System		
Time Protocol		
Reset Configuration		
Upgrade		
Backup/Restore		

2. Click the **Reset** button.

Factory defaults are restored.



Note: *Keep in mind that if you do reset the configuration from this page, you are doing so for this access point only; not for other access points in the cluster.*

For information on the factory default settings, see “Default Settings For The 9160 Wireless Gateway” on page 23.

23.8 Upgrading The Firmware

As new versions of the 9160 Wireless Gateway firmware become available, you can upgrade the firmware on your devices to take advantage of new features and enhancements.



Important: *Do not upgrade the firmware from a wireless client that is associated with the access point you are upgrading. Doing so will cause the upgrade to fail. Furthermore, all wireless clients will be disassociated and no new associations will be allowed.*

If you encounter this scenario, the solution is to use a wired client to gain access to the access point:

- *Create a wired Ethernet connection from a PC to the access point.*
- *Bring up the Administration UI.*

Repeat the upgrade process using with the wired client.



Note: *You must do this per access point; you cannot upgrade firmware automatically across the cluster.*

Keep in mind that a successful firmware upgrade restores the access point configuration to the factory defaults. (See “Default Settings For The 9160 Wireless Gateway” on page 23.)

To upgrade the firmware on a particular access point:

1. Navigate to *Advanced, Upgrade* on the Administration Web pages for that access point.

BASIC SETTINGS

CLUSTER

STATUS

ADVANCED

Access Points

User Management

Sessions

Interfaces

Events

Transmit / Receive Statistics

Client Associations

Neighboring Access Points

Ethernet (Wired) Settings

Wireless Settings

Time Protocol

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Quality of Service

Wireless Distribution System

Password

Reset Configuration

Upgrade

Upgrade firmware

ModelGateway 7001 802.11 G Wireless Access Point

Platformx86pc

Firmware VersionDEV 11

New Firmware Image

Browse...

Update

?

On this page you can upgrade the firmware of the access point to get new features and bug fixes.

Firmware upgrades are available at <http://www.instant802.com/>.

The upgrade file must be in the format `<221aWes>.upgrade.tar`.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation using factory default configuration settings.

[More ...](#)

Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.

2. If you know the path to the *New Firmware Image* file, enter it in the textbox. Otherwise, click the **Browse** button and locate the firmware image file.



Note: *The firmware upgrade file supplied must be in the format <File-Name>.upgrade.tar. Do not attempt to use <FileName>.bin files or files of other formats for the upgrade; these will not work.*

23.8.1 Update

Click **Update** to apply the new firmware image.

Upon clicking **Update** for the firmware upgrade, a popup confirmation window is displayed that describes the upgrade process.

Click **OK** to confirm the upgrade, and start the process.



Important: *The firmware upgrade process begins once you click Update and then OK in the popup confirmation window.*

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation using the factory default configuration settings.

23.8.2 Verifying The Firmware Upgrade

To verify that the firmware upgrade completed successfully, check the firmware version shown on the *Advanced, Upgrade* tab (and also on the *Basic Settings* tab). If the upgrade was successful, the updated version name or number will be indicated.

BACKING UP THE CONFIGURATION 24

24.1 Navigating To Backup And Restore Settings	225
24.2 Backing Up Configuration Settings For An Access Point	225
24.3 Restoring Access Point Settings To A Previous Configuration	226

You can save a copy of the current settings on the 9160 Wireless Gateway to a backup configuration file. The backup file can be used at a later date to restore the access point to the previously saved configuration.

24.1 Navigating To Backup And Restore Settings

To backup or restore a configuration for an access point, navigate to the *Advanced*, *Backup and Restore* tab and use the interface as described below.

STATUS

- Interfaces
- Events
- Transmit / Receive Statistics
- Client Associations
- QoS Monitor

ADVANCED

- Ethernet (Wired) Settings
- Wireless Settings
- Security
- Password
- Radio
- MAC Filtering
- Wireless Distribution System
- Time Protocol
- Reset Configuration
- Upgrade
- Backup/Restore

Backup or Restore this Access Point's Configuration

To Save the Current Configuration to a Backup File ...

Click the link below to download a file containing the current configuration for this AP.

[\[download configuration\]](#)

To Restore the Configuration from a Previously Saved File ...

Enter the path and file name of the configuration backup file you want to use, or click "Browse" to open a dialog where you can locate and select the file. Then click "Restore" to load this file in place of the current configuration.

Note: When you click "Restore", the access point will reboot. Please wait for the reboot process to complete (a minute or two). After a moment, try accessing the AP Administration Web pages again. The Administration Web pages will not be accessible until the AP has rebooted.

Upon reboot, you should see the configuration settings restored to those contained in the specified backup file.

24.2 Backing Up Configuration Settings For An Access Point

To save a copy of the current settings on an access point to a backup configuration file (.cbk format):

1. Click the **download configuration** link.
A File Download or Open dialog is displayed.
2. Choose the **Save** option on this first dialog.
This brings up a file browser.
3. Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

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

24.3 Restoring Access Point Settings To A Previous Configuration

To restore the configuration on an access point to previously saved settings:

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

(Only those files that were created with the Backup function and saved as `.cbk` backup configuration files are valid to use with Restore; for example, `apconfig.cbk`.)

2. Click the **Restore** button.

The access point will reboot.



Note: *When you click **Restore**, the access point will reboot. A “reboot” confirmation dialog and follow-on “rebooting” status message will be displayed. Please wait for the reboot process to complete (a minute or two). After a moment, try accessing the Administration Web pages as described in the next step; they will not be accessible until the AP has rebooted.*

When the access point has rebooted, access the Administration Web pages either by clicking again on one of the tabs (if the UI is still displayed) or by typing the IP address of the 9160 Wireless Gateway as a URL in the address field of the Web browser. The URL for the Access Point should be entered as `http://IPAddressOfAccessPoint`.

Now you should see the configuration settings restored to the saved configuration from the Backup file you selected.

25.1 Physical Description	229
25.2 Environmental Requirements	229
25.3 AC Power Requirements	229
25.4 Power Over Ethernet Requirements	230
25.5 Processor And Memory	230
25.6 Network Interfaces	230
25.7 Mini-PCI Card Radios	230



Note: *Performance specifications are nominal and subject to change without notice.*

25.1 Physical Description

Enclosure:	Jet black in colour, FR2000 bay blend material
Dimensions:	$\leq 30 \times 20 \times 12.5$ cm (11.8 x 7.9 x 4.9 in.)
Weight:	≤ 2.25 kg (5.0 lbs.) (excludes radios, antennas, and options)

25.2 Environmental Requirements

Operating Temperature:	0°C to 55°C (32°F to 131°F)
Operating Rel. Humidity:	10% to 90%
Storage Temperature:	0°C to 70°C (32°F to 158°F)
Dust and Rain:	IP42 or greater
Vibration:	EH0002 (Shipping vibration only)
Reliability:	MTBF 25,000 Hours (MIL-HDBK-217F)

25.3 AC Power Requirements

AC universal input via a standard IEC320 connector. Disables Power over Ethernet (802.3af discovery) when connected.

Input voltage:	100 - 240 VAC nominal
Current:	5.0 A maximum



Warning: *A ground wire, not exceeding 3 m in length, must be connected between the ground screw (located on the quick-release mount) and a suitable earth ground bonding point on any 9160 connected to an antenna that is installed outdoors.*

25.4 Power Over Ethernet Requirements

Compliant with IEEE 802.3af (disabled when AC power is connected).	
Input voltage:	37 - 57 VDC
On-board	
Power Supplies:	2.5W (Assume $\eta=0.8$ at full 12.5 watt from Ethernet)
Dual 802.11b radios:	4W
Main Logic Board:	6W

25.5 Processor And Memory

Intel IXP420 processor running at 266 MHz	
8 MB Flash ROM	
32 MB SDRAM	

25.6 Network Interfaces

On-Board Ethernet:	10BaseT/100BaseT (10/100Mb/s) card with auto-negotiation, half and full duplex. Data rate is auto-sensed.
--------------------	--

25.7 Mini-PCI Card Radios

Mini-PCI card 802.11A/G radio without integrated antenna	
Mini-PCI card 802.11G radio without integrated antenna	
Transmitter Power	100 mW for FCC countries; 50 mW for ETSI
Frequency Range	2.4 - 2.5 GHz (802.11b/g); 5.1 - 5.5 GHz (802.11a)
Data Rate	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 54 Mb/s
No. of Channels	11 802.11b/g - 12 802.11a (FCC)
	13 802.11b/g - 19 802.11a (ETSI)

APPENDIX

A

SUPPORT SERVICES AND WORLDWIDE OFFICES

Psion Teklogix provides a complete range of product support services to its customers worldwide. These services include technical support and product repairs.

A.1 Technical Support

Technical Support for Mobile Computing Products is provided via e-mail through the Psion Teklogix customer and partner extranets. To reach the website, go to www.psionteklogix.com and click on the appropriate Teknet link on the home page. Then click on the “Log-in” button or the “Register” button, depending on whether you have previously registered for Teknet. Once you have logged in, search for the “Support Request Form”.

A.2 Product Repairs

International

For technical support outside of Canada or the U.S.A., please contact your local Psion Teklogix office listed on our worldwide website:

<http://www.psionteklogix.com>

Click on the heading labelled “Contacts” to choose a Psion Teklogix technical support representative closest to you.

Canada/U.S.A

Canadian and U.S. customers can receive access to repair services, by calling the toll-free number below, or via our secure website (see *Technical Support*, above).



Note: *Customers calling the toll-free number should have their Psion Teklogix customer number or trouble ticket number available.*

Voice: 1 800 387-8898 (press option “2”)

Fax: 1 905 812-6304

Website: <http://service.psionteklogix.com>

A.3 Worldwide Offices

COMPANY HEADQUARTERS AND CANADIAN SERVICE CENTRE

Psion Teklogix Inc.

2100 Meadowvale Blvd.

Mississauga, Ontario

Canada L5N 7J9

Tel: +1 905 813 9900

Fax: +1 905 812 6300

E-mail: salescdn@psion.com

NORTH AMERICAN HEADQUARTERS AND U.S. SERVICE CENTRE

Psion Teklogix Corp.

1810 Airport Exchange Boulevard

Suite 500

Erlanger, Kentucky

USA 41018

Tel: +1 859 371 6006

Fax: +1 859 371 6422

E-mail: salesusa@psion.com

INTERNATIONAL SUBSIDIARIES

(SEE ALSO WWW.PSIONTEKLOGIX.COM)

Psion Teklogix S.A.

La Duranne

135 Rue Rene Descartes

BP 421000

13591 Aix-En-Provence

Cedex 3; France

Tel: +33 4 42 90 88 09

Fax: +33 4 42 90 88 88

E-mail: tekeuro@psion.com

APPENDIX **B**

PORT PINOUTS AND CABLE DIAGRAMS

B.1 Console Port

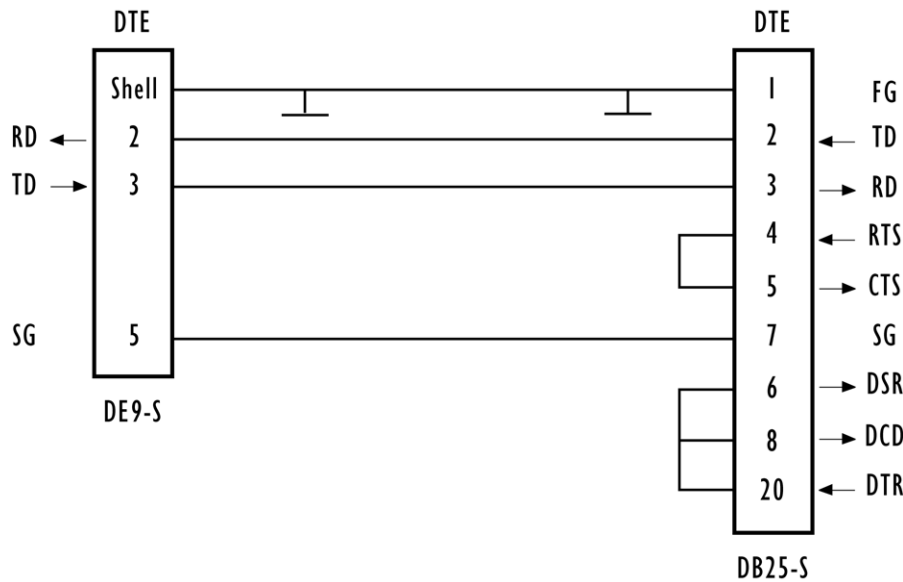
Pin No.	Name	Function	Direction
3	TD	Transmit Data	Out
2	RD	Receive Data	In
5	SG	Signal Ground	—
4*	DTR	Data Terminal Ready	Out
7*	RTS	Request to Send	Out

* always pulled high

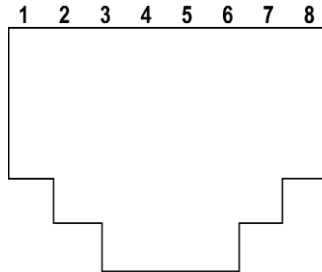
B.2 Serial Cable Descriptions

Cable No.	Function	Connection	Standard Length
19387	9160 to Console	Direct	6 feet

Console Port Cable No. 19387



B.3 RJ-45 Connector Pinouts (10BaseT/100BaseT Ethernet)



9160 using AC		9160 using Power over Ethernet*	
Contact	Signal	Contact	Signal
1	TD+	1	TD+
2	TD-	2	TD-
3	RD+	3	RD+
4	Not used	4	
5	Not used	5	
6	RD-	6	RD-
7	Not used	7	
8	Not used	8	
		* The 9160 can also accept 48 VDC power bias on the data line pairs (1,2) and (3,6) from such systems providing power over Ethernet.	



