WiNG Express 5.8.1

Access Point

User Guide
Contents

Chapter 1 Introduction to WiNG Express ................................................................. 4

Chapter 2 Basic WiNG Express Access Point Configuration ................................. 7

Chapter 3 DashBoard ............................................................................................. 15

Chapter 4 Monitor ................................................................................................... 19

Chapter 5 Configuration ......................................................................................... 31

Chapter 6 Event History .......................................................................................... 61

Chapter 7 Customer Support .................................................................................. 63
Chapter 1

WiNG Express is a new *User Interface* (UI) that simplifies the configuration and monitoring of small Access Point deployments by limiting monitoring, analytics, and configuration capabilities. WiNG Express is a simplified version of the WiNG operating system currently shipping with the WiNG family of controllers, service platforms and Access Points.

WiNG Express is designed for single-site Access Point deployments not exceeding more than 24 Access Points of the same model. The following network profiles are specifically targeted:

- Single AP deployment, LAN

![Network Diagram](case1)

*Case 1: Single AP deployment, LAN*

- Single AP deployment, WAN

![Network Diagram](case2)

*Case 2: Single AP deployment, WAN*
- Multi AP deployment, LAN

Case 3: Multi AP deployment, LAN

- Multi AP deployment, WAN

Case 4: Multi AP deployment, WAN
For the WiNG Express version SKUs, both the WiNG Express UI and an over the air (OTA) provisioning configuration is required. For a non WiNG Express SKU, there’s no OTA configuration required.
For a WiNG Express SKU Access Point, both the WiNG Express UI and an Over The Air (OTA) provisioning configuration are required for a basic setup and network connection. For a non WiNG Express SKU Access Point, there’s no OTA support, and the Access Point utilizes just the UI for its basic setup.

To provide the Access Point a basic configuration and access WiNG Express management functions:

1. Power up the Access Point.
   The Access Point can be powered using an appropriately rated power adapter, POE injector or POE switch resource.

2. Connect to the Access Point.
   For WiNG Express Models:
   Connect to the WiNG Express SSID. For Windows systems, locate the SSID by selecting the network icon on the bottom right corner of the screen. For MAC systems, locate the SSID by selecting the network icon on the top right corner of the screen.

   ![Identifying WiNGExpress](image)

   Open a browser (Chrome, Firefox or Internet Explorer) and enter https://express.zebra.com.
   The login screen displays.

   For non-WiNG Express Models:
   Refer to the bottom of the Access Point to obtain the numeric IP address used for connecting to the device. Point the Web browser to the Access Point’s IP address.
   The login screen displays.

3. Enter the default username admin in the Username field.
4. Enter the default password admin123 in the Password field.
5. Select the Login button to load the management interface.
If this is the first time the WiNG Express interface has been accessed, a screen displays prompting for the Access Point’s country code.

Select the **Country Code** specific to this Access Point’s deployment location.

Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. Select **Apply** to implement the selected Country Code. SKU’s only support certain countries (for example: a US SKU only includes US, Guam, Puerto Rico, American Samoa, US Virgin Islands and Mariana Island).

The Access Point automatically displays a Dashboard where users can assess network health and conduct a diagnostic review of Access Point performance.
Note: At some point in the Access Point’s initial setup, the default password should be changed to enhance the security of the network. Refer to the Configuration > Management screen to change the default password to a more secure password.

7 Expand the Configuration menu item and select **Basic**.

**Configuration -> Basic Settings**

Basic Configuration Settings

- **AP Name:** ap6521-42936C
- **Country Code:** India-in
- **Virtual Controller:** [ ]
- **Timezone:** Etc/UTC
- **Date & Time:** 04/01/2014, 5:00 AM
- **NTP Server:** 192.168.1.55

8 Set the following Basic Configuration Settings for this Access Point:

- **AP Name** - Provide an AP Name used as this Access Point’s WING Express network identifier. If setting this Access Point as a Virtual Controller, each Access Point managed by this Virtual Controller lists this Access Point’s AP Name as its own. The AP Name is a required parameter.

- **Country Code** - If the Country Code was not set when the Access Point was initially powered on, set the country now to ensure the Access Point’s legal operation. The Access Point’s wireless capabilities are disabled until the required country code is set.

- **Virtual Controller** - Select this option to define this Access Point as a Virtual Controller capable of managing and provisioning up to 24 Access Points of the same model. If selecting this Access Point as a Virtual Controller, those Access Points managed by this Virtual Controller will list this Access Point’s AP Name as its own. Only one Virtual Controller can be designated.
- **Timezone** - Use the drop-down menu to specify the geographic timezone where the Access Point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.

- **Date & Time** - Set the date, hour and minute for the Access Point’s current system time. Specify whether the current time is in the AM or PM.

- **NTP Server** - Optionally provide the IP address of a NTP server resource. *Network Time Protocol* (NTP) manages time and/or network clock synchronization within the WiNG Express network. NTP is a client/server implementation. Access Points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an Access Point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

- **Controller Adoption** - To adopt to a controller enter the IP address in the Host filed and select a Level from the drop-down menu.

9 Select **Apply** to implement the updates. Select **Apply** to implement the updates.

10 Expand the **Configuration** menu item and select **WAN**.

**WAN Settings**

- **Enable**: ✔
- **Port**: ge1
- **Interface**: vlan1

  - **DHCP Client**
  - **Static IP**
  - **PPTP Settings**

  **Static IP/Mask**: 192.168.131.1 /24
  **Primary DNS**: 4.4.4.4
  **Secondary DNS**: 192.168.1.10
  **Default Gateway**: 192.168.1.1

11 Refer to the **WAN Settings** field and set the following:

- **Enable** - Select this option to allow a connection between the Access Point and a larger network or outside world through the WAN port. Disable this option to isolate the WAN connection. No connections to a larger network or Internet are possible. Clients cannot communicate beyond configured subnets. Both the physical Port used to connect to the WAN and the *virtual Interface* (VLAN) are also listed and fixed.

- **DHCP Client** - Select this option to enable DHCP for the Access Point WAN connection. This is useful, if the target network or *Internet Service Provider* (ISP) uses DHCP. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The WAN and LAN ports should not both be configured as DHCP clients.

- **Static IP** - Select this option to bypass DHCP address allocation resources and manually set the IP address for the Access Point’s WAN connection. Manually provide the Access Point’s Static IP/Mask and Default Gateway.
- **PPPoE Settings** - Optionally enable *Point-to-Point Protocol over Ethernet* (PPPoE) on the WAN network. If PPPoE is enabled, provide the required Auth Type, Login Name and Login Password. Server Name and Default Gateway are optional settings. PPP is a data-link protocol for dialup connections allowing an Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression as specified by the PPPoE protocol. PPPoE enables the Access Point to establish a point-to-point connection to an ISP over an existing Ethernet interface.

- **Static IP / Mask** - Specify an IP address for the WAN connection if using static address assignment for the WAN port. An IP address uses a series of four numbers expressed in dot notation, for example, 190.188.12.1. Additionally, specify a Mask for the access point’s WAN connection. This number is available from the ISP for a DSL or cable-modem connection, or from an administrator if the Access Point connects to a larger network.

- **Primary/Secondary DNS/Default Gateway** - If using a static IP or DHCP, enter the Primary and Secondary DNS server resource’s numerical IP address and Default Gateway.

---

**Note:** If segmenting traffic between the Access Point’s WAN and LAN, you’ll need to create a VLAN. Complete steps 13 and 14 to define the required VLAN. Otherwise, proceed to step 15.

12 Select **Apply** to implement the updates.

13 Expand the **Configuration** menu item and select **Access Points**. Each **AP Name** displays as a link that can be selected to update the configuration of that specific Access Point. Select a target AP Name link from amongst those displayed in the Access Points screen.

**NAT Interface Settings**

<table>
<thead>
<tr>
<th>Interface (1-4094)</th>
<th>Description</th>
<th>IP Address</th>
<th>NAT Enable</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td></td>
<td>192.168.13.21/24</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Refer to the **LAN IP Interface Settings** field, and add a VLAN and Static IP as required for enabling DHCP (within the Configuration > Services screen) for client IP address requests and ensuring routable traffic.