Note: Usually, a straight-through connection is needed to connect Twisted-Pair (10BaseT or 100BaseT) to the hub.

APPENDIX C

CONFIGURING SECURITY SETTINGS ON WIRELESS CLIENTS

C.1 Network Infrastructure And Choosing Between Built-in Or External Authentication Server.	C-4
C.1.1 Using The Built-in Authentication Server (EAP-PEAP)	C-4
C.1.2 Using An External RADIUS Server With EAP-TLS Certificates Or EAP-PEAP	C-4
C.2 Make Sure The Wireless Client Software Is Up-to-Date	C-5
C.3 Accessing The Microsoft Windows Wireless Client Security Settings. . .	C-5
C.4 Configuring A Client To Access An Unsecure Network (Plain-text Mode) C-7	
C.5 Configuring Static WEP Security On A Client	C-8
C.6 Configuring IEEE 802.1x Security On A Client	C-11
C.6.1 IEEE 802.1x Client Using EAP/PEAP	C-11
C.6.2 IEEE 802.1x Client Using EAP/TLS Certificate	C-14
C.7 Configuring WPA/WPA2 Enterprise (RADIUS) Security On A Client .	C-18
C.7.1 WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP . .	C-19
C.7.2 WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate	C-23
C.8 Configuring WPA/WPA2 Personal (PSK) Security On A Client.	C-27
C.9 Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway	C-30
C.10 Obtaining A TLS-EAP Certificate For A Client.	C-34

Typically, users will configure security on their wireless clients for access to many different networks (access points). The list of “Available Networks” will change depending on the location of the client and which APs are online and detectable in that location.¹ Once an AP has been detected by the client and security is configured for it, it remains in the client’s list of networks but shows as either reachable or unreachable depending on the situation. For each network (AP) you want to connect to, configure security settings on the client to match the security mode being used by that network.

We describe security setup on a client that uses Microsoft® Windows® client software for wireless connectivity. The Windows client software is used as the example because of its widespread availability on Windows computers and laptops. These procedures will vary slightly if you use different software on the client (such as Funk Odyssey®), but the configuration information you need to provide is the same.



Note: *The recommended sequence for security configuration is (1) set up security on the access point, and (2) configure security on each of the wireless clients.*

We expect that initially, you will connect to an access point that has no security set (plain-text mode) from an unsecure wireless client. With this initial connection, you can go to the access point Administration Web pages and configure a security mode (Advanced, Security).

*When you re-configure the access point with a security setting and click **Update**, your wireless client will be disassociated and you will lose connectivity to the AP Administration Web pages. In some cases, you may need to make additional changes to the AP security settings before configuring the client. Therefore, you must have a backup Ethernet (wired) connection.*

The following sections describe how to set up each of the supported security modes on wireless clients of a network served by the 9160 Wireless Gateway.

¹The exception to this is if the access point is set to prohibit the broadcast of its network name. In this case the SSID will not show up in the list of Available Networks on the client. Instead, the client must have the exact network name configured in the network connection properties before it will be able to connect.

C.1 Network Infrastructure And Choosing Between Built-in Or External Authentication Server

Network security configurations including *Public Key Infrastructures* (PKI), *Remote Authentication Dial-in User Server* (RADIUS) servers, and *Certificate Authority* (CA) can vary a great deal from one organization to the next in terms of how they provide *Authentication*, *Authorization*, and *Accounting* (AAA). Ultimately, the particulars of your infrastructure will determine how clients should configure security to access the wireless network. Rather than try to predict and address the details of every possible scenario, this document provides general guidelines about each type of client configuration supported by the 9160 Wireless Gateway.

C.1.1 Using The Built-in Authentication Server (EAP-PEAP)

If you do not have a RADIUS server or PKI infrastructure in place and/or are unfamiliar with many of these concepts, we strongly recommend setting up the 9160 Wireless Gateways with security that uses the *Built-in Authentication Server* on the AP. This will mean setting up the AP to use either IEEE 802.1x or WPA/WPA2 Enterprise (RADIUS) security mode. (The built-in authentication server uses EAP-PEAP authentication protocol.)

- If the 9160 Wireless Gateway is set up to use IEEE 802.1x mode and the Built-in Authentication Server, then configure wireless clients as described in “IEEE 802.1x Client Using EAP/PEAP” on page C-11.
- If the 9160 Wireless Gateway is configured to use WPA/WPA2 Enterprise (RADIUS) mode and the Built-in Authentication Server, configure wireless clients as described in “WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP” on page C-19.

C.1.2 Using An External RADIUS Server With EAP-TLS Certificates Or EAP-PEAP

We make the assumption that if you have an external RADIUS server and PKI/CA setup, you will know how to configure client security options appropriate to your security infrastructure beyond the fundamental suggestions given here. Topics covered here that particularly relate to client security configuration in a RADIUS - PKI environment are:

- “IEEE 802.1x Client Using EAP/TLS Certificate” on page C-14.
- “WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate” on page C-23.
- “Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway” on page C-30.
- “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Details on how to configure an EAP-PEAP client with an external RADIUS server are not covered in this document.

C.2 Make Sure The Wireless Client Software Is Up-to-Date

Before starting out, please keep in mind that service packs, patches, and new releases of drivers and other supporting technologies for wireless clients are being generated at a fast pace. A common problem encountered in client security setup is not having the right driver or updates to it on the client. For example, if you are setting up WPA on the client, make sure you have a driver installed that supports WPA, which is a relatively new technology. Even many client cards currently available do not ship from the factory with the latest drivers.

C.3 Accessing The Microsoft Windows Wireless Client Security Settings

Generally, on Windows XP there are two ways to get to the security properties for a wireless client:

1. From the *Wireless Connection* icon on the Windows task bar:
 - Right-click on the Wireless connection icon in your Windows task bar and select **View available wireless networks**.
 - Select the SSID of the network to which you want to connect and click **Advanced** to bring up the *Wireless Network Connection Properties* dialog.

OR

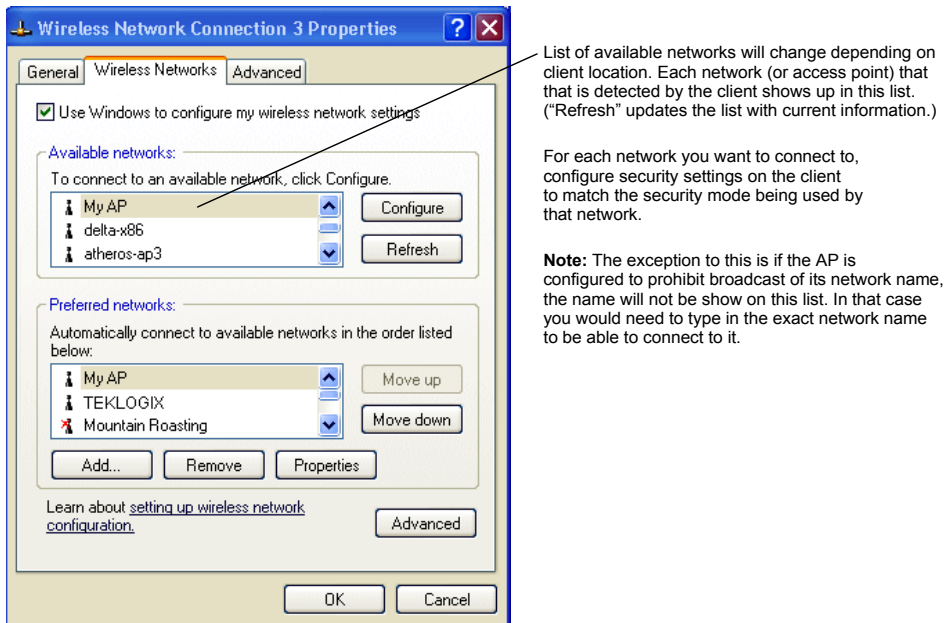
2. From the Windows *Start* menu at the left end of the task bar:
 - From the Windows *Start* menu on the task bar, choose **Start, My Network Places** to bring up the Network Connections window.

Appendix C: Configuring Security Settings On Wireless Clients

Accessing The Microsoft Windows Wireless Client Security Settings

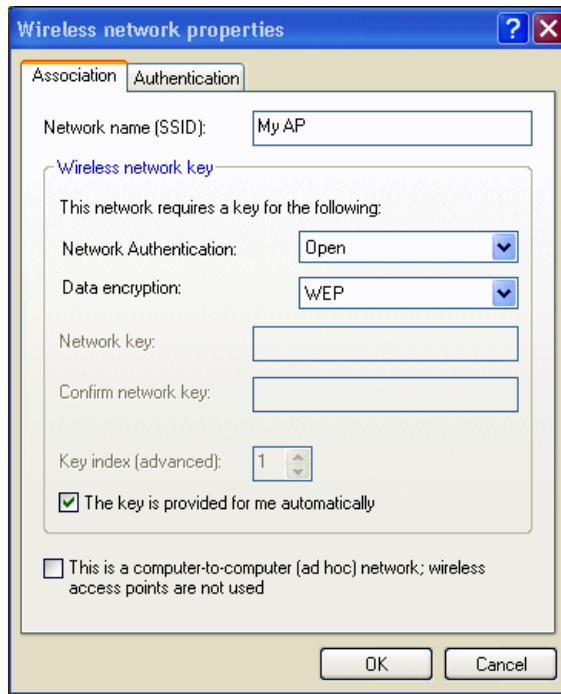
- From the *Network Tasks* menu on the left, click **View Network Connections** to bring up the *Network Connections* window.
- Select the *Wireless Network Connection* you want to configure, right-mouse click and choose **View available wireless networks**.
- Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

The *Wireless Networks* tab (which should be automatically displayed) lists *Available networks* and *Preferred networks*.



3. From the list of *Available networks*, select the SSID of the network to which you want to connect and click **Configure**.

This brings up the *Wireless Network Connection Properties* dialog with the *Association* and *Authentication* tabs for the selected network.



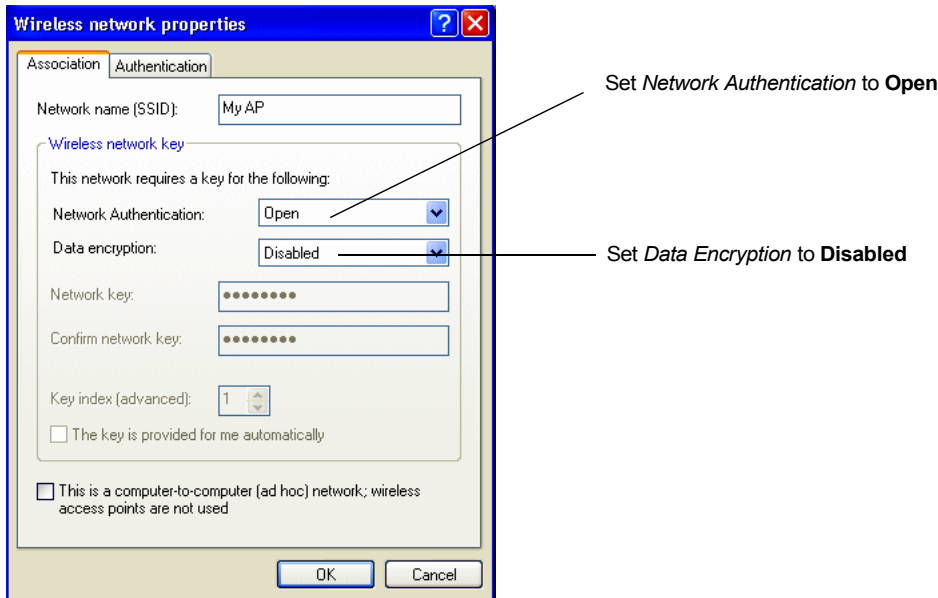
Use this dialog for configuring all the different types of client security described in the following sections. Make sure that the *Wireless Network Properties* dialog you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

C.4 Configuring A Client To Access An Unsecure Network (Plain-text Mode)

If the access point or wireless network to which you want to connect is configured as “Plain-text” security mode (no security), you need to configure the client accordingly. A client using no security to connect is configured with *Network Authentication* **Open** to that network and *Data Encryption* **Disabled**, as described below.

If you do have security configured on a client for properties of an unsecure network, the security settings actually can prevent successful access to the network because of the mismatch between client and access point security configurations.

To configure the client to not use any security, bring up the client *Network Properties* dialog, and configure the following settings.



Network Authentication	Open
Data Encryption	Disabled

Table C.1 Association Settings

C.5 Configuring Static WEP Security On A Client

Static *Wired Equivalent Privacy* (WEP) encrypts data moving across a wireless network based on a static (non-changing) key. The encryption algorithm is a “stream” cipher called RC4. The access point uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the access point. Different clients can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

Appendix C: Configuring Security Settings On Wireless Clients

Configuring Static WEP Security On A Client

If you configured the 9160 Wireless Gateway to use Static WEP security mode . . .

Modify security settings that apply to the Internal Network

Broadcast SSID ☒ Allow ☐ Prohibit
Station Isolation ☒ Off ☐ On

Security Mode Static WEP

Transfer Key Index 1
Key Length ☐ 64 bits ☒ 128 bits
Key Type ☐ ASCII ☒ Hex
Characters Required 26
WEP Keys 1: 01234567890012345678900123
2: 01234567890012345678900123
3:
4:
Authentication Algorithms Shared Key

. . . then configure WEP security on each client as follows.

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open
Data encryption: WEP
Network key:
Confirm network key:
Key index (advanced): 1
☐ The key is provided for me automatically
☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Choose **Open** or **Shared**
Choose **WEP** as the Data Encryption mode
Enter a **network key** that matches the WEP key on the access point in the position set to the transfer key index (and re-type to confirm)
Optionally set a different transfer **key index** to send data from client back to access point
Disable auto key option

OK Cancel

Appendix C: Configuring Security Settings On Wireless Clients

Configuring Static WEP Security On A Client

Network Authentication	Open or Shared, depending on how you configured this option on the access point. Note: When the Authentication Algorithm on the access point is set to Both, clients set to either Shared or Open can associate with the AP. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the AP. Clients configured to use WEP as an Open system can associate with the AP even without a valid WEP key (but a valid key will be required to actually view and exchange data). For more information, see Online Help on the access point.
Data Encryption	WEP
Network Key	Provide the WEP key you entered on the access point <i>Security settings</i> in the Transfer Key Index position. For example, if the Transfer Key Index on the access point is set to 1, then for the client Network Key specify the WEP Key you entered as WEP Key 1 on the access point.
Key Index	Set key index to indicate which of the WEP keys specified on the access point <i>Security</i> page will be used to transfer data from the client back to the access point. For example, you can set this to 1, 2, 3, or 4 if you have all four WEP keys configured on the access point.
The key is provided for me automatically	Disable this option (click to uncheck the box).

Table C.2 Association Settings

Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is disabled (box should be unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)
--	---

Table C.3 Authentication Settings

Click **OK** on the *Wireless Network Properties* dialog to close it and save your changes.

Connecting To The Wireless Network With A Static WEP Client

Static WEP clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a WEP key. The WEP key configured on the client security settings is automatically used when you connect.

C.6 Configuring IEEE 802.1x Security On A Client

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

C.6.1 IEEE 802.1x Client Using EAP/PEAP

The Built-In Authentication Server on the 9160 Wireless Gateway uses *Protected Extensible Authentication Protocol* (EAP) referred to here as “EAP/PEAP”.

- If you are using the Built-in Authentication server with “IEEE 802.1x” security mode on the 9160 Wireless Gateway, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to:

(1) Add the 9160 Wireless Gateway to the list of RADIUS server clients.

AND

(2) Configure your IEEE 802.1x wireless clients to use PEAP.



Note: *The following example assumes that you are using the Built-in Authentication server that comes with the 9160 Wireless Gateway. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example, especially with regard to certificate validation.*

Appendix C: Configuring Security Settings On Wireless Clients

IEEE 802.1x Client Using EAP/PEAP

If you configured the 9160 Wireless Gateway to use IEEE 802.1x security mode . . .

Modify security settings that apply to the Internal Network

Broadcast SSID

☒ Allow ☐ Prohibit

Station Isolation

☒ Off ☐ On

Security Mode

IEEE 802.1x

Authentication Server

Built-in

Radius IP

10 . 10 . 1 . 9

Radius Key

XXXXXXXXXX

☒ Enable radius accounting

. . . then configure IEEE 802.1x security with PEAP authentication on each client as follows:

Choose **Open**

Choose **WEP**
Data Encryption mode

Enable (click to check) IEEE 8021x authentication

Choose **Protected EAP (PEAP)**

... then, click **Properties**

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

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

1

OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

Properties

☐ Authenticate as computer when computer information is available

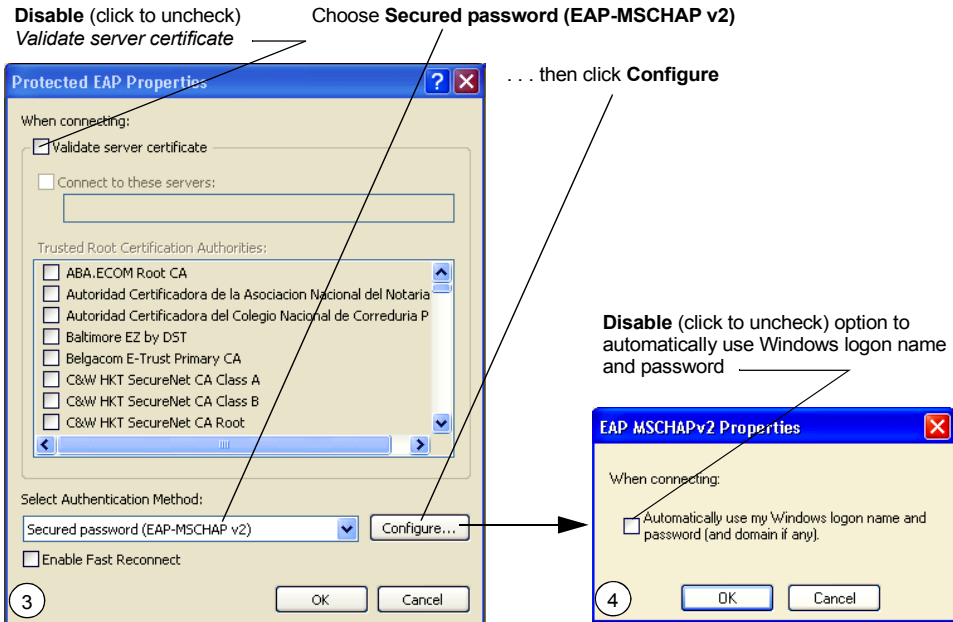
☐ Authenticate as guest when user or computer information is unavailable

2

OK Cancel

C-12 Psion Teklogix 9160 Wireless Gateway User Manual

Appendix C: Configuring Security Settings On Wireless Clients IEEE 802.1x Client Using EAP/PEAP



1. Configure the following settings on the *Association* tab on the *Network Properties* dialog.

<i>Network Authentication</i>	Open
<i>Data Encryption</i>	WEP Note: An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
<i>This key is provided for me automatically</i>	Enable (click to check) this option.

Table C.4 Association Settings

2. Configure this setting on the *Authentication* tab.

<i>EAP Type</i>	Choose Protected EAP (PEAP) .
-----------------	--------------------------------------

Table C.5 Authentication Settings

3. Click **Properties** to bring up the *Protected EAP Properties* dialog and configure the following settings.

<i>Validate Server Certificate</i>	Disable this option (click to uncheck the box). Note: <i>This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.</i>
<i>Select Authentication Method</i>	Choose Secured password (EAP-MSCHAP v2) .

Table C.6 Protected EAP Properties Settings

4. Click **Configure** to bring up the *EAP MSCHAP v2 Properties* dialog. On this dialog, **disable** (click to uncheck) the option to *Automatically use my Windows login name . . . etc.*
- Click **OK** on all dialogs (starting with the *EAP MSCHAP v2 Properties* dialog) to close and save your changes.

Logging On To The Wireless Network With An IEEE 802.1x PEAP Client

IEEE 802.1x PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

C.6.2 IEEE 802.1x Client Using EAP/TLS Certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA/WPA2 Enterprise (RADIUS) and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.



Note: *If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.*

Some good starting points available on the Web for the Microsoft Windows PKI software are:

“How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;231881> , and

“How to Configure a Certificate Server” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

To use this type of security, you must do the following:

1. Add the 9160 Wireless Gateway to the list of RADIUS server clients. (See “Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway” on page C-30.)
2. Configure the 9160 Wireless Gateway to use your RADIUS server (by providing the RADIUS server IP address as part of the “IEEE 802.1x” security mode settings).
3. Configure wireless clients to use IEEE 802.1x security and “Smart Card or other Certificate” as described in this section.
4. Obtain a certificate for this client as described in “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Appendix C: Configuring Security Settings On Wireless Clients

IEEE 802.1x Client Using EAP/TLS Certificate

If you configured the 9160 Wireless Gateway to use IEEE 802.1x security mode with an external RADIUS server . . .

Modify security settings that apply to the Internal Network

Broadcast SSID

☒ Allow ☐ Prohibit

Station Isolation

☒ Off ☐ On

Security Mode

IEEE 802.1x

Authentication Server

External

Radius IP

10 . 10 . 1 . 9

Radius Key

☒ Enable radius accounting

. . . then configure IEEE 802.1x security with certificate authentication on each client as follows:

Choose **Open**

Choose **WEP**
Data Encryption mode

Enable (click to check) IEEE 8021x authentication

Choose **Smart Card/Certificate**

... then, click **Properties**

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

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

1 OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

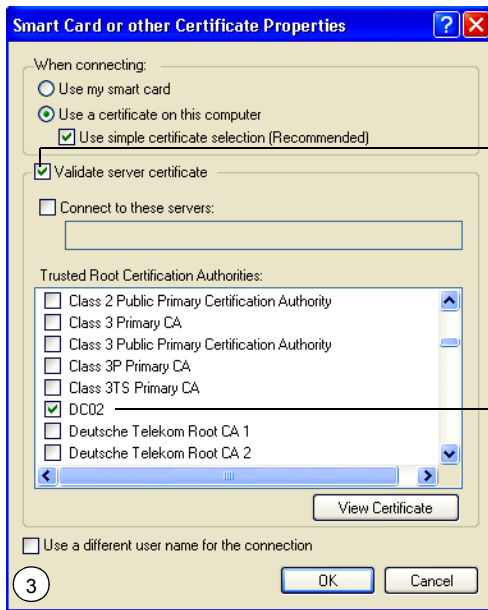
Properties

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel

Appendix C: Configuring Security Settings On Wireless Clients IEEE 802.1x Client Using EAP/TLS Certificate



Enable (click to check)
Validate server certificate

Select (check) the name of certificate
on this client (downloaded from
RADIUS server in a prerequisite procedure)

1. Configure the following settings on the *Association* tab on the *Network Properties* dialog.

<i>Network Authentication</i>	Open
<i>Data Encryption</i>	WEP Note: An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
<i>This key is provided for me automatically</i>	Enable (click to check) this option.

Table C.7 Association Settings

2. Configure these settings on the *Authentication* tab.

<i>Enable IEEE 802.1x authentication for this network</i>	Enable (click to check) this option.
<i>EAP Type</i>	Choose Smart Card or other Certificate .

Table C.8 Authentication Settings

3. Click **Properties** to bring up the *Smart Card or other Certificate Properties* dialog and enable the **Validate server certificate** option.

Validate Server Certificate	Enable this option (click to check the box).
Certificates	In the certificate list shown, select the certificate for this client.

Table C.9 Smart Card Or Other Certificate Properties Settings

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Connecting To The Wireless Network With An IEEE 802.1x Client Using A Certificate

IEEE 802.1x clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for logon information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

C.7 Configuring WPA/WPA2 Enterprise (RADIUS) Security On A Client

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS) is an implementation of the Wi-Fi Alliance IEEE **802.11i** 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.

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

When you configure WPA/WPA2 Enterprise (RADIUS) security mode on the access point, you have a choice of whether to use the Built-in Authentication Server or an external RADIUS server that you provide.

The 9160 Wireless Gateway Built-in Authentication Server supports *Protected Extensible Authentication Protocol* (EAP) known as “EAP/PEAP” and *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAP V2), which provides authentication for point-to-point (PPP) connections between a Windows-based computer and network devices such as access points.

So, if you configure the network (access point) to use security mode and choose the Built-in Authentication server, you must configure client stations to use WPA/WPA2 Enterprise (RADIUS) and EAP/PEAP.

If you configure the network (access point) to use this security mode with an external RADIUS server, you must configure the client stations to use WPA/WPA2 Enterprise (RADIUS) and whichever security protocol your RADIUS server is configured to use.