14 Select **Apply** to commit the updates to the selected Access Point’s configuration.

15 Expand the **Configuration** menu item and select **Wireless**.

The Wireless screen displays fields where Radio Settings and Wireless LAN settings can be defined. Default radio settings remain as is for the Access Point’s basic setup.

In respect to the **Radio Settings**, the professional installer should be aware of the following:
Note: The above example includes a field for setting the antenna gain. This setting is only available for external antenna model Access Points and does not display for internal antenna model Access Points.

- The Channels available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
- Selecting Smart as the Power setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.
- For external antenna model Access Points, configure the Antenna Gain based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the Access Point and the antenna.

In respect to the Wireless LAN settings, the professional installer should be aware WiNG Express Access Points ship with a default WLAN (WINGExpress). However, this WLAN does not provide adequate authentication to protect from unauthorized user access. An additional WLAN configuration can be created and validated before deleting default WLAN.

16 To create a new WLAN, select Add from the upper, left-hand side of the Wireless LAN field.

17 Set the following configuration attributes for the new WLAN:

- **Name** - Provide a unique name for the WLAN as its network identifier. This is a required setting.
- **Enable** - Select this setting to enable this WLAN within the Access Point managed network and to provide some measure of data protection not available in the default WLAN.

- **SSID** - Specify the WLAN’s SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters. This is a required setting. Select **Client-To-Client Communication** to enable client interoperability within this WLAN. The default is disabled, meaning clients are not allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but if this setting is disabled on the other WLAN, clients are not permitted to interoperate at all.

- **Security** - The screen displays with the **Open** option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended.

If selecting **Secure-PSK**, select an encryption type of WEP-64, WEP-128, TKIP-CCMP or WPA2-CCMP. When the encryption type is selected, enter an encryption key. Define whether the key is entered in ASCII or HEX characters. Detailed security and encryption information is available in the **Configuration > Wireless** section of the documentation.

If selecting **Secure-802.1x**, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to the Access Point’s WLAN resources.

Selecting **Guest** displays fields for captive portal Web page creation, and is beyond the scope of this basic Access Point configuration.

- **Band** - Select the 2.4 GHz and/or 5 GHz (if supported) radio bands supports by the Access Point and its connected client traffic. If this Access Point is designated as a Virtual Controller AP, both radio bands should be enabled.

- **VLAN** - Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Do not use VLAN 1 with the WLAN if the WAN port has been enabled.

- **Description** - Optionally enter a WLAN description to further describe the WLAN’s deployment objective within the WiNG Express managed network.

Select **Apply** to commit the updates to the Access Point’s WLAN configuration.

Expand the **Configuration** menu item and select **Services**.

18 Select **Enable DHCP Server** to ensure the Access Point can provision IP addresses to requesting clients over the specified interface.

20 Select **Enable DHCP Server** to ensure the Access Point can provision IP addresses to requesting clients over the specified interface.
Note: A VLAN must be already configured and available to the DHCP server as a viable interface between the Access Point and requesting client. Refer to the LAN IP Interface Settings field (within the Edit Access Point screen), and add a VLAN.

Select + Add and provide a default gateway, primary dns server, and a starting and ending IP range of addresses that constitute a pool of addresses available to requesting clients. Additional DHCP options are available and are documented in the Configuration > Services > DHCP section.

21 Select Apply to commit the updates to the Access Point’s DHCP configuration.

22 At this point, you’re ready to connect to the network using the security restrictions applied to the newly created WLAN. Ensure the new secure WLAN has been enabled, and check whether a client is able to access the network.

Note: Only when the new WLAN configuration is validated as accessible should the existing WiNG Express default WLAN be deleted.
The dashboard enables administrators to review and troubleshoot Access Point managed network operation. Additionally, the dashboard allows an administrator to assess network component health and conduct a diagnostic review of device performance.

In This Chapter

DashBoard ................................................................. 16
**DashBoard**

The dashboard enables administrators to review and troubleshoot Access Point managed network operation. Additionally, the dashboard allows an administrator to assess network component health and conduct a diagnostic review of device performance.

To review high-level Access Point dashboard information:

1. Select **Dashboard** in the main menu.

2. Review the following to assess the health of the network:

<table>
<thead>
<tr>
<th>System Information</th>
<th>Displays the administrator assigned <em>AP Name</em>, required <em>Country Code</em> for legal geographic deployment in, number of detected <em>Offline APs</em>, whether the Access Point has been enabled as a <em>Virtual Controller</em> to manage peer Access Points, the designated <em>Virtual Controller MAC address</em>, <em>Current Time</em> and <em>Up Time</em> listing when the Access Point was last offline.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Segmentation</td>
<td>Displays a set of pie charts segregating the WLAN utilization amongst peer Access Points and client types. Use this information to help assess whether the client loads exceed the number and type of WLANs currently being deployed with Access Points.</td>
</tr>
<tr>
<td>Network Usage</td>
<td>Displays the network throughput (both in the transmit and receive directions) for the selected Radio or WLAN over the defined trending period of 30 minutes, 2 hours or 24 hours.</td>
</tr>
<tr>
<td>Network Client Count</td>
<td>Displays the total client count for the network over the selected time period of 30 minutes, 2 hours or 24 hours. Clients are partitioned into their current 2.4Ghz and 5Ghz radio bands to help assess whether the client load is adequately supported in each band.</td>
</tr>
</tbody>
</table>
The Monitor screens provide detailed, real-time information about the network and RF health for Access Point Radios, WLANs and wireless Clients. Use the information on these screens to track RF traffic, throughput, signal to noise ratio and client health.

In This Chapter

Radios ................................................................. 19
WLANs ............................................................... 23
Clients ................................................................. 26
Application Visibility .......................................... 29

Radios

Use the Radios screen to assess the quality of the Access Point radio’s utilization, power consumption, and client connections.

To monitor Access Point radios:
1. Select Monitor from the main menu and click on Radios.
2 Select a time interval of 30 minutes, 2 hours or 24 hours from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput utilization, power and signal strength.

3 Review the following Access Point Radio Details:

<table>
<thead>
<tr>
<th>Radio MAC Address</th>
<th>Access Point Name</th>
<th>Radio</th>
<th>Channel</th>
<th>Power (dBm)</th>
<th>Status</th>
<th>Antenna Gain (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-DA-B1-C5-00-1A</td>
<td>ap6521-42036C</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>online</td>
<td>0.0</td>
</tr>
</tbody>
</table>

- **Radio MAC Address**: Displays the *Media Access Control (MAC)* address factory assigned to each radio as its hardware identifier on the network.
- **Access Point Name**: Displays the Access Point's unique administrator assigned name provided upon initial connection.
- **Radio**: Displays the radio number for each Access Point radio on the network. AP6511E and AP6521E models are single radio models, other models support at least two radios.
- **Channel: Current / Config**: Displays the current channel number each listed Access Point radio is set to transmit and receive on, as well as its configured channel number. The *Channels* available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.
<table>
<thead>
<tr>
<th><strong>Power (dBm):</strong>&lt;br&gt;<strong>Current / Config</strong></th>
<th>Displays the current power level in dBm for each Access Point radio as well as its configured power level. If Smart is the defined power setting, the radio automatically configures power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. If Smart is the defined channel, the radio automatically configures the channel to support detected radio coverage holes. The country selected automatically limits the maximum output power that can be set.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Displays the current status for each Access Point. If an Access Point is up, two green up arrows display. If an Access Point is down, two green down arrows display.</td>
</tr>
<tr>
<td><strong>Clients</strong></td>
<td>Displays the number of clients currently associated to each Access Point radio on the network. AP6511E and AP6521E single radio Access Points support 128 clients, the other models support up to 256 client connections.</td>
</tr>
<tr>
<td><strong>Retry (%)</strong></td>
<td>Displays the retry percentage for packets sent on each Access Point radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connection rate in both directions.</td>
</tr>
<tr>
<td><strong>SNR</strong></td>
<td>Displays the connected client's signal to noise ratio (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different Access Point connection to improve performance.</td>
</tr>
</tbody>
</table>

4 Select Details to assess individual Access point radio utilization data in greater detail.
Details

Access Point radio data can be assessed in detail to define periods where the radio's transmit and receive capabilities are jeopardized, or whether noise detected on the network is excessive and warrants administration. Client connections can also be reviewed to determine if the radio has an optimal number of connected client devices in respect to times of day when the radio is over/under utilized.