C.7.1 WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP

The Built-In Authentication Server on the 9160 Wireless Gateway uses *Protected Extensible Authentication Protocol* (EAP) known as “EAP/PEAP”.

- If you are using the Built-in Authentication server with “WPA/WPA2 Enterprise (RADIUS)” security mode on the 9160 Wireless Gateway, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to:

(1) Add the 9160 Wireless Gateway to the list of RADIUS server clients.

AND

(2) Configure your “WPA/WPA2 Enterprise (RADIUS)” wireless clients to use PEAP.



Note: *The following example assumes you are using the Built-in Authentication server that comes with the 9160 Wireless Gateway. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.*

Appendix C: Configuring Security Settings On Wireless Clients

WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP

If you configured the 9160 Wireless Gateway to use WPA/WPA2 Enterprise (RADIUS) security mode and to use either the Built-in Authentication Server or an external RADIUS server that uses EAP/PEAP . . .

Modify security settings that apply to the Internal Network

Broadcast SSID

☒ Allow ☐ Prohibit

Station Isolation

☒ Off ☐ On

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

XXXXXXXXXX

☐ Enable radius accounting

☐ Allow non-WPA IEEE 802.1x clients

Appendix C: Configuring Security Settings On Wireless Clients WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP

First set up user accounts on the access point (*Cluster, User Management*). . . .

SELECTED	EDIT	USER NAME	REAL NAME	STATUS
☐	[Edit]	samantha	samantha stevens	enabled
☐	[Edit]	darren	darren stevens	enabled

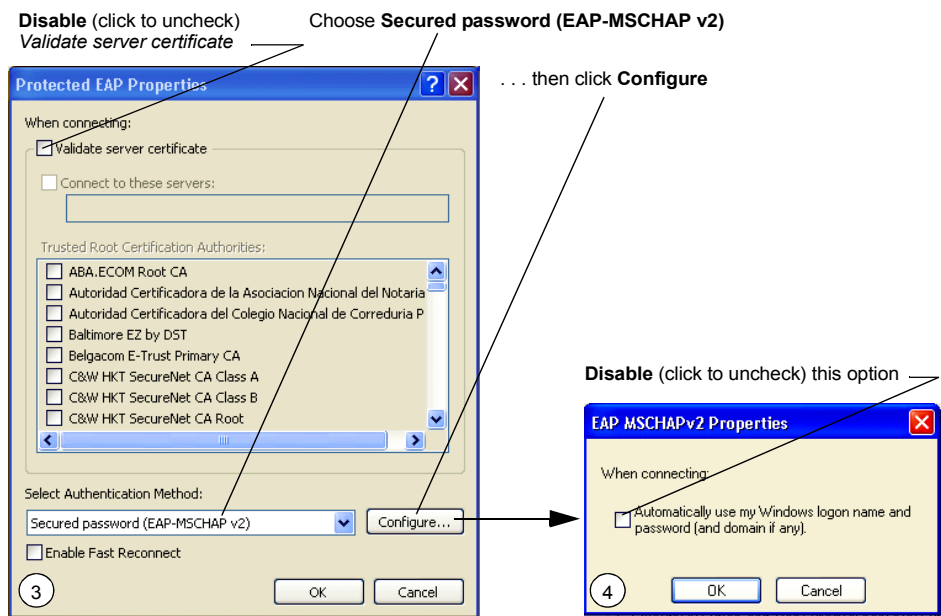
. . . then configure WPA security with PEAP authentication on each client as follows.

Choose **WPA** Choose either **TKIP** or **AES** for the Data Encryption mode Choose **Protected EAP (PEAP)** . . . then, click **Properties**

1 **2**

Appendix C: Configuring Security Settings On Wireless Clients

WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP



1. Configure the following settings on the *Association* and *Authentication* tabs on the *Network Properties* dialog.

<i>Network Authentication</i>	WPA
<i>Data Encryption</i>	TKIP or AES depending on how this option is configured on the access point. Note: When the Cipher Suite on the access point is set to “Both”, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Online Help on the access point.

Table C.10 Association Settings

2. Configure this setting on the *Authentication* tab.

<i>EAP Type</i>	Choose Protected EAP (PEAP)
-----------------	------------------------------------

Table C.11 Authentication Settings

- Click **Properties** to bring up the *Protected EAP Properties* dialog and configure the following settings.

<i>Validate Server Certificate</i>	Disable this option (click to uncheck the box). Note: <i>This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.</i>
<i>Select Authentication Method</i>	Choose Secured password (EAP-MSCHAP v2) .

Table C.12 Protected EAP Properties Settings

- Click **Configure** to bring up the *EAP MSCHAP v2 Properties* dialog.
On this dialog, **disable** (click to uncheck) the option to *Automatically use my Windows logon name . . . etc.* so that upon logon you will be prompted for user name and password.
Click **OK** on all dialogs (starting with the *EAP MSCHAP v2 Properties* dialog) to close and save your changes.

Logging On To The Wireless Network With A WPA/WPA2 Enterprise (RADIUS) PEAP Client

“WPA/WPA2 Enterprise (RADIUS)” PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

C.7.2 WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate

Extensible Authentication Protocol (EAP) *Transport Layer Security* (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA/WPA2 Enterprise (RADIUS) and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.



Note: *If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), includ-*

WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate

ing a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are:

“How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;231881>, and

How to “Configure a Certificate Server” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

To use this type of security, you must do the following:

1. Add the 9160 Wireless Gateway to the list of RADIUS server clients. (See “Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway” on page C-30.)
2. Configure the 9160 Wireless Gateway to use your RADIUS server (by providing the RADIUS server IP address as part of the “WPA/WPA2 Enterprise [RADIUS]” security mode settings).
3. Configure wireless clients to use WPA security and “Smart Card or other Certificate” as described in this section.
4. Obtain a certificate for this client as described in “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Appendix C: Configuring Security Settings On Wireless Clients WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate

If you configured the 9160 Wireless Gateway to use WPA/WPA2 Enterprise (RADIUS) security mode with an external RADIUS server . . .

Modify security settings that apply to the Internal Network

Broadcast SSID ☒ Allow ☐ Prohibit
Station Isolation ☒ Off ☐ On

Security Mode WPA/WPA2 Enterprise (RADIUS) ▼

Supported Client Stations Both ▼
☒ Enable pre-authentication

Cipher Suites TKIP ▼

Authentication Server External ▼

Radius IP 10 . 0 . 1 . 9

Radius Key XXXXXXXXXX

☒ Enable radius accounting
☐ Allow non-WPA IEEE 802.1x clients

. . . then configure WPA security with certificate authentication on each client as follows.

Choose **WPA** Choose either **TKIP** or **AES** for the Data Encryption mode Choose **Smart Card** or other **Certificate** and enable **Authenticate as computer** then, click **Properties**

1

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA ▼

Data encryption: TKIP ▼

Network key:

Confirm network key:

Key index (advanced): 1 ▼

☒ The key is provided for me automatically

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

OK Cancel

2

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network.

EAP type: Smart Card or other Certificate ▼

☒ Authenticate as computer when computer information is available

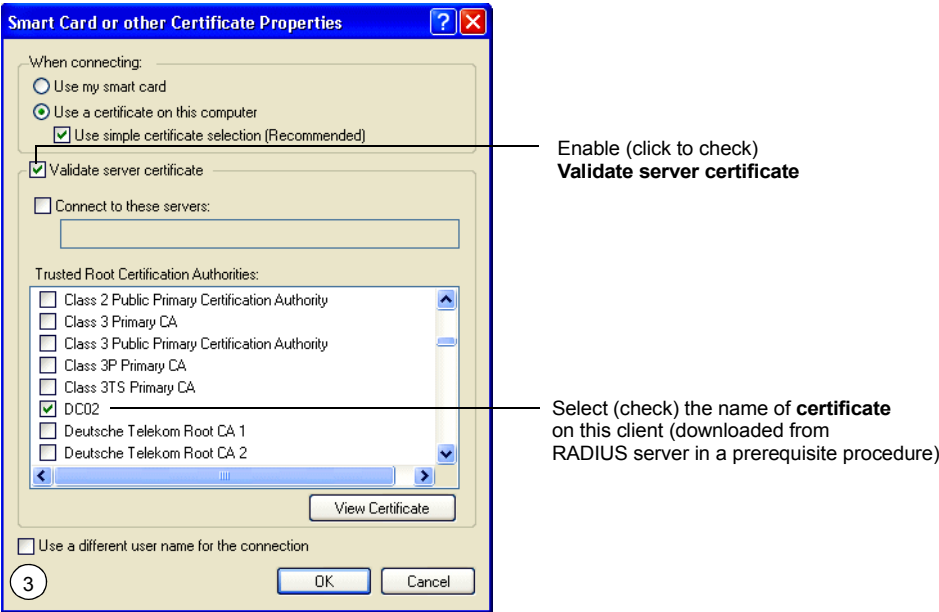
☐ Authenticate as guest when user or computer information is unavailable

Properties

OK Cancel

Appendix C: Configuring Security Settings On Wireless Clients

WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate



1. Configure the following settings on the *Association* tab on the *Network Properties* dialog.

<i>Network Authentication</i>	WPA
<i>Data Encryption</i>	TKIP or AES depending on how this option is configured on the access point. Note: When the Cipher Suite on the access point is set to "Both", then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Online Help on the access point.

Table C.13 Association Settings

2. Configure these settings on the *Authentication* tab.

<i>Enable IEEE 802.1x authentication for this network</i>	Enable (click to check) this option.
<i>EAP Type</i>	Choose Smart Card or other Certificate .

Table C.14 Authentication Settings

3. Click **Properties** to bring up the *Smart Card or other Certificate Properties* dialog and enable the **Validate server certificate** option.

Validate Server Certificate	Enable this option (click to check the box).
Certificates	In the certificate list shown, select the certificate for this client.

Table C.15 Smart Card Or Other Certificate Properties Settings

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining A TLS-EAP Certificate For A Client” on page C-34.

Logging On To The Wireless Network With A WPA Client Using A Certificate

WPA clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for logon information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

C.8 Configuring WPA/WPA2 Personal (PSK) Security On A Client

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Advanced Encryption Algorithm* (AES), and *Counter mode/CBC-MAC Protocol* (CCMP) mechanisms. PSK employs a pre-shared key for an initial check of client credentials.

Appendix C: Configuring Security Settings On Wireless Clients

Configuring WPA/WPA2 Personal (PSK) Security On A Client

If you configured the 9160 Wireless Gateway to use WPA/WPA2 Personal (PSK) security mode . . .

Modify security settings that apply to the Internal Network

Broadcast SSID

☒ Allow ☐ Prohibit

Station Isolation

☒ Off ☐ On

Security Mode

WPA/WPA2 Personal (PSK)

Supported Client Stations

WPA

Cipher Suites

TKIP

Key

012345678

. . . then configure WPA/WPA2 Personal (PSK) security on each client as follows.

Wireless network properties

Association

Authentication

Network name (SSID):

My AP

Wireless network key

This network requires a key for the following:

Network Authentication:

WPA-PSK

Data encryption:

TKIP

Network key:

.....

Confirm network key:

.....

Key index (advanced):

1

☐ The key is provided for me automatically

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

OK

Cancel

Choose **WPA-PSK**

Choose either **TKIP** or **AES** for the Data Encryption mode

Enter a **network key** that matches the one specified on the access point (and confirm by re-typing).

Appendix C: Configuring Security Settings On Wireless Clients

Configuring WPA/WPA2 Personal (PSK) Security On A Client

<i>Network Authentication</i>	WPA-PSK
<i>Data Encryption</i>	TKIP or AES depending on how this option is configured on the access point. Note: When the Cipher Suite on the access point is set to "Both", then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Online Help on the access point.
<i>Network Key</i>	Provide the key you entered on the access point Security settings for the cipher suite you are using. For example, if the key on the access point is set to use a TKIP key of "012345678", then a TKIP client specify this same string as the network key.
<i>The key is provided for me automatically</i>	This box should be disabled automatically based on other settings.

Table C.16 Association Settings

<i>Enable IEEE 802.1x authentication for this network</i>	Make sure that IEEE 802.1x authentication is disabled (unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)
---	--

Table C.17 Authentication Settings

Click **OK** on the Wireless Network Properties dialog to close it and save your changes.

Connecting To The Wireless Network With A WPA-PSK Client

WPA-PSK clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a key. The TKIP or AES key you configured on the client security settings is automatically used when you connect.

C.9 Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway

An external *Remote Authentication Dial-in User Server* (RADIUS) running on the network can support EAP-TLS smart card/certificate distribution to clients in a *Public Key Infrastructure* (PKI), as well as EAP-PEAP user account setup and authentication. By *external* RADIUS server, we mean an authentication server external to the access point itself. This is to distinguish between the scenario in which you use a network RADIUS server versus one in which you use the *Built-in Authentication Server* on the 9160 Wireless Gateway.

This section provides an example of configuring an external RADIUS server for the purposes of authenticating and authorizing TLS-EAP certificates from wireless clients of a particular 9160 Wireless Gateway configured for either “WPA/WPA2 Enterprise (RADIUS)” or “IEEE 802.1x” security modes. The intention of this section is to provide some idea of what this process will look like; procedures will vary depending on the RADIUS server you use and how you configure it. For this example, we use the Internet Authentication Service that comes with Microsoft Windows 2003 server.



Note: *This document does not describe how to set up Administrative users on the RADIUS server. In this example, we assume you already have RADIUS server user accounts configured. You will need a RADIUS server user name and password for both this procedure and the following one that describes how to obtain and install a certificate on the wireless client. Please consult the documentation for your RADIUS server for information on setting up user accounts.*

The purpose of this procedure is to identify your 9160 Wireless Gateway as a “client” to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the AP. This procedure is required *per access point*. If you have more than one access point with which you plan to use an external RADIUS server, you need to follow these steps for each of those APs.

Keep in mind that the information you need to provide to the RADIUS server about the access point corresponds to settings on the access point (*Advanced, Security*) and vice versa. You should have already provided the RADIUS server IP Address to the AP; in the steps that follow you will provide the access point IP address to the RADIUS server. The RADIUS Key provided on the AP is the “shared secret” you will provide to the RADIUS server.

Appendix C: Configuring Security Settings On Wireless Clients
Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway

Modify security settings that apply to the Internal Network

Broadcast SSID

☒ Allow ☐ Prohibit

Station Isolation

☒ Off ☐ On

Security Mode

IEEE 802.1x

Authentication Server

External

Radius IP

10.10.1.9

Radius Key

☒ Enable radius accounting

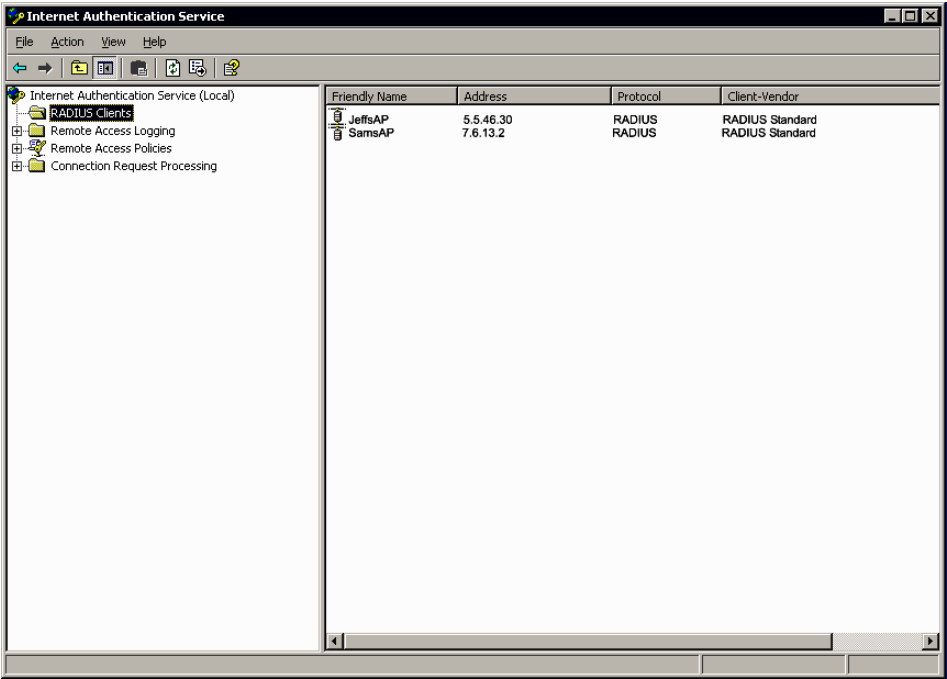


Note: The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the 9160 Wireless Gateway, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The 9160 Wireless Gateway is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

Appendix C: Configuring Security Settings On Wireless Clients

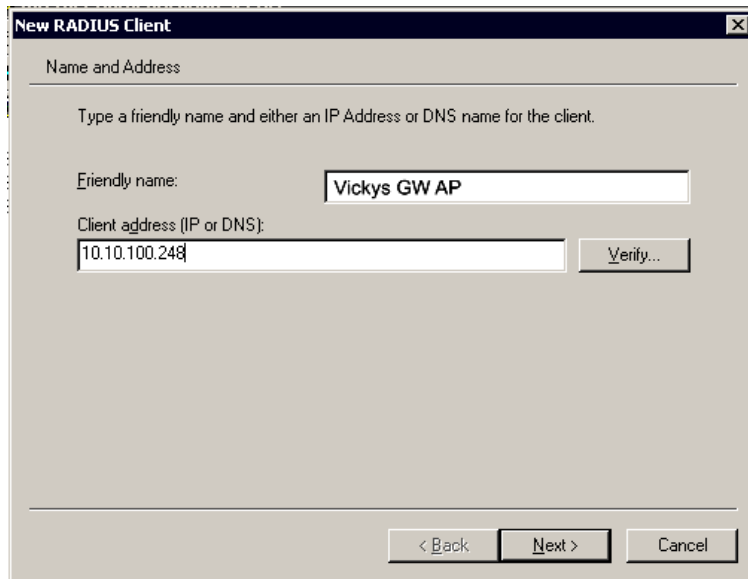
Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway

1. Log on to the system hosting your RADIUS server and bring up the Internet Authentication Service.



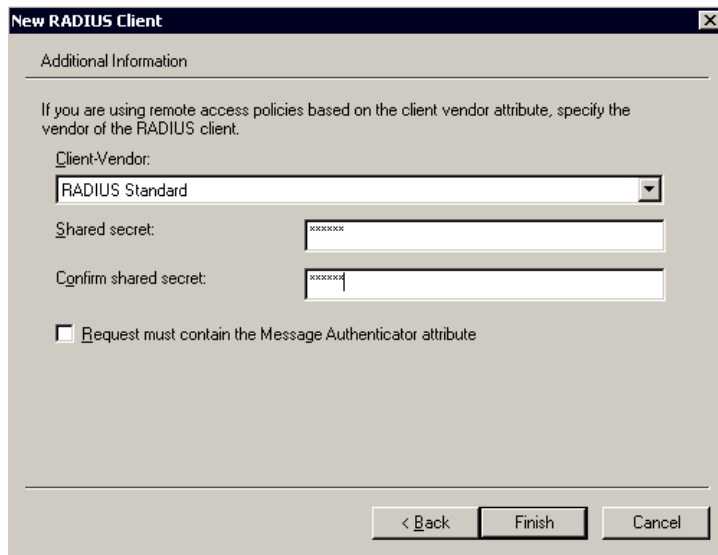
2. In the left panel, right click on **RADIUS Clients** node and choose **New, Radius Client** from the popup menu.
3. On the first screen of the *New RADIUS Client* wizard, provide information about the 9160 Wireless Gateway to which you want your clients to connect:
 - A logical (friendly) name for the access point. (You might want to use DNS name or location.)
 - IP address for the access point. Click **Next**.

Appendix C: Configuring Security Settings On Wireless Clients
Configuring An External RADIUS Server To Recognize The 9160 Wireless Gateway



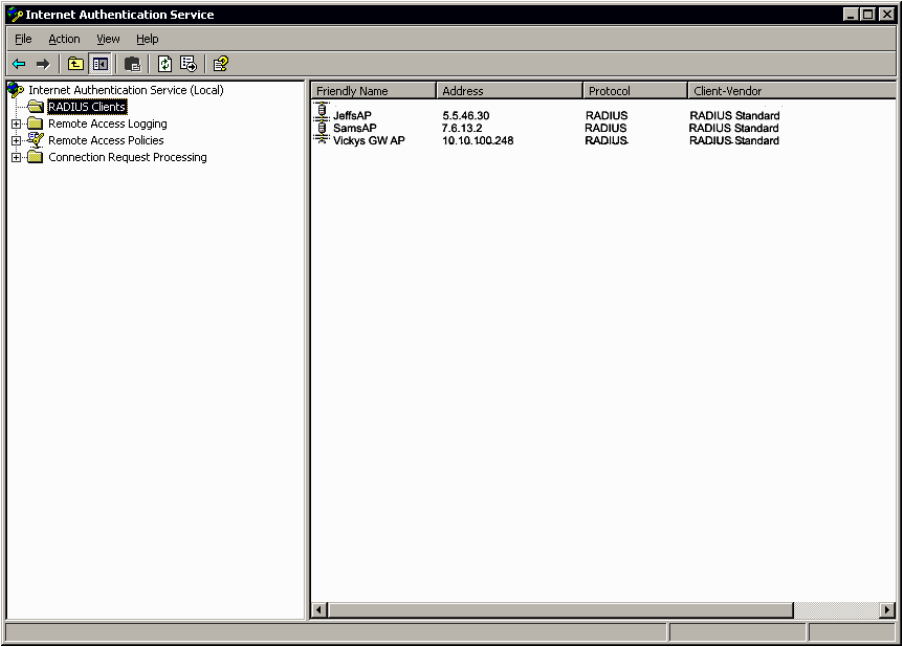
The dialog box is titled "New RADIUS Client" and has a close button (X) in the top right corner. The "Name and Address" tab is selected. The instructions state: "Type a friendly name and either an IP Address or DNS name for the client." There are two input fields: "Friendly name:" with the text "Vickys GW AP" and "Client address (IP or DNS):" with the text "10.10.100.248". A "Verify..." button is located to the right of the client address field. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

4. For the *Shared secret* enter the **RADIUS Key** you provided to the access point (on the *Advanced, Security* page). Re-type the key to confirm.



The dialog box is titled "New RADIUS Client" and has a close button (X) in the top right corner. The "Additional Information" tab is selected. The instructions state: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." There is a "Client-Vendor:" dropdown menu with "RADIUS Standard" selected. Below this are two input fields for "Shared secret:" and "Confirm shared secret:", both containing "xxxxxx". There is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

5. Click **Finish**. The access point is now displayed as a client of the Authentication Server.



C.10 Obtaining A TLS-EAP Certificate For A Client



Note: If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA) server, configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are:

“How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> , and

“How to Configure a Certificate Server” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

Wireless clients configured to use either “WPA/WPA2 Enterprise (RADIUS)” or “IEEE 802.1x” security modes with an external RADIUS server that supports TLS-EAP certificates must obtain a TLS certificate from the RADIUS server.

This is an initial one-time step that must be completed on each client that uses either of these modes with certificates. In this procedure, we use the Microsoft Certificate Server as an example.

To obtain a certificate for a client, follow these steps.

1. Go to the following URL in a Web browser:

<https://IPAddressOfServer/certsrv/>

Where *IPAddressOfServer* is the IP address of your external RADIUS server, or of the *Certificate Authority (CA)*, depending on the configuration of your infrastructure.

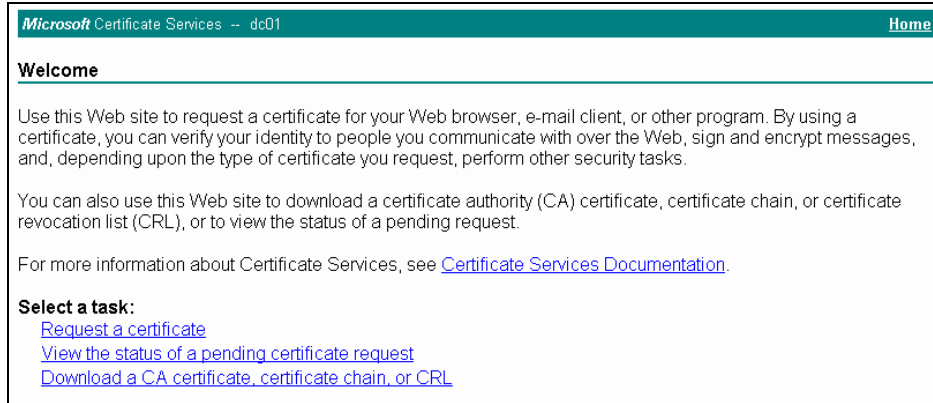
2. Click **Yes** to proceed to the secure Web page for the server.



Appendix C: Configuring Security Settings On Wireless Clients

Obtaining A TLS-EAP Certificate For A Client

The Welcome screen for the Certificate Server is displayed in the browser.



The screenshot shows a web browser window titled "Microsoft Certificate Services -- dc01" with a "Home" link in the top right. The main heading is "Welcome". The text explains that the site is used to request a certificate for a web browser, email client, or other program, and that it can also be used to download a CA certificate, certificate chain, or CRL. It provides a link to "Certificate Services Documentation". Under the "Select a task:" section, there are three links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

3. Click **Request a certificate** to get the login prompt for the RADIUS server.
4. Provide a valid **user name** and **password** to access the RADIUS server.