To review Access Point radio details:
1. Select **Monitor** from the main menu and select **Radios**. Select a radio, then **Details**.

2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.

3. Review the **Throughput** table to assess periods of heavy or light transmission and receive utilization over trended periods.

4. Refer to the **SNR (dBm)** field to assess periods where the Access Point's radio quality could be compromised due to excessive noise on the network.

   *Signal to noise ratio* (SNR) is an interference measurement to help administrators assess whether an Access Point needs load balancing with the assistance of neighbor radios. Additionally, a low SNR could warrant power compensation to account for poorly performing radios. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance.

   Use the **Client Count** table to help determine whether the client load should be increased or decreased based on radio under/over utilization (throughput) and the level of interference detect.

   AP6511E and AP6521E single radio Access Points support 128 clients, other models support up to 256 client connections.
To return to the parent radio screen, select **<<Summary** in the upper, right-hand, side of the graph.

### WLANs

A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provide to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

Periodically refer to the WLANs screen to monitor an Access Point's WLAN utilization and whether WLAN usage is consistent with an Access Point's deployment objective and the security needs of its connected clients.

To review an Access Point's WLAN utilization:

1. Select **Monitor** from the main menu and select **WLANs**.
2. Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio’s throughput, noise ratio and client counts.

### WLAN Details

<table>
<thead>
<tr>
<th>WLAN Name</th>
<th>SSID</th>
<th>Clients</th>
<th>WLAN</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>WINGExpress</td>
<td>WINGExpress</td>
<td>0</td>
<td>2100</td>
<td>captive</td>
</tr>
</tbody>
</table>

Review the following WLAN information to help determine whether the Access Point’s WLAN utilization is optimally set for its deployment objective:

**WLAN Name**
Displays the administrator defined WLAN name for each of the WLANs. Spaces between words are not permitted in the name. The name could be a logical representation of the WLAN’s coverage area (engineering, marketing etc.). The name cannot exceed 32 characters.
SSID

Displays the Services Set Identification (SSID) associated with the WLAN. The maximum number of characters for the SSID is 32.

Clients

Displays the collective number of clients comprising the WLAN's membership, as pooled from each of the Access Points using this listed WLAN.

VLAN

Displays the VLAN ID to which the WLAN is mapped.

Security

Displays the encryption and/or authentication security settings, if any, applied to Access Point member traffic either with peer Access Points or client connection. Authentication ensures only known and trusted users or devices access a WLAN's network resources.

Encryption is central for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. When the 802.11 specification was introduced, Wired Equivalent Privacy (WEP) was the primary encryption mechanism. New device deployments should use either WPA or WPA2 encryption.

Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information.

A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network.

4 To review more granular details of a specific WLAN, select it from the table and select the Details >> link.

Details

A WLAN's configuration can be periodically reviewed in detail to assess whether its configuration still supports the deployment objectives of those Access Points utilizing it, or if configuration changes are needed to better support network client connections.

To review an Access Point information in detail:

1 Select Monitor from the main menu and click on WLANs.
2 Select a reporting interval of 30 minutes, 2 hours or 24 hours from the radio buttons at the top of the page. The graph updates accordingly with the radio’s throughput, noise ratio and client counts.

3 Refer to the following throughput and client data for the selected WLAN:

| Throughput | Displays the WLAN’s time trended throughput (as impacted by the Access Point’s utilizing this WLAN) in both the transmit and receive directions. Use the Throughput table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green. |
| Client Count | Displays the time trended number of clients comprising the WLAN’s membership, as pooled from each of the Access Point’s using this WLAN. AP6511E and AP6521E single radio Access Points support 128 clients, remaining models support up to 256 client connections. |

4 To return to the WLAN screen, select <<Summary. |
Clients

Refer to the Clients screen to assess performance on specific wireless client interfaces.

To review an Access Point's wireless interface connection utilization:

1. Select Monitor from the main menu and click on Clients.

2. Select a reporting interval of 30 minutes, 2 hours or 24 hours from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.

3. Review the following information for clients connected to Access Point radios:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Displays the current IP address, the client is using as its network identifier.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the Media Access Control (MAC) address factory assigned to each wireless client as its unique hardware network identifier.</td>
</tr>
<tr>
<td>Signal (dBm)</td>
<td>Displays the client radio's current power level in dBm. Use this information to assess whether client performance could be improved by connecting to a different Access Point.</td>
</tr>
<tr>
<td>SNR</td>
<td>Displays the connected client's signal to noise ratio (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different Access Point connection to improve performance.</td>
</tr>
<tr>
<td>Radio Type</td>
<td>Lists the 802.11 radio types present in the wireless client. AP7502E and AP7522E models are capable of 802.11ac connections.</td>
</tr>
</tbody>
</table>
**Data Rate (Mbps) Tx / Rx**
Displays the listed client radio's transmit and receive data rates (in Mbps). Use this information to assess RF activity versus other managed client radios in the same radio coverage area.

**BSSID**
Displays the BSSID of the WiNG Express managed Access Point establishing the clients wireless connection.

**Access Point Name**
Displays the Access Point's unique administrator assigned name provided upon initial device connection.

**WLAN**
Displays the SSID of the Wireless LAN, if any, which the wireless client is currently associated with.

**VLAN**
Displays the number of the VLAN which the wireless client is marked to pass traffic on.

**Authentication Status**
Displays the authentication type in use by the wireless client to securely connect to its associated WLAN.

**Activity Last (sec)**
Displays the last detected transmit and receive activity for the listed client within the Access Point device radio coverage area.

**Retry (%)**
Displays the retry percentage for packets sent on each client radio. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connect rate in both directions.

**Vendor**
Displays the manufacturer of each listed client as a means of assessing its support capabilities.

---

**Details**

Refer to the Clients screen to assess performance on specific wireless client interfaces.

To review an Access Point's wired interface connection utilization:

1. Select Monitor from the main menu and click on Clients.
2 Select **Details** to display the **Client Details** graph.

3 Select a reporting interval of **30 minutes**, **2 hours** or **24 hours** from the radio buttons at the top of the page. The graph updates accordingly with the radio's throughput, noise ratio and client counts.

4 Refer to the following throughput and client data for the selected Clients:

<table>
<thead>
<tr>
<th><strong>Throughput (Kbps)</strong></th>
<th>Displays the WLAN's time trended throughput (as impacted by the Access Point's utilizing this WLAN) in both the transmit and receive directions. Use the <em>Throughput</em> table to assess periods of heavy or light transmission and receive utilization over trended periods. Transmitted packets display in blue, received packets in green.</th>
</tr>
</thead>
</table>

| **SNR** | Refer to the **SNR (dBm)** field to assess periods where the client's radio quality could be compromised due to excessive noise on the network. Displays the connected client's *signal to noise ratio* (SNR). SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A SNR of 45 or high indicates excellent RF performance. A SNR of less than 15 indicates poor RF performance. A low SNR could warrant a different Access Point connection to improve performance. |

5 To return to the Clients screen, select **<<Summary**.
Application Visibility

Deep packet inspection (DPI) is an advanced packet filtering technique functioning at the application layer. Use DPI to find, identify, classify, reroute or block packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

Application

To monitor application visibility:
1. Select **Monitor** from the main menu and click on **Application Visibility**.
2. Refer to the **Top 10 Applications** graph to assess the most prolific, and allowed, application data passing through member devices.