The screenshot shows a Windows-style dialog box titled "Connect to 10.10.1.9". It features a key icon and a status bar at the bottom with "OK" and "Cancel" buttons. The main area contains the text "Connecting to 10.10.1.9". Below this, there is a "User name:" label followed by a text box containing "larry" and a dropdown arrow. To the right of the text box is a small icon of a person. Below the user name field is a "Password:" label followed by a text box filled with dots. To the right of the password field is a small icon of a key. Below the password field is a checkbox labeled "Remember my password".



Note: The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Please consult the documentation for your RADIUS server for these procedures.

5. Click **User Certificate** on the next page displayed.

Microsoft Certificate Services -- dc01 Home

Request a Certificate

Select the certificate type:
[User Certificate](#)

Or, submit an [advanced certificate request](#).

6. Click **Yes** on the dialog displayed to install the certificate.

Microsoft Certificate Services -- dc01 Home

User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit.
[More Options >>](#)

Security Warning

Do you want to install and run "Microsoft Certificate Enrollment Control" signed on 5/14/2001 2:35 PM and distributed by:

[Microsoft Corporation](#)

Publisher authenticity verified by Microsoft Code Signing PCA

Caution: Microsoft Corporation asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation to make that assertion.

☐ Always trust content from Microsoft Corporation

Yes No More Info

7. Click **Submit** to complete and click **Yes** to confirm the submittal on the popup dialog.

Microsoft Certificate Services -- dc01 Home

User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit.
[More Options >>](#)

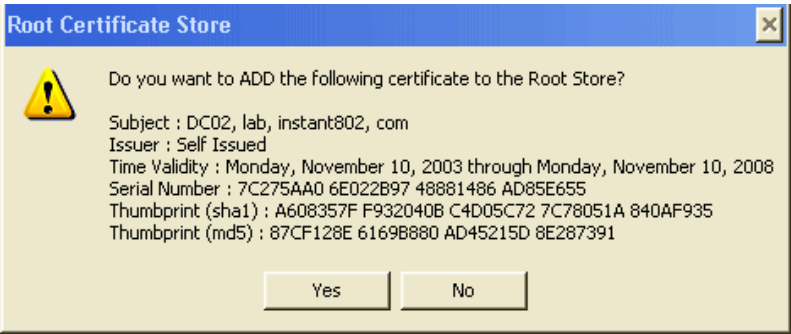
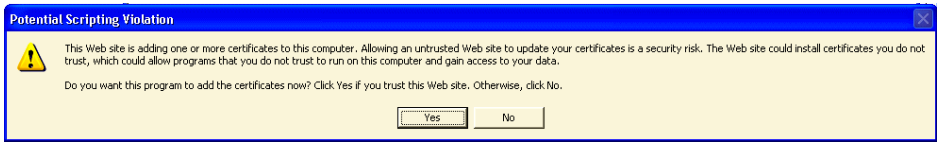
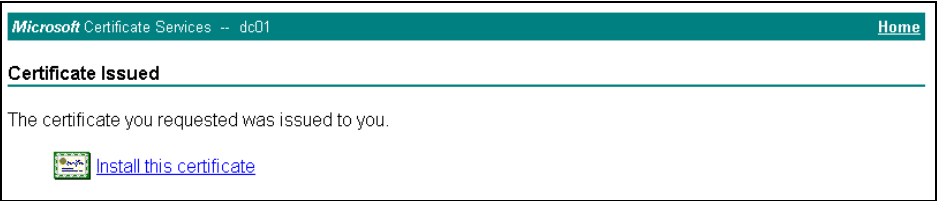
Potential Scripting Violation

 This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

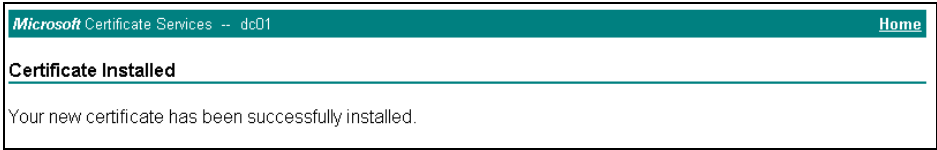
Appendix C: Configuring Security Settings On Wireless Clients

Obtaining A TLS-EAP Certificate For A Client

8. Click **Install this certificate** to install the newly issued certificate on your client station. (Also, click **Yes** on the popup windows to confirm the install and to add the certificate to the Root Store.)



A success message is displayed indicating the certificate is now installed on the client.



APPENDIX **D**

TROUBLESHOOTING

D.1 Wireless Distribution System (WDS) Problems And Solutions	D-3
D.2 Cluster Recovery	D-4
D.2.1 Reboot Or Reset Access Point	D-4
D.2.2 Stop Clustering And Reset Each Access Point In The Cluster . .	D-5

This section provides information about how to solve common problems you might encounter in the course of updating network configurations on networks served by multiple, clustered access points.

D.1 Wireless Distribution System (WDS) Problems And Solutions

If you are having trouble configuring a WDS link, be sure you have read the notes and cautions in “Configuring WDS Settings” on page 190. These notes are reprinted here for your convenience. The most common problem Administrators encounter with WDS setups is forgetting to set both access points in the link to the same radio channel and IEEE 802.11 mode. That prerequisite, as well as others, is listed in the notes below.



Notes:

- *The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, we recommend using WDS to bridge the Guest network only for this release. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.*
- *When using WDS, be sure to configure WDS settings on both access points participating in the WDS link.*
- *You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.*
- *Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See “Configuring Radio Settings” on page 157 for information on configuring the Radio mode and channel.)*
- ***Do not create loops*** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. Spanning Tree Protocol (STP), which manages path redundancy and prevents unwanted loops, is not enabled for this release. Keep the following rules in mind when working with WDS on this release of the 9160 Wireless Gateway:

Cluster Recovery

Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both. Do not create “backup” links.

If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.

You can only extend or bridge either the Internal or Guest network but not both.

D.2 Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

D.2.1 Reboot Or Reset Access Point

These recovery methods are given in the order you should try them. In all but the last case (stop clustering), you only need to reset or reboot the particular access point whose configuration is out of sync with other cluster members or cannot remove/join the cluster.

- Physically reboot the access point by cycling the power (pressing the Power button Off, then On).
- Reset the access point from its Administration UI. To do this, go to *<http://IPAddressOfAccessPoint>*, navigate to **Advanced, Reset Configuration**, and click the **Reset** button. (IP addresses for APs are on the *Cluster, Access Points* page for any cluster member.)
- In some extreme cases, reboot or reset may not solve the problem. In these cases, follow the procedure described next in “Stop Clustering And Reset Each Access Point In The Cluster” on page D-5 to recover every access point on the subnet.

D.2.2 Stop Clustering And Reset Each Access Point In The Cluster

If the previous reboot or reset methods do not solve the problem, do the following to stop clustering and reset all APs.

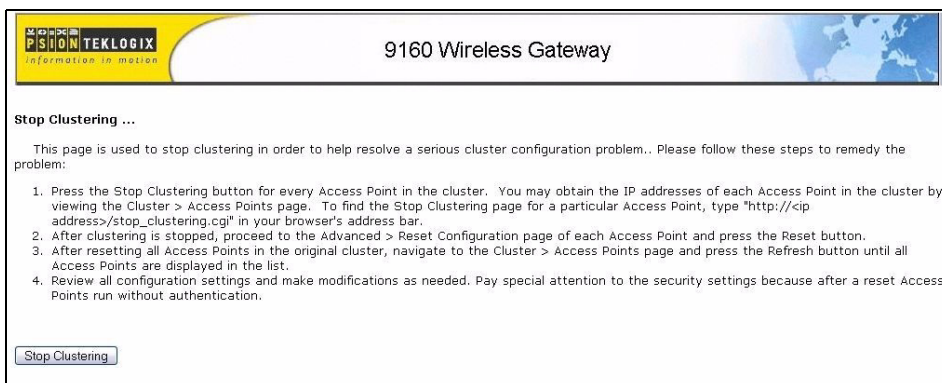
1. Stop clustering on each access point in the cluster.

To do this, enter the **Stop Clustering URL** in the address bar of your Web browser as follows:

http://IPAddressOfAccessPoint/stop_clustering.cgi

Where *IPAddressOfAccessPoint* is the IP address of the access point you want to stop clustering. You can find the IP addresses for the cluster members on the Cluster, Access Points page for any of the clustered access points. We recommend making a note of all IP addresses at this point.

The *Stop Clustering* page for this access point is displayed.



Click the **Stop Clustering** button.

Repeat this “stop clustering” step for every access point in the cluster.



Important: *Do not proceed to the next step of resetting any access points until you have stopped clustering on all of them. Make sure that you first “Stop Clustering” on every access point on the subnet, and only then perform the next part of the process of resetting each one to the factory defaults.*

Appendix D: Troubleshooting

Stop Clustering And Reset Each Access Point In The Cluster

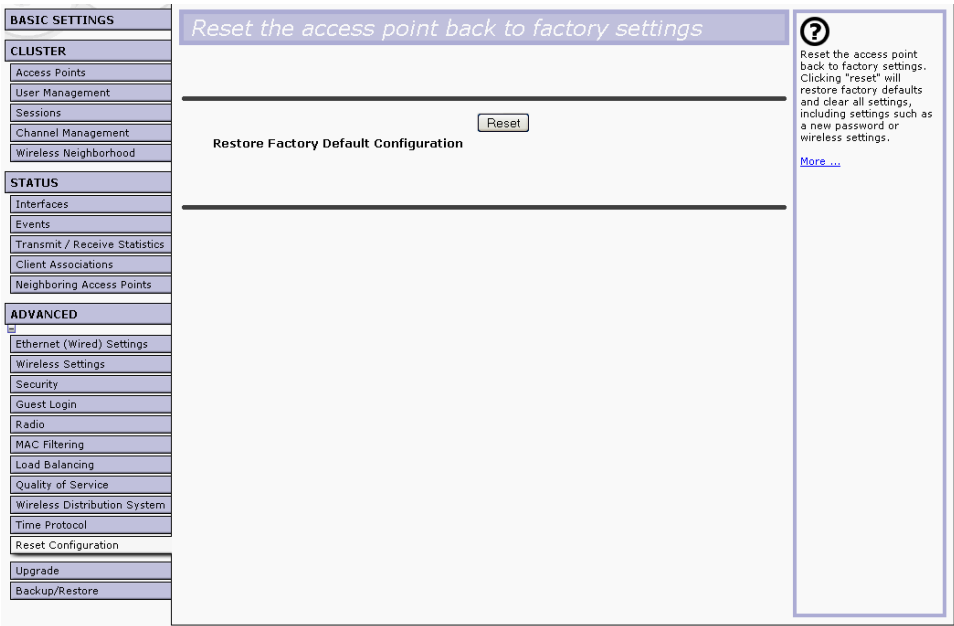
2. Reset each access point.

To do this, go to the Administration Web pages of the access point you want to reset by entering its URL into the address bar of your Web browser:

http://IPAddressOfAccessPoint/

Where *IPAddressOfAccessPoint* is the IP address of the access point you want to reset.

On the *Administration UI left-hand* tabs, click **Advanced**, **Reset Configuration** to bring up the *Reset* page.



Click **Reset** to restore the factory defaults on the access point. (This will clear all of your previous settings, including updated passwords.)

Repeat this “reset” step for every access point in the cluster.



Important: *Do not proceed to the next step until you have stopped clustering on all of access points in the pre-existing cluster.*

3. Refresh the cluster view as follows.

On the *Administration Web* pages for any one of the access points, click **Cluster, Access Points** to bring up the *Access Points cluster management* page and click the **Refresh** button.

At this point you should see all previous cluster members displayed in the list. Before proceeding to the last step, verify that the cluster has reformed by making sure all access points are listed.

Manage access points in the cluster

Access Points...

Status: connected to cluster.

the list of Access Points.

☐	LOCATION	MAC ADDRESS	IP ADDRESS
☐	not set	00:0a:01:98:9b:2c	10.10.5.213
☒	not set	00:0a:01:98:9b:3b	10.10.5.235

the selected Access Points from the cluster.

Clustered

2 Access Points

0 User Accounts

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 ...](#)

Review all configuration settings and make modifications as needed.

Pay special attention to the security settings because after a reset, access points run without any security in place.

GLOSSARY

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0-9**802**

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a **LAN**. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of **LAN**.

Included in the 802 family of **IEEE** standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing **EAP** packets over an **802.11** wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the **LLC** layer for the **802** family of standards.

802.3

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the **MAC** layer for networks that use **CSMA/CA**. **Ethernet** is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (**MAC**) and physical layer (**PHY**) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by **802.11b**.

IEEE 802.11 is also used generically to refer to the family of **IEEE** standards for wireless local area networks.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) is a **PHY** standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.