<table>
<thead>
<tr>
<th>Total Bytes</th>
<th>Displays the top ten utilized applications in respect to total data bytes passing through the network. These are only the administrator allowed applications approved for proliferation within the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Uploaded</td>
<td>Displays the top ten applications in respect to total data bytes uploaded through the network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).</td>
</tr>
<tr>
<td>Bytes Downloaded</td>
<td>Displays the top ten applications in respect to total data bytes downloaded from the network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).</td>
</tr>
</tbody>
</table>

3. Refer to the **Application Details** table to assess specific application data utilization:

<table>
<thead>
<tr>
<th>Name</th>
<th>Lists the allowed application name whose data (bytes) are passing through the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uploaded</td>
<td>Displays the number of uploaded application data (in bytes) passing the through the network.</td>
</tr>
<tr>
<td>Downloaded</td>
<td>Displays the number of downloaded application data (in bytes) passing the through the network.</td>
</tr>
<tr>
<td>Num Flows</td>
<td>Lists the total number of application data flows passing through the network for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow.</td>
</tr>
<tr>
<td>Clear All</td>
<td>Select this option to clear the application assessment data counters and begin a new assessment.</td>
</tr>
</tbody>
</table>
Category

To monitor an application category:

1. Select **Monitor** from the main menu and click on **Application Visibility**.
2. Refer to the **Top 10 Category** graph to assess the most prolific, and allowed, application data categories utilized.

<table>
<thead>
<tr>
<th>Total Bytes</th>
<th>Displays the top ten application categories in respect to total data bytes passing through the network. These are only the administrator allowed application categories approved for proliferation within the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Uploaded</td>
<td>Displays the top ten application categories in respect to total data bytes uploaded through the network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority).</td>
</tr>
<tr>
<td>Bytes Downloaded</td>
<td>Displays the top ten application categories in respect to total data bytes downloaded from the network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority).</td>
</tr>
</tbody>
</table>

3. Refer to the **Category Details** table to assess specific application category data utilization:

<table>
<thead>
<tr>
<th>Name</th>
<th>Lists the allowed category whose application data (in bytes) is passing through the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uploaded</td>
<td>Displays the number of uploaded application category data (in bytes) passing through the network.</td>
</tr>
<tr>
<td>Downloaded</td>
<td>Displays the number of downloaded application category data (in bytes) passing through the network.</td>
</tr>
<tr>
<td>Num Flows</td>
<td>Lists the total number of application category data flows passing through devices. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow.</td>
</tr>
<tr>
<td>Clear All</td>
<td>Select this option to clear the application category assessment data counters and begin a new assessment.</td>
</tr>
</tbody>
</table>
The Configuration screens contain the settings needed to configure basic device information and wired and wireless network settings, security, DHCP, access management and Access Point settings.

In This Chapter

- Basic .......................................................... 31
- LAN ............................................................ 33
- WAN ............................................................ 35
- Wireless ....................................................... 37
- Security ....................................................... 45
- DHCP .......................................................... 49
- Services ....................................................... 50
- Management ............................................... 53
- Access Points ............................................. 55

Basic

Refer to the Basic screen to set many of the basic parameters required to get the Access Point up and running with little additional configuration.

To configure an Access Point's basic settings:

1. Select Configuration Settings from the main menu then select Basic.
The Basic Configuration Settings screen also displays the first time a user connects to the user interface on an unconfigured Access Point.

2 Configure the following Basic Configuration Settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Provide an AP Name used as this Access Point’s administrative network identifier. If setting this Access Point as a Virtual Controller, each Access Point managed by this Virtual Controller lists this Access Point’s AP Name as its own. The AP Name is a required parameter.</td>
</tr>
<tr>
<td>Country Code</td>
<td>If the Country Code was not set when the Access Point was initially powered on, set the country now to ensure the Access Point’s legal operation. The Access Point’s wireless capabilities are disabled until the required country code is set.</td>
</tr>
<tr>
<td>Virtual Controller</td>
<td>Select this option to define this Access Point as a Virtual Controller capable of managing and provisioning up to 24 Access Points of the same model. If selecting this Access Point as a Virtual Controller, those Access Points managed by this Virtual Controller will list this Access Point’s AP Name as its own. Only one Virtual Controller can be designated.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Use the drop-down menu to specify the geographic timezone where the Access Point is deployed. Different geographic time zones have daylight savings clock adjustments, so specifying the timezone correctly is important to account for geographic time changes.</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>Set the date, hour and minute for the Access Point’s current system time. Specify whether the current time is in the AM or PM.</td>
</tr>
</tbody>
</table>
NTP Server

Optionally provide the IP address of a NTP server resource. *Network Time Protocol* (NTP) manages time and/or network clock synchronization within the WiNG Express network. NTP is a client/server implementation. Access Points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, an Access Point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

**Note:** Changing the Country Code resets the Access Point’s radio(s). During the reset there is no communication with the Access Point through its wireless interfaces. When the reset is complete, communication with the Access Point is restored.

3 In the *Controller Adoption* section, to adopt a controller enter the IP address in the *Host* filed and select a *Level* from the drop-down menu.

4 When all required settings are configured, click *Apply* to save the changes to the Basic Configuration Settings.

**LAN**

Refer to the *LAN* screen to set the virtual controller’s wired interfaces.

To configure an Access Point’s wired interface settings:

1 Select *Configuration* settings from the main menu then select *LAN*.

---

**LAN Port Settings**

<table>
<thead>
<tr>
<th>Port</th>
<th>Enable</th>
<th>Allowed VLANs (1-5,6,7)</th>
<th>Untagged VLAN (1-40)</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IP Settings**

Go to Access Points page to add interfaces with static IP addresses.

<table>
<thead>
<tr>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>DHCP</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN10000</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>VLAN401</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

The *LAN* page is divided into *LAN Port Settings* and *IP Settings* fields.

**Note:** Changes made to an Access Point’s *Configuration* are pushed (provisioned) to up to 24 Access Points of the same model.

2 Configure the following *LAN Port Settings* for each LAN port:
### Port
Displays the physical interface (GE1, FE1, etc.) for each Access Point wired connection on the network. Supported Access Point models each have unique physical interface connections. Supported interfaces include:

- **AP6511E** - FE1, FE2, FE3, FE4, UP1/POE
- **AP6521E** - GE1/POE (LAN)
- **AP6522E** - GE1/POE (LAN)
- **AP6562E** - GE1/POE (LAN)
- **AP7502E** - GE1, FE1, FE2, FE3
- **AP7522E** - GE1/POE (LAN)

### Enable
Select *Enable* to allow traffic on the selected wired interface. Uncheck this option to disable wired traffic on a selected Access Point interface.

### Allowed VLAN
Displays the VLAN(s) that traffic is allowed on as a virtual interface for each Access Point wired port.

### Untagged VLAN
Displays the VLAN(s) that untagged traffic will be transmitted and received on.

### Edit
Select *Edit* to make changes to the selected interface.

3. Select either Default or Details for the view and configure the following **IP Settings** for each VLAN interface:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Displays the VLAN information for each VLAN interface utilized by the Access Point's wired port connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Optionally provide a description for each VLAN interface.</td>
</tr>
<tr>
<td><strong>DHCP Client</strong></td>
<td>Select DHCP to configure IP Address and Mask information using a DHCP Server. To manually configure the network address manually, uncheck the DHCP check box and enter an IP Address and subnet mask.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Select <em>Edit</em> to make changes to the selected interface.</td>
</tr>
</tbody>
</table>
WAN

Refer to the **WAN** screen to set specific Access Point wide area network interface settings.