802.11a Turbo

IEEE 802.11a Turbo is a proprietary variant of the **802.11a** standard from Atheros Communications. It supports accelerated data rates ranging from 6 to 108Mbps. Atheros Turbo 5 GHz is IEEE 802.11a Turbo mode. Atheros Turbo 2.4 GHz is IEEE 802.11g Turbo mode.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial **802.11 PHY** to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11d

IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. PHY requirements such as provides frequency hopping tables, acceptable channels, and power levels for each country are provided. Enabling support for IEEE 802.11d on the access point causes the AP to broadcast which country it is operating in as a part of its beacons. Client stations then use this information. This is particularly important for AP operation in the 5GHz IEEE 802.11a bands because use of these frequencies varies a great deal from one country to another.

802.11e

IEEE 802.11e is a developing *IEEE* standard for *MAC* enhancements to support *QoS*. It provides a mechanism to prioritize traffic within **802.11**. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in μ sec) of a burst of data.

IEEE 802.11e is still a draft *IEEE* standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements (WMM)* standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (*IAPP*) for access points (wireless hubs) in an extended service set (*ESS*). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the **802.11b PHY**, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11i

IEEE 802.11i is a comprehensive *IEEE* standard for security in a wireless local area network (*WLAN*) that describes *Wi-Fi Protected Access 2 (WPA2)*. It defines

802.11k

enhancements to the **MAC** Layer to counter some of the weaknesses of **WEP**. It incorporates stronger encryption techniques than the original **Wi-Fi Protected Access (WPA)**, such as Advanced Encryption Standard (**AES**).

The original **WPA**, which can be considered a subset of 802.11i, uses *Temporal Key Integrity Protocol (TKIP)* for encryption. WPA2 is backwards-compatible with products that support the original WPA.

IEEE 802.11i / WPA2 was finalized and ratified in June of 2004.

802.11k

IEEE 802.11k is a developing **IEEE** standard for wireless networks (**WLANs**) that helps auto-manage network **Channel** selection, client **Roaming**, and **Access Point** (AP) utilization. 802.11k capable networks will automatically load balance network traffic across APs to improve network performance and prevent under or over-utilization of any one AP. 802.11k will eventually complement the **802.11e** quality of service (**QoS**) standard by ensuring QoS for multimedia over a wireless link.

802.1Q

IEEE 802.1Q is the **IEEE** standard for *Virtual Local Area Networks (VLANs)* specific to wireless technologies. (See <http://www.ieee802.org/1/pages/802.1Q.html>.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.1Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

A

Access Point

An *access point* is the communication hub for the devices on a **WLAN**, providing a connection or bridge between wireless and wired network devices. It supports a **Wireless Networking Framework** called **Infrastructure Mode**.

When one access point is connected to wired network and supports a set of wireless stations, it is referred to as a basic service set (**BSS**). An extended service set (**ESS**) is created by combining two or more BSSs.

Ad hoc Mode

Ad hoc mode is a **Wireless Networking Framework** in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (**IBSS**).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

B

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames provide the “heartbeat” of a **WLAN**, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion. It carries the following information (some of which is optional):

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.

Bridge

- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.
- The *Capability Information* lists requirements of stations that want to join the **WLAN**. For example, it indicates that all stations must use **WEP**.
- The *Service Set Identifier (SSID)*.
- The **Basic Rate Set** is a bitmap that lists the rates that the **WLAN** supports.
- The optional *Parameter Sets* indicates features of the specific signalling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map (TIM)* identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (**LANs**) using the same protocol, such as Ethernet or **IEEE 802.1x**.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form of **IEEE 802.1x Frames** to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also **Unicast** and **Multicast**.

Broadcast Address

See **IP Address**.

BSS

A *basic service set* (BSS) is an ***Infrastructure Mode Wireless Networking Framework*** with a single access point. Also see extended service set (***ESS***) and independent basic service set (***IBSS***).

BSSID

In ***Infrastructure Mode***, the *Basic Service Set Identifier* (BSSID) is the 48-bit ***MAC*** address of the wireless interface of the ***Access Point***.

C**CCMP**

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for ***802.11i*** that uses ***AES***. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an ***HTTP*** server. It specifies how to pass arguments to the executing program as part of the ***HTTP*** request. It may also define a set of environment variables.

A CGI program is a common way for an ***HTTP*** server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each ***802.11*** standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European

CSMA/CA

Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (**DCF**). See also **RTS** and **CTS**.

The CSMA/CA protocol used by **802.11** networks is a variation on CSMA/CD (used by **Ethernet** networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an **IEEE 802.11** client station in response to an *request to send* (**RTS**) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 **CSMA/CA** protocol. (See also **RTS**.)

D

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows. See also **EDCF**.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server “offers” a “lease” (for a pre-configured period of time—see ***Lease Time***) to the client system. The information supplied includes the client's IP addresses and netmask plus the address of its ***DNS*** servers and ***Gateway***.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, *www* is the host name of a Web server and *www.pSIONteklogix.com* is the fully-qualified name of that server. DNS translates the domain name *www.pSIONteklogix.com* to some IP address, for example 66.93.138.219.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which *top level domain* (TLD) it belongs to. Every country has its own top-level domain, for example *.de* for Germany, *.fr* for France, *.jp* for Japan, *.tw* for Taiwan, *.uk* for the United Kingdom, *.us* for the U.S.A., and so on. There are also *.com* for commercial bodies, *.edu* for educational institutions, *.net* for network operators, and *.org* for other organizations as well as *.gov* for the U. S. government and *.mil* for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, images, tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some **Beacon** frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the **Access Point** awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See *IP Address*.

E

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

EDCF

Enhanced Distribution Control Function is an extension of **DCF**. EDCF, a component of the IEEE Wireless Multimedia (WMM) standard, provides prioritized access to the wireless medium

ESS

An *extended service set* (ESS) is an **Infrastructure Mode Wireless Networking Framework** with multiple access points, forming a single subnetwork that can support more clients than a basic service set (**BSS**). Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (**LAN**) architecture supporting data transfer rates of 10 Mbps to 1 Gbps. The Ethernet specification is the basis for the **IEEE 802.3** standard, which specifies the physical and lower software layers. It uses the **CSMA/CA** access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as “*XbaseY*”, where *X* is the data rate in Mbps and *Y* is the category of cabling. The original cable was *10base5* (Thicknet or “Yellow Cable”). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by **IEEE 802.11g** stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the **IEEE 802.11g** standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel.

Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations.

If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the access point and enable *request to send (RTS)* and *clear to send (CTS)* protection before sending data.

See also **CSMA/CA** protocol.

F

Frame

A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network. Each frame includes a

Gateway

source and destination **MAC** address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a **Packet**, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the **OSI** model).

G

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a **LAN** can access the Internet, it needs to know the address of its *default gateway*.

H

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an `<html>` tag and ends with a `</html>` tag. A properly formatted document also contains a `<head> ... </head>` section, which contains the metadata to define the document, and a `<body> ... </body>` section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986.

HTML documents are sent from server to browser via **HTTP**. Also see **XML**.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a **URL** and a command (GET, HEAD, POST, etc.), a request followed by a response.

I**IAPP**

The *Inter Access Point Protocol* (IAPP) is an **IEEE** standard (**802.11f**) that defines communication between the access points in a “distribution system”. This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an **Ad hoc Mode Wireless Networking Framework** in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See **802**, **802.1x**, **802.11**, **802.11a**, **802.11b**, **802.11e**, **802.11f**, **802.11g**, and **802.11i**.)

For more information about IEEE task groups and standards, see <http://standards.ieee.org/>.

Infrastructure Mode

Infrastructure Mode is a **Wireless Networking Framework** in which wireless stations communicate with each other by first going through an **Access Point**. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (**BSS**) or a number of access points (**ESS**).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly. It is combined with higher-level protocols, such as **TCP** or **UDP**, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called *IPv6* or *IPng*, is under development. *IPv6* is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in form 192.168.2.254. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A **Subnet Mask** is used to define the portions. There are two special host numbers:

- The **Network Address** consists of a host number that is all zeroes (for example, 192.168.2.0).
- The **Broadcast Address** consists of a host number that is all ones (for example, 192.168.2.255).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

A **Dynamic IP Address** is an IP address that is automatically assigned to a host by a **DHCP** server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A **Static IP Address** is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the **IP** layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.
- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

J

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including **Latency**), **QoS** for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. **QoS** is designed to reduce jitter along with other factors that can impact network performance.

Latency

L

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a **Packet** from sender to receiver. Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. **QoS** features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. **Ethernet** is the most common technology implementing a LAN.

Wireless Ethernet (**802.11**) is another very popular LAN technology (also see **WLAN**).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the **DHCP** Server gives its clients an **IP Address** and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the **PHY** layer, working in conjunction with the **MAC** layer.

M

MAC

The *Media Access Control* (MAC) layer handles moving data packets between **NICs** across a shared channel. It is a higher level protocol over the **PHY** layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. **IEEE 802** network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

MDI and MDI-X

Medium Dependent Interface (MDI) and *MDI crossover* (MDIX) are twisted pair cabling technologies for Ethernet ports in hardware devices. Built-in twisted pair cabling and auto-sensing enable connection between like devices with the use of a standard Ethernet cable. (For example, if a wireless access point supports MDI/MDIX, one can successfully connect a PC and that access point with an Ethernet cable rather than having to use a crossover cable).

MIB

Management Information Base (MIB) is a database of objects used for network management. **SNMP** agents along with other SNMP tools can be used to monitor any network device defined in the MIB.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for **PPP** connections between a Windows-based computer and an **Access Point** or other network access device.

MTU

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of *IEEE 802.1x Frames* to a specified set of client stations (*MAC* addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also *Unicast* and *Broadcast*.

N

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a *LAN*. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See *IP Address*.

NIC

A *Network Interface Card* is an adaptor or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, **Ethernet** or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

O**OSI**

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a components of the physical layer.
- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as **CSMA/CA** and components like **MAC** addresses, and **Frames** are all defined and dealt with as a part of the Data-Link layer.
- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. **Packets** and logical **IP Addresses** operate on the network layer.
- Layer 4, the Transport layer, defines connection oriented protocols such as **TCP** and **UDP**.

Packet

- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).
- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.
- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (**HTTP**), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

P

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. **QoS** features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see **OSI**). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal - through the network at the electrical and mechanical level. It provides the

hardware means of sending and receiving data on a medium, including defining cables, *NICs*, and physical aspects.

Ethernet and the *802.11* family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the `fork()` system call. It can be used by `wait()` or `kill()` to perform actions on the given process.

Port Forwarding

Port Forwarding creates a ‘tunnel’ through a firewall, allowing users on the Internet access to a service running on one of the computers on your *LAN*, for example, a Web server, an FTP or SSH server, or other services. From the outside user’s point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (*IP* packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a *LAN* to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunnelling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (*VPN*) within the *Point-to-Point Protocol* (*PPP*). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real

PSK

server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see ***Shared Key***.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see ***Shared Key***.

Q

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize ***Latency***, ***Jitter***, ***Packet Loss***, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The ***IEEE*** standard for implementing QoS on wireless networks is currently in-work by the ***802.11e*** task group. A subset of ***802.11e*** features is described in the ***WMM*** specification.

R

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ***ISPs***.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Roaming

In *IEEE 802.11* parlance, *roaming clients* are mobile client stations or devices on a wireless network (*WLAN*) that require use of more than one *Access Point* (AP) as they move out of and into range of different base station service areas. *IEEE 802.11f* defines a standard by which APs can communicate information about client associations and disassociations in support of roaming clients.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (*LANs*) or between a *LAN* and a wide-area network (*WAN*), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an *802.1x* value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTP

Real-Time Transport Protocol (RTP) is an Internet protocol for transmitting real-time data like audio and video. It does not guarantee delivery but provides support mechanisms for the sending and receiving applications to enable streaming data.

RTS

RTP typically runs on top of the **UDP** protocol, but can support other transport protocols as well.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the access point, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 **CSMA/CA** protocol. (See also **RTS Threshold** and **CTS**.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (**RTS**) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

S

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see **Public Key**.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the **TCP/IP** protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (**MIBs**) and return this data to the SNMP management system when requested.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See *IP Address*.

STP

The *Spanning Tree Protocol* (STP) an IEEE 802.1 standard protocol (related to network management) for **MAC** bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and re-establishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as 255.255.255.0) or as a number appended to the IP address (for example, 192.168.2.0/24).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is 192.168.2.128 and the netmask is 255.255.255.0, the resulting Network address is 192.168.2.0.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

<i>IP address</i>	192.168.2.128	11000000 10101000 00000010 10000000
<i>Netmask</i>	255.255.255.0	11111111 11111111 11111111 00000000
<i>Resulting network address</i>	192.168.2.0	11000000 10101000 00000010 00000000

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the ***Basic Rate Set***.

T

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (***IP***). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although ***TCP*** and ***IP*** are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, ***UDP***, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called “Michael”), and a re-keying mechanism. It uses a ***RC4*** stream cipher to encrypt the frame body and CRC of each ***802.11*** frame before transmission. It is an important component of the ***WPA*** and ***802.11i*** security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit *Type of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way “best-effort” settings depending upon the requirements of the data. The ToS field is used by the 9160 Wireless Gateway to provide configuration control over *Quality of Service* (*QoS*) queues for data transmitted from the AP to client stations.

U

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an *IP* packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of *IEEE 802.1x Frames* directly to a single client station *MAC* address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also *Multicast* and *Broadcast*.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML

VLAN

document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, `ftp://ftp.devicescape.com/downloads/myfile.tar.gz` specifies a file that should be fetched using the FTP protocol; `http://www.devicescape.com/index.html` specifies a Web page that should be fetched using the **HTTP** protocol.

V

VLAN

A *virtual LAN* (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The 9160 Wireless Gateway supports the configuration of a wireless VLAN. This technology is leveraged on the access point for the “virtual” guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

W

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites.

The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an **Access Point** is connected to a wired **LAN**. WDS allows access points to be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for **802.11** wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) **Shared Key** for data encryption. It uses a **RC4** stream cipher to encrypt the frame body and CRC of each **802.11** frame before transmission.

Wi-Fi

A test and certification of interoperability for **WLAN** products based on the **IEEE 802.11** standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an **Ad hoc Mode** network, also known as an independent basic service set (**IBSS**).
- Stations communicate through an **Access Point** in an **Infrastructure Mode** network. A single access point creates an infrastructure basic service set (**BSS**) whereas multiple access points are organized in an extended service set (**ESS**).

WLAN

WLAN

Wireless Local Area Network (WLAN) is a **LAN** that uses high-frequency radio waves rather than wires to communicate between its nodes.

WMM

Wireless Multimedia (WMM) is a **IEEE** technology standard designed to improve the quality of audio, video and multimedia applications on a wireless network. Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled. WMM features are based on is a subset of the **WLAN** IEEE **802.11e** draft specification. Wireless products that are built to the standard and pass a set of quality tests can carry the “Wi-Fi certified for WMM” label to ensure interoperability with other such products. For more information, see the WMM page on the Wi-Fi Alliance Web site: <http://www.wi-fi.org/OpenSection/wmm.asp>.

WPA

Wi-Fi Protected Access (WPA) is a **Wi-Fi** Alliance version of the draft **IEEE 802.11i** standard. It provides more sophisticated data encryption than **WEP** and also provides user authentication. WPA includes **TKIP** and **802.1x** mechanisms.

WPA2

Wi-Fi Protected Access (WPA2) is an enhanced security standard, described in **IEEE 802.11i**, that uses Advanced Encryption Standard (**AES**) for data encryption.

The original **WPA** uses Temporal Key Integrity Protocol (**TKIP**) for data encryption. WPA2 is backwards-compatible with products that support the original **WPA**.

WPA2, like the original **WPA**, supports an *Enterprise* and *Personal* version. The Enterprise version requires use of IEEE **802.1x** security features and *Extensible Authentication Protocol* (**EAP**) authentication with a **RADIUS** server.

The Personal version does not require IEEE **802.1x** or **EAP**. It uses a *Pre-Shared Key* (**PSK**) password to generate the keys needed for authentication.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for **802.11i** that uses *AES* but another encryption mode (OCB) for encryption and integrity.

X

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986, designed especially for electronic publishing.

INDEX

A

- access point
 - administrator password 201
 - clustering 56
 - configuration policy 50
 - ethernet (wired) settings 97
 - guest network 141
 - load balancing 165
 - MAC filtering 161
 - monitoring 205
 - QoS 171
 - radio 153
 - security 113
 - standalone 58
 - time protocol 197
 - user management 65
 - WDS bridging 185
 - wireless settings 105
- administrator
 - password 203
 - on Basic Settings 49
 - platform 26
- ANSI, connecting terminals 20
- antenna requirements 17, 18
- approvals xvi
- associated wireless clients 214
- Atheros Turbo modes 7, 8
- authentication
 - in different security modes 116
- authentication server
 - for IEEE 802.1x security mode 131
 - for WPA/WPA2 Enterprise (RADIUS) security mode 136
- auto-synch of cluster configuration 60

B

- back up
 - AP configuration 223
 - user accounts database 71
- backup links, WDS 189
- basic settings, viewing 42

- beacon interval, configuring 157
- bridges, WDS 187
- broadcast modes 7

C

- cables
 - console port No. 19387 B-2
 - serial descriptions B-2
- cables, coaxial 18
- captive portal 145
- certificate
 - obtaining TLS-EAP certificate for client C-34
 - security for IEEE 802.1x client C-14
 - security for WPA/WPA2 Enterprise (RADIUS) client C-23
- channel
 - automated management of clustered APs 81
 - configuring 157
- channel management of clustered APs
 - advanced settings 86
 - example 82
 - proposed channel assignments 86
 - understanding 81
 - viewing/setting locks 85
- client
 - associations 214
 - link integrity monitoring 214
 - platform 27
 - security C-1
 - sessions 73
 - See also *stations* 157
- cluster
 - adding an access point to 62
 - auto-synch 60
 - channel management 79
 - definition 56
 - formation 59
 - mode 58
 - neighbors 89
 - removing an access point from 61

- security 60
- size 56
- size and membership 59
- troubleshooting *D-4*
- types of access points supported 56
- understanding 56
- cluster neighbors 91
- configuration policy setting 50
- connecting
 - ANSI compatible terminals 20
 - console 20
 - Ethernet 19
 - video display terminal 20
- connectors
 - RJ-45 *B-3*
- console
 - port
 - cable No. 19387 *B-2*
 - pinouts *B-1*
- console, connecting 20

D

- data rate, serial 20
- DCF as related to QoS 176
- DEC VT220, connecting 20
- default settings
 - defined 23
 - resetting to 218
- DHCP
 - understanding in relation to self-managed APs 28
- directional antenna 17
- DTIM period, configuring 157

E

- EAP-PEAP
 - configuring on IEEE 802.1x client *C-11*
 - configuring on WPA/WPA2 Enterprise (RADIUS) client *C-19*
- electrical safety approvals *xvi*
- Emissions Information, Canada *xv*
- encryption in different security modes 116
- environmental requirements 15
 - operating relative humidity 229
 - operating temperature 229
 - overview 15
 - storage temperature 229
- Ethernet

- adaptor cards 230
- cable lengths 19
- connections 19, 34
- settings 97, 147
- status indicator LED 20
- 10BaseT 19
 - pinouts *B-3*
- 100BaseT 19
 - pinouts *B-3*
- events
 - log 208
 - monitoring 208
- extended service set
 - with WDS bridging 187
- external devices 18

F

- factory defaults
 - described 23
 - reverting to from Web UI 218
- features overview 8
- Firefox 20
- firmware upgrade 219
- Flash ROM 230
- fragmentation threshold, configuring 157

G

- guest interface
 - configuring 144
 - explanation 143
 - features overview 10
 - VLANs 144

H

- hardware connections 34

I

- icons on UI 52
- IEEE 802.1x
 - security mode
 - client configuration *C-11*
 - configuring 131
 - when to use 118
- IEEE 802.11
 - radio mode, configuring 157
 - rate set, configuring 157
 - standards support 8
- IEEE 802.11a
 - configuring 157
- IEEE 802.11b

- configuring 157
- IEEE 802.11g
 - configuring 157
- input voltage (power requirements) 16, 230
- installation
 - antennas 19
 - environmental requirements 15, 229
 - LAN 19
 - power cable 19
 - safety xvii
- interfaces, network 230
- interframe spaces
 - as related to QoS 176
- Internet Explorer 20
- IP addresses
 - navigating to 63
 - understanding policies for self-managed APs 28
 - viewing for access points 55, 75, 91

K

- key management, security 116
- kickstart
 - running to find access points 37

L

- LAN installations 19
- LEDs 20
- link integrity monitoring 214
- load balancing, configuring 169
- location, describing 61
- logon administration Web pages 41
- loops, WDS 189

M

- MAC filtering, configuring 164
- maintenance requirements 16
- management password 203
- memory 230
- Microsoft Internet Explorer 20
- Mini-PCI card radios
 - installation and antennas 16
 - specifications 230
 - status indicator LEDs 20

N

- Neighbor 91

- neighboring access points 215
- networking, features overview 11
- network interfaces 230
- NTP server
 - configuring access point to use 200

O

- offices list A-2
- omnidirectional antenna 17
- operating
 - relative humidity 229
 - temperature 229
- orchestrator features overview 10

P

- packet bursting
 - as related to QoS 178
- parameters
 - changing with a web browser 20
- password
 - configuring administrator 203
 - network setting for administrator 49
 - on Basic Settings 49
- PEAP
 - configuring on IEEE 802.1x client C-11
 - configuring on WPA/WPA2 Enterprise (RADIUS) client C-19
- physical
 - description 229
 - specifications 229
- pinouts *See port pinouts*
- plain-text security mode
 - client configuration C-7
 - configuring 126
 - when to use 117
- platform
 - administrator requirements 26
 - client requirements 27
- policy
 - configuration for new access points 50
- port
 - pinouts
 - console port B-1
 - RJ-45 connector (10BaseT) B-3
- ports
 - hardware 33
 - location 18
- power

- connections 34
- requirements 16, 230
- Power Over Ethernet specifications 230
- processor 230
- progress bar for cluster auto-synch 60

Q

- quality of service 171
- queues, configuring for QoS 178

R

- radio
 - beacon interval 157
 - broadcast modes 7
 - channel managed of clustered APs 79
 - configuring one or two radio AP 157
 - DTIM period 157
 - fragmentation threshold 157
 - IEEE 802.11 mode 157
 - maximum stations 157
 - Mini-PCI card radios 230
 - rate sets 157
 - RTS threshold 157
 - specifications 230
 - status indicator LEDs 20
 - SuperAG 157
 - transmit power 157
 - Turbo broadcast mode, not recommended 8
 - turning on or off 157
- RADIUS server
 - configuring to acknowledge access points C-30
 - See also *authentication server*
 - reset access point to factory defaults 218
 - restore configuration 223
 - RJ-45 connector pinouts (10BaseT Ethernet) B-3
 - rogue access points 215
 - RTS threshold, configuring 157

S

- safety
 - approvals xvi
 - instructions xvii
- SDRAM 230
- security
 - authentication server C-30
 - certificates on client C-34

- comparison of modes 116
- configuring on the access point 124
- configuring on wireless clients C-1
- features overview 9
- IEEE 802.1x 131
- plain-text 126
- pros and cons of different modes 115
- static WEP 126
- WPA/WPA2 Enterprise (RADIUS) 136
- WPA/WPA2 Personal (PSK) 133
- serial
 - data rate 20
 - status indicator LED 20
- session monitoring 76
- specifications
 - Mini-PCI card radios 230
 - physical 229
- standalone mode 58
- standards 8
- starting the network 51
- static WEP security mode
 - configuring 126
 - on WDS bridge 190
 - when to use 117
- stations
 - configuring maximum allowed 157
 - See also *client*
- status indicators (LEDs) 20
- supported platforms
 - administrator 26
 - client 27
- synchronization of cluster 60

T

- terminal
 - connecting a video display 20
- text conventions 7
- time
 - configuring an access point to use NTP server 200
- TLS-EAP
 - configuring on IEEE 802.1x client C-14
 - configuring on WPA/WPA2 Enterprise (RADIUS) client C-23
 - obtaining certificate for client C-34
- ToS as related to QoS 174
- transmit/receive information 212

transmit power, configuring 157
troubleshooting startup problems 44
Turbo broadcast mode, not recommended
8

U

upgrading the firmware 219
user accounts
 backing up and restoring 71
 for built-in authentication server 65
user authentication
 configuring on IEEE 802.1x client
 C-11
 configuring on WPA/WPA2 Enterprise
 (RADIUS) client C-19

V

video display terminal, connecting 20
VLANs
 for internal and guest interface 144
Voice over IP
 improved service with QoS 171
voltage, input 16, 230

W

wait time for cluster auto-synch 60
WDS
 configuring 190
 example 194
 explanation 187
 rules 192
web browser 20
WEP security mode
 client configuration C-8
 configuring 126
 when to use 117
Wi-Fi compliance 8
wired settings 97, 147
wireless
 neighborhood 89
 overview of AP features 7
 settings 105
worldwide offices A-2
WPA/WPA2 Enterprise (RADIUS) security
 mode
 client configuration C-18
 configuring 136
 when to use 120
WPA/WPA2 Personal (PSK) security mode

client configuration C-27
configuring 133
when to use 119

10BaseT Ethernet 19, B-3
100BaseT Ethernet 19, B-3