To configure an Access Point's WAN interface settings:

1. Select **Configuration** settings from the main menu, then select **WAN**.

2. Configure the following **WAN Settings**:

   | **Enable** | **Select this option to allow a connection between the Access Point and a larger network or outside world through the WAN port. Disable this option to isolate the WAN connection. No connections to a larger network or Internet are possible. Clients cannot communicate beyond configured subnets. Both the physical Port used to connect to the WAN and the Virtual Local Area Network (VLAN) interface are also listed and fixed.** |
   | **PPPoE Settings** | **Optionally enable Point-to-Point Protocol over Ethernet (PPPoE) on the WAN network. If PPPoE is enabled, provide the Login Name, Login Password, Server Name, Default Gateway, Primary DNS and Secondary DNS IP addresses. PPP is a data-link protocol for dialup connections. PPPoE allows an Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables Access Points to establish a point-to-point connection to an ISP over an existing Ethernet interface.** |
   | **Login Name** | **Provide the login name provided by your ISP.** |
   | **Login Password** | **Provide the password associated to the login name provided by your ISP.**
<table>
<thead>
<tr>
<th><strong>Server Name</strong></th>
<th>Optionally, provide a server name if required by your ISP.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Gateway</strong></td>
<td>Enter the IP address of the network's default gateway. A default gateway provides an entry/exit point for the network as it commonly connects an internal network to an external network.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>Enter an IP Address for the main DNS server resource for the Access Point's WAN interface.</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong></td>
<td>Enter an IP Address for the backup (secondary) Domain Name Server providing DNS services for the Access Point's WAN interface.</td>
</tr>
</tbody>
</table>

3. The **NAT Interface Settings** section displays the following NAT information:

<table>
<thead>
<tr>
<th><strong>Interface</strong></th>
<th>Displays the VLAN interface (1-4094) for each entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Displays the description configured each NAT entry configured in the Configuration &gt; Access Points edit screen.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Displays the IP Address for each configured NAT interface.</td>
</tr>
<tr>
<td><strong>NAT Enable</strong></td>
<td>Displays if the <em>Network Address Translation</em> (NAT) is enabled on the selected LAN interface. NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The Access Point's router maps its local (Inside) network addresses to WAN (Outside) IP addresses and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address.</td>
</tr>
</tbody>
</table>
Wireless

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one wireless controller connected Access Point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs are mapped to radios on each connected Access Point. A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

Periodically refer to the *Wireless* screen to monitor an Access Point's WLAN utilization and whether WLAN usage is consistent with an Access Point's deployment objective and the security needs of its connected clients.

To configure WLAN properties to be complimentary with Access Point deployment objectives and client support needs:

1. Select **Configuration** settings from the main menu then select **Wireless**.

The *Wireless* screen is partitioned into **Radio Settings**, **Wireless LAN** and **MeshConnex** fields.
Note: Changes made to an Access Point's Configuration are pushed (provisioned) to up to 24 managed Access Points of the same model.

2 Configure the following **Radio Settings** for the 2.4Ghz and 5Ghz radios on the Access Point:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Use the drop-down menu to select an operational mode of either 2.4Ghz or 5Ghz.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>Use the drop-down menu to select a channel for the 2.4Ghz or 5Ghz radio. Point. To enable automatic channel selection based on RF conditions, select <em>Smart</em> from the drop-down menu. The channels available for configuration are channels for which the product is approved in its selected country. The professional installer must ensure the product is set to operate under conditions, and on channels, approved by country regulations.</td>
</tr>
<tr>
<td>Power</td>
<td>Specify a radio power for the 2.4Ghz or 5Ghz radio or select Smart to let the Access Point manage the power settings based on network conditions. Selecting Smart as the Power setting automatically configures radio power to not exceed the maximum power allowed by the defined country. For static power settings, the professional installer must ensure the configured power levels are compliant with local and regional regulations. The county selected automatically limits the maximum output power that can be set.</td>
</tr>
<tr>
<td>Gain</td>
<td>Set the antenna gain between 0.00 - 15.00 dBi. The Access Point’s <em>Power Management Antenna Configuration File</em> (PMACF) automatically configures the radio transmit power based on antenna type, antenna gain (provided here) and the deployed country’s regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. The default value is 0.00. For external antenna model Access Points, configure the Antenna Gain based on the antenna used in the deployment. The set gain value should include the antenna gain, along with any additional components, such as extension cables used between the Access Point and the antenna.</td>
</tr>
</tbody>
</table>

3 To add a new WLAN select **+Add**, to edit an existing WLAN click the name of the WLAN. To remove an existing WLAN highlight it and select **Delete**.
The Wireless LAN Edit screen displays.

Wireless LAN Edit Screen

4 In the **Wireless LAN** section specify the following information for each WiNG Express managed WLAN:

<table>
<thead>
<tr>
<th><strong>Wireless LAN Section</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name:</strong> Add or edit a name for the WLAN. This name is used throughout the WiNG Express user interface as network identifier.</td>
<td></td>
</tr>
<tr>
<td><strong>Enable:</strong> Displays a green check mark if the WLAN (and all its unique configuration attributes) is enabled for Access Point utilization and a red X if the WLAN is disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>SSID:</strong> Specify the WLAN's SSID. The WLAN SSID is case sensitive and alphanumeric. SSID length should not exceed 32 characters.</td>
<td></td>
</tr>
<tr>
<td><strong>Client-To-Client Communications:</strong> Select this option to enable client to client communication within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is also disabled on that WLAN, clients are not permitted to interoperate.</td>
<td></td>
</tr>
</tbody>
</table>

---

**WLAN Rate Limit**

**Enable:**
- Per-Client: (0-1,000,000) Kbps
- Aggregate (WLAN): (0-1,000,000) Kbps

**Other Settings**

- **Client Ream Assist:**
- **Voice VLAN:**
| **Security** | Displays the WLAN Authentication type. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information. 

The screen displays with the Open option selected. Naming and saving such a policy (as is) would provide no security and might only make sense in a network wherein no sensitive data is either transmitted or received. This default setting is not recommended. 

If selecting Secure-PSK, select an encryption type for the WLAN. Define whether the key is entered in ASCII or HEX characters. Selecting Show to expose the key is not recommended. 

If selecting Secure-802.1x, provide an IP address (or hostname) and a shared secret (password) used to access an external RADIUS server resource designated to validate user requests to the Access Point’s WLAN resources. 

Selecting Guest displays fields for captive portal Web page creation, and is beyond the scope of this basic Access Point configuration. |
| **Band** | Select a band, 2.4Ghz or 5Ghz (if supported), to enable operation of that band on the WLAN. |
| **VLAN** | Use the spinner control to specify a VLAN from 1 - 4,094 for this WLAN. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. Do not use VLAN 1 with the WLAN if the WAN port has been enabled. |
| **Description** | Optionally, enter descriptive text which can be used by administrators to help identify each WLAN. |
Encryption (Secure-PSK only)

When Secure-PSK security is selected, use the drop-down menu to select an encryption type. Available encryption types include:

**WEP-64** - *Wired Equivalent Privacy* (WEP) is a security protocol specified in the Wi-Fi standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP can be used with open, shared, MAC and 802.1X EAP authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication. WEP 64 uses a 40 bit key concatenated with a 24-bit *initialization vector* (IV) to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP is only recommended when clients are incapable of using more robust forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

**WEP-128** - WEP 128 uses a 104 bit key which is concatenated with a 24-bit *initialization vector* (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys. WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.

**TKIP-CCMP** - CCMP is a security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result. The encryption method is *Temporal Key Integrity Protocol* (TKIP). TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check and an extended initialization vector. However, TKIP also has vulnerabilities.

**WPA2-CCMP** - WPA2 is a 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result. WPA2/CCMP is based on the concept of a *Robust Security Network* (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any a controller, service platform or Access Point provides for its connected clients.
When Secure-PSK security is selected, enter an encryption key. For WEP-64 and WEP-128 enter a 4 to 32 character Pass Key and click the **Generate** button. The pass key can be any alphanumeric string. Controllers, service platforms, Access Points and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. For TKIP-CCMP and WPA2-CCMP, enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

5 In the **WLAN Rate Limit** section configure the following settings:

**Enable (Per-Client)**
Select this option to enable WLAN Rate limiting on a per client basis. Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Once enabled configure the value in the per-client field.

**Per-Client**
If per-client WLAN rate limiting is enabled, use the spinner controls to configure the per-client data rate limit between 50 to 1,000,000 kbps. Maximum data speed is limited to the configuration rate.

**Enable (Aggregate WLAN)**
Select this option to enable WLAN Rate limiting for the WLAN as a whole. Once enabled configure the value in the aggregate field.

**Aggregate (WLAN)**
If aggregate WLAN rate limiting is enabled, use the spinner controls to configure the WLAN aggregate data rate limit between 50 to 1,000,000 kbps. The collective data rate for all clients on the WLAN is limited the configured rate.

6 In the **Other Settings** section configure the following settings:

**Client Roam Assist**
Select this option to enable client roam assist. By constantly monitoring a client's packets and the received signal strength indicator (RSSI) of a given client by a group of Access Points, decision can be made on the optimal Access Point to which the client needs to roam. Then forcefully direct the client to the optimal Access Point.

**Voice VLAN**
Select this option to enable a dedicated voice VLAN for the WLAN. If enabled voice traffic will be tagged with with this VLAN.
To view and configure mesh wireless settings select the MeshConnex tab.

### Name
Displays the names of configured mesh points. Mesh points are Access Points dedicated to mesh network support. Mesh networking enables users to access broadband applications anywhere (including moving vehicles).

### Enable
Specifies the status of each configured mesh point, either Enabled or Disabled.

### Mesh ID
Displays the IDs (mesh identifiers) assigned to mesh points as unique numeric identifiers.

### Control VLAN
Displays the VLAN (virtual interface ID) for the control VLAN on each of the configured mesh points.

### Allowed VLANs
Displays the list of VLANs allowed on each of the configured mesh points.

### Security Mode
Displays the security for each of the configured mesh points. The field will display None for no security or PSK for pre-shared key authentication.
To add a mesh point, select **+Add** and configure the following:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Wireless LAN</th>
<th>+MeshConnect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Enable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mesh ID</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allowed VLANs</strong></td>
<td>1 (1,5,6,8,9,12,...) range: 1-4094</td>
<td></td>
</tr>
<tr>
<td><strong>Radio Bands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allowed Channel Lists</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table: Configuration Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the new mesh point. The name should be descriptive to easily differentiate it from other mesh points. This field is mandatory.</td>
</tr>
<tr>
<td>Enable</td>
<td>Toggles the status of a mesh point on or off. To enable a mesh point, select this option.</td>
</tr>
<tr>
<td>Mesh ID</td>
<td>Specify a mesh identifier for this mesh point. This field is optional.</td>
</tr>
<tr>
<td>Security</td>
<td>Select a security authentication mode for the mesh point. Select <em>none</em> to have no authentication for the mesh point. Select <em>PSK</em> to set a pre-shared key as the authentication for the mesh-point. If PSK is selected enter a pre-shared key in the <em>Key Settings</em> section below. Select EAP to use 802.1X EAP. The certificate should be issued from an Enterprise or public certificate authority to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials.</td>
</tr>
<tr>
<td>Allowed VLANs</td>
<td>Specify the VLANs allowed to pass traffic on the mesh point. Separate all VLANs with a comma. To specify a range of allowed VLANs separate the starting VLAN and the ending VLAN with a hyphen.</td>
</tr>
<tr>
<td>Radio Band</td>
<td>Select to enable 2.4 GHz and 5.0 GHz radio bands for the mesh point. Unselecting a radio band will disable it for the mesh point.</td>
</tr>
<tr>
<td>Allowed Channel List</td>
<td>Selecting this option enables dynamic update of a channel list for the mesh point.</td>
</tr>
</tbody>
</table>
Security

When protecting wireless traffic to and from an Access Point, an administrator should not lose sight of the security solution in its entirety, since the chain is as weak as its weakest link. Zebra Access Points provide seamless data protection and user validation to protect and secure data at each vulnerable point in the Access Point managed network. Zebra Access Points support a Layer 2 wired/wireless firewall and Wireless Intrusion Protection System (WIPS) capabilities, while additionally strengthened with a premium multi-vendor overlay security solution from Air Defense with 24x7 dedicated protection. This security is offered at the most granular level, with role, location and device categorization based network access control available to users based on identity as well as the security posture of the client device.

Firewall

A firewall is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the Access Point managed network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. Firewalls implement uniquely defined access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value, and in fact could provide a false sense of network security.

With Zebra Access Points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing an Access Point's managed wireless clients. Well designed firewalls block traffic from outside the network, but permit authorized users to communicate freely with outside the network. All messages entering or leaving an Access Point pass through the firewall, which examines each message and blocks those not meeting the security criteria (rules) defined.

Firewall rules define the traffic permitted or denied within the network. Rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set. For example, if the packet stream meets all conditions, traffic is permitted, authenticated and sent to the destination device.

To configure Firewall rules:
1. Select Configuration from the main menu. Select Security, then Firewall.
   The firewall screen is divided into WLAN ACL Rules and Wireless Client Association ACL Rules fields.

**Note:** Changes made to an Access Point's Configuration are pushed (provisioned) to up to 24 Access Points of the same model.

2. Set the following WLAN ACL Rules:

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Specify or modify a precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select a firewall rule’s Enable or Disable icon to determine this rule’s inclusion with the IP firewall policy.</td>
</tr>
</tbody>
</table>
### Action

Every IP firewall rule is made up of matching criteria rules. The action defines what to do with a packet if it matches the specified criteria. The following actions are supported:

* **Deny** - Instructs the firewall to stop a packet from its destination.

* **Permit** - Instructs the firewall to allow a packet to proceed to its destination.

### Source IP

Determine whether filtered packet source for this IP firewall rule do not require any classification (any), are designated as a set of configurations consisting of protocol and port mappings (an alias), set as a numeric IP address (host) or defined as network IP and mask.

### Destination IP

Determine whether filtered packet destinations for this IP firewall rule do not require any classification (any), are designated as a set of configurations consisting of protocol and port mappings (an alias), set as a numeric IP address (host) or defined as network IP and mask. Selecting alias requires a destination network group alias be available or created.

### Protocol

Define the access protocols impacted by the WLAN's ACL rule configuration.

### Direction

Specify the direction for ACL rule.

### Interface

Specify the interface for the WLAN ACL rule to affect.

---

3. Set the following **Wireless Client Association ACL Rules**:

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Specify or modify a precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>Every IP firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>* <strong>Deny</strong> - Instructs the firewall to stop a packet from its destination.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Permit</strong> - Instructs the firewall to allow a packet to proceed to its destination.</td>
</tr>
<tr>
<td><strong>Source MAC</strong></td>
<td>Specify the source MAC address or network group configuration used as basic matching criteria for this ACL rule. The source MAC ensures only an authenticated endpoint is allowed to send traffic.</td>
</tr>
<tr>
<td><strong>End MAC</strong></td>
<td>Specify the destination MAC address or network group configuration used as basic matching criteria for this ACL rule. The end MAC represents the destination MAC address of the packet examined for matching purposes and potential device exclusion.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Use the drop-down menu to specify the interface configurations impacted by the ACL's rule configuration.</td>
</tr>
</tbody>
</table>
WIPS

Zebra Access Points can utilize the *Wireless Intrusion Protection Systems* (WIPS) to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. WIPS is supported through the use of dedicated sensor devices designed to actively detect and locate unauthorized Access Points. Upon detection, they use mitigation techniques to block the devices by manual termination or air lockdown.

Unauthorized APs are untrusted Access Points connected to a LAN accepting client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured Access Points that do not adhere to corporate policies. An attacker can install an unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a *man-in-the middle* attack or assume control of wireless clients to launch denial-of-service attacks.

Zebra Access Points support unauthorized AP detection, location and containment natively. A WIPS server can alternatively be deployed (in conjunction with the Access Point) as a dedicated solution within a separate enclosure. When used within a network and its associated Access Point radios, a WIPS deployment provides the following enterprise class security management features and functionality:

♦ *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the Access Point managed wireless network.

♦ *Rogue Detection and Segregation* - A WIPS supported Access Point distinguishes itself by both identifying and categorizing nearby Access Points. WIPS identifies threatening versus non-threatening Access Points by segregating Access Points attached to the network (unauthorized APs) from those not attached to the network (neighboring Access Points). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of neighboring Access Points to isolate the few attached to the network.

To configure *Wireless IPS*:

1. Select *Configuration* from the main menu. Select *Security*, then *Wireless IPS*.
2. Select *Enable Rogue AP Detection* to allow the detection of unauthorized (unsanctioned) devices from this WIPS policy.
3 Select **Off-Channel Scan** to scan across all channels using this Access Point's radio. Channel scans use Access Point resources and can be time consuming, so only enable when you're sure the radio can afford bandwidth be dedicated to the channel scan and does not negatively impact client support.

**Note:** Changes made to an Access Point's Configuration are pushed (provisioned) to up to 24 Access Points of the same model.

4 Review the following **Wireless IPS** event information:

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Displays the rogue AP event type detected by the sensor. Several different event types can occur:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An <em>Excessive Action Event</em> is an event where an action is performed repetitively and continuously. DoS attacks come under this category.</td>
</tr>
<tr>
<td></td>
<td><em>MU Anomaly Events</em> are suspicious events by wireless clients that can compromise the security and stability of the network.</td>
</tr>
<tr>
<td></td>
<td><em>AP Anomaly Events</em> are suspicious frames sent by neighboring APs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reporting AP</th>
<th>Displays the hardware encoded <em>Media Access Control</em> (MAC) address of the Access Point reporting the listed WIPS event.</th>
</tr>
</thead>
</table>

| Originating Device       | Displays the MAC address of the AP which triggered the reported event. Review this address carefully to validate whether this is a known and network approved Access Point or if this Access Point is unauthorized and could jeopardize network security, and consequently warrants quarantine. |
**Detector Radio**

Displays the radio number of the detecting Access Point reporting the event. AP6511E and AP6521E model Access Points are single radio devices, other supported Access Points are dual radio models.

**Time Reported**

Displays the date and time stamp for each WIPS event reported.

---

**DHCP**

*Dynamic Host Configuration Protocol (DHCP)* allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside.

To configure DHCP **Services**:

1. Select **Configuration** from the main menu. Select **Services**. The **DHCP Settings** screen displays.

2. Select **Enable DHCP Server** to assign IP addresses to requesting wireless clients. Enabling DHCP allows the Access Point's onboard DHCP server resource to provide IP and DNS information to requesting clients on the LAN interface.

3. If the DHCP server is enabled, configure the following settings:

   - **Interface**: Use the drop-down menu to select an interface for the DHCP server. Supported Access Points have the following interface availability:
     - **AP6511E** - FE1, FE2, FE3, FE4, UP1
     - **AP6521E** - GE1/POE (LAN)
     - **AP6522E** - GE1/POE (LAN)
     - **AP6562E** - GE1/POE (LAN)
     - **AP7502E** - GE1, FE1, FE2, FE3
     - **AP7522E** - GE1/POE (LAN)

   - **IP**: Specify the IP mask for each entry in the DHCP server. Applying a subnet mask to an IP address separates the address into a host address and an extended network address. Subnets can improve network security and performance by organizing hosts into logical groups.

   - **Default Gateway**: Enter the IP address of the network's default gateway. A default gateway provides an entry/exit point for the network, as it commonly connects an internal network to an external network.
Primary DNS | Enter an IP Address for the main DNS server resource for the Access Point's WAN interface.
---|---
Secondary DNS | Enter an IP Address for the backup (secondary) Domain Name Server providing DNS services for the Access Point's WAN interface.
Start IP | Enter the starting IP Address for each DHCP address pool range configured. Ensure the range is large enough to meet the needs of requesting clients.
End IP | Enter the ending IP Address for each DHCP address pool range configured. Ensure the range is large enough to meet the needs of requesting clients.
Lease Time (days) | If a lease time has been defined for a listed network pool, it displays in an interval in days. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client.
Lease Time (hours) | If a lease time has been defined for a listed network pool, it displays in an interval in hours. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client.
Lease Time (minutes) | If a lease time has been defined for a listed network pool, it displays in an interval in minutes. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another requesting DHCP client.

**Services**

**RADIUS**

An Access Point's RADIUS server allows the configuration of user groups with common user policies associated to them. User group names and associated users are stored in the Access Point's local database. The user ID in the received access request is mapped to the associated wireless group for authentication.

To view RADIUS configurations:

1. Select **Configuration** tab from the main menu.
2. Select the **Services** tab from the **Configuration** menu.
   The upper pane of the user interface displays the **DHCP** and **RADIUS** options.
3 Select RADIUS.

4 Select Enable Radius Server to activate the internal RADIUS server.

5 Select Start Radius Server to start the RADIUS service on the AP.

6 Review the following RADIUS group configuration information. To create a new RADIUS group click + Add. To remove an existing group or groups, select them from the table and click Delete.

<table>
<thead>
<tr>
<th>RADIUS Group</th>
<th>Displays the group name or identifier assigned to each listed group when it was created. The name cannot exceed 32 characters or be modified as part of the group edit process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest User Group</td>
<td>Select to enable RADIUS access to the guest user group with the settings outlined in this section.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Displays the VLAN ID used by the group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the controller managed network (once authenticated by the local RADIUS server).</td>
</tr>
<tr>
<td>WLAN SSID</td>
<td>Displays the Service Set ID (SSID) of the network to which the Access Point belongs to.</td>
</tr>
<tr>
<td>Rate limit from air</td>
<td>Specify the maximum data rate in kbps between 100 and 1,000,000 for traffic originating on the wireless network.</td>
</tr>
</tbody>
</table>
7 Review the following RADIUS schedule information and modify as needed:

<table>
<thead>
<tr>
<th>Access by time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>When Access by Time is enabled, specify the starting time users within each listed group can access local RADIUS resources.</td>
</tr>
<tr>
<td>End Time</td>
<td>When Access by Time is enabled, specify the starting time users within each listed group lose access to the local RADIUS resources.</td>
</tr>
</tbody>
</table>

8 When adding or editing a RADIUS user, verify and configure the following:

<table>
<thead>
<tr>
<th>User ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the name or identifier assigned to each user when it was created. The name cannot exceed 32 characters or be modified as part of the edit process.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guest User</th>
<th>Select to enable RADIUS access using the guest user group with this user.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Use the pull-down menu to select which group to associate with the RADIUS user.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Email ID</th>
<th>Specify an e-mail address for the RADIUS user. This can be a local e-mail address or a fully qualified e-mail address.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Specify the telephone number associated with the RADIUS user. This is an optional field.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Start Date / Start Time</th>
<th>Specify a starting date and time when this RADIUS user will be activated.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Expiry Date / Expiry Time</th>
<th>Specify an end date and time when this RADIUS user will be deactivated.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Access Duration</th>
<th>Specify how long the RADIUS user will be active by selecting an access duration. To allow the use of the Expiry Date and Expiry Time fields select the Till Expiry option. To specify a duration of time the account will be active, specify a duration in Days:Hours:Minutes format. The RADIUS user will be deactivated once the set duration has passed.</th>
</tr>
</thead>
</table>
Management

Zebra Access Points have mechanisms to allow/deny access for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled/disabled as required for unique policies. This access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

To enhance security, administrators can apply various restrictions as needed to:

- **Restrict SNMP and Web UI access to specific hosts or subnets**
- **Disable un-used and insecure interfaces as required within managed access profiles.** Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices
- **Provide authentication for management users**
- **Apply access restrictions and permissions to management users**

Management restrictions should be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical Access Point resources. Management restrictions can also be applied to reduce the Access Point’s attack footprint when guest services are deployed.

To configure the Access Point’s management settings:

1. Select **Configuration** settings from the main menu then select **Management**.

   - **Administrator** section:
     - **Change User Password**
   - **Access** settings:
     - **HTTP**
     - **HTTPS**
     - **Telnet**
     - **SSH**
   - **Syslog Server**
     - **Logging**
     - **Logging Level**
     - **Server IP**
   - **SNMP Settings**
     - **Enable SNMPv1**
     - **Enable SNMPv2c**
     - **Enable SNMPv3**
   - **SNMP v3 Users**
     - **Username**
     - **Password**
     - **Authentication**
     - **Encryption**
   - **SNMP Traps**
     - **Trap Generation**
     - **IP Address**
     - **Port**
     - **Version**

The Management screen is partitioned into Administrator, Access, Syslog Server, SNMP Settings and SNMP Traps fields.

**Note:** Changes made to an Access Point’s Configuration are pushed (provisioned) to up to 24 Access Points of the same model.

2. In the **Administrator** section, select **Change User Password** to change the default administrator login password to something more proprietary and secure.

3. Set the following **Access** settings:

   | **HTTP** | Select the checkbox to enable HTTP device access. HTTP provides limited authentication and no encryption. |

---
HTTPS
Select the checkbox to enable HTTPS device access. HTTPS (Hypertext Transfer Protocol Secure) is more secure than HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication (as is the case with HTTP).

Telnet
Select the checkbox to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but does provide a measure of authentication. Telnet access is disabled by default.

SSHv2
Select the checkbox to enable SSH device access. SSH (Secure Shell) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.

4 In the Syslog Server section configure the following settings:

<table>
<thead>
<tr>
<th>Logging</th>
<th>Select this option to log system events to a log file or a syslog server. Selecting this option enables the rest of the parameters required to define the Access Point’s logging configuration. This option is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Level</td>
<td>Event severity coincides with the syslog logging level defined for the Access Point. Assign a numeric identifier to log events based on criticality. Severity levels include 0 - Emergency, 1 - Alert, 2 - Critical, 3 - Errors, 4 - Warning, 5 - Notice, 6 - Info and 7 - Debug. The default logging level is 4.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Enter the IP addresses where logged system events can be sent on behalf of the event generating Access Point.</td>
</tr>
</tbody>
</table>

5 Set the following SNMP Settings:

| Enable SNMPv1 | SNMP v1 exposes a device’s management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified as text strings, with version 1 being the original (rudimentary) implementation. SNMPv1 is disabled by default. |
| Enable SNMPv2 | Select the checkbox to enable SNMPv2 support. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPv2 is enabled by default. |
| Enable SNMPv3 | Select the checkbox to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default. |
SNMP v1/v2
Community String:
Access Control

Set the access permission for each community string used to retrieve or modify information. Available options include:

*Read Only* - Allows a remote device to retrieve information.

*Read-Write* - Allows a remote device to modify settings.

SNMPv3 Users:
User Name

Use the drop-down menu to define a user name of *snmpmanager*, *snmpoperator* or *snmptrap*.

SNMPv3 Users:
Password

Provide the user's password in the field provided. Select the *Show* check box to display the actual character string used in the password, while leaving the check box unselected protects the password and displays each character as "*".

SNMPv3 Users:
Authentication

Select the user authentication type used with the listed SNMPv3 user. The selected authentication scheme ensures only trusted users can utilize Access Point network resources.

SNMPv3 Users:
Encryption

Select the encryption scheme used with the listed SNMPv3 user. The selected encryption scheme ensures only trusted devices can utilize Access Point network resources.

6 In the SNMP Traps section configure the following:

<table>
<thead>
<tr>
<th>Trap Generation</th>
<th>Select the <em>Trap Generation</em> checkbox to enable trap generation using the trap receiver configuration defined. This feature is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Sets the IP address of an external server resource dedicated to receive SNMP traps on behalf of the Access Point.</td>
</tr>
<tr>
<td>Port</td>
<td>Set the virtual port of the server resource dedicated to receiving SNMP traps. The default port is port 162.</td>
</tr>
<tr>
<td>Version</td>
<td>Sets the SNMP version to send SNMP traps. SNMPv2c is the default.</td>
</tr>
</tbody>
</table>

**Access Points**

Individual Access Points can be selected and their configurations customized as required to better support the deployment objective of the network.

To review Access Points:

1. Select **Access Points** from the main menu.

The **Access Points** screen displays information about managed Access Points.

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Status</th>
<th>IP Address</th>
<th>2.4 GHz</th>
<th>5 GHz</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODEL-AP1000G</td>
<td>- (online)</td>
<td>192.168.13.21</td>
<td>4x116</td>
<td>4x116</td>
<td>5.7.0.0-480R</td>
</tr>
</tbody>
</table>

2. The **Managed Access Points** section displays the following for each Access Point:
### AP Name
Displays the administrator assigned Access Point name. Names can be revised using the Edit menu.

### AP Status
Displays the active state of each listed Access Point. If an Access Point is up, two green up arrows are displayed. If an Access Point is down two green down arrows display.

### IP Address
Displays the current IP Address assigned to each Access Point as its network identifier. IPv6 formatted IP addresses are not supported, and the IP address is in an IPv4 format.

### 2.4GHz Channel
Displays the current radio channel number set for the 2.4 GHz radio on each managed Access Point. AP6511E and AP6521E Access Points are single radio models, the other support Access Points are dual radio models.

### 2.4 GHz Power
Displays the 2.4 GHz radio's current power level in dBm. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function.

### 5 GHz Channel
Displays the current radio channel number for the 5 GHz radio, if applicable, on each managed Access Point. AP6511E and AP6521E Access Points are single radio models, and will not display information channel information for a second radio.

### 5 GHz Power
Displays the 5 GHz radio's current power level in dBm. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function.

### Firmware
Displays the full version number of the active firmware on each listed Access Point. Periodically compare the Access Point's firmware version against the latest version available on the Support site to help ensure the Access Point is deployed with the most recent firmware, providing the most recent feature set.

### To access advanced Access Point options, select an AP or multiple APs from the Managed Access Points section and select the Tools drop-down menu. The following tools are available:

#### Factory-Default
Selecting **Factory-Default** displays a prompt confirming you want to reset the device to factory defaults. Selecting **Yes** will reset the device to factory default settings and will reboot the device. Choosing this option will erase all information and settings stored on the device. Selecting **No** will cancel the reset and return to the Access Point screen.

#### Reboot
Selecting **Reboot** displays a prompt confirming you want to reboot the device. Selecting **Yes** will reboot the device and the user interface will be unavailable until the device has rebooted. You will be required to log in to the user interface once the devices has finished rebooting. Selecting **No** will cancel the reboot and return to the Access Point screen.
### Upgrade

Selecting *Upgrade* displays the Device Upgrade page. If *Basic* is selected, enter the URL for the upgrade firmware in the following format:

**URL Syntax:**
- `tftp://<hostname/IP>[:port]/path/file`
- `ftp://<user>:<passwd>@<hostname/IP>[:port]/path/file`

If *Advanced* is selected, configure the Protocol, Port, Hostname or IP Address, Username, Password and the path for the firmware file. Firmware upgrades are supported via the FTP, TFTP and HTTP protocols.

### Tech-Support

Selecting *Tech-Support* displays the Copy Tech Support screen where system information and logs can be transferred to technical support by configuring the Protocol, Port, Hostname or IP Address, Username, Password and the path for the tech support server. Transfer of this information is supported via FTP, TFTP and HTTP protocols. It will be nice to mention that the techsupport filename is auto generated by the device based on the device mac address, passing file name in path results in failure.

### Export / Import Config

Selecting *Export / Import Config* displays a screen where configuration files can be imported to or exported from the device. When *Local* is selected the start-up system configuration file is displayed as plain text in a window. To import a new configuration using this method, erase the contents of the configuration window and paste the contents of a new configuration file into the window. When all changes are complete, click the import button to import the new configuration file onto the device. To export a configuration file and *Local* is selected, simply copy the contents of the configuration window and paste it into a text file on your local system. Configuration files can also be imported from or exported to remote systems. To use this select *Remote* and specify the Protocol, Port, Hostname or IP Address, Username, Password and the path for the remote server. Transfer of this information is supported via FTP, TFTP and HTTP protocols.

### Locator ON

Selecting *Locator ON* will start flashing the Access Point’s LEDs to make it easier to find in large deployments.

### Locator OFF

Selecting *Locator OFF* will stop flashing the LEDs if they have been set to flash using the *Locator ON* option.

### Delete Offline Devices

Use this option to delete offline APs from the system. The Access Point must first be offline before it may be deleted.
4 To edit an Access Point's settings, click on the AP Name of the Access Point you wish to edit. The edit screen displays.

5 Refer to the following device information in Basic Settings:

| **AP Name** | Displays the unique name assigned to the Access Point. This name can be changed on this screen or the Configuration > Basic screen. |
| **Location** | Displays the location name configured on the Configuration > Basic screen. |
| **Version** | Displays the currently active firmware version running on the Access Point. |
| **Model** | Displays the device model number for the Access Point. |
| **Up Time** | Displays the amount of time in days, hours and minutes since the last time the device rebooted. Use this information to determine whether a newer firmware version is available potentially providing an enhanced feature set. |

6 Configure the following options for Wireless Settings:

| **2.4GHz Channel / Power** | Use the drop-down menu to select a channel for the 2.4GHz radio on the Access Point. AP6511E and AP6521E Access Points are single radio version models. Set the transmit power of the selected Access Point radio. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the Smart option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 0 dBm, Smart RF, is the default value. |
If applicable, use the drop-down menu to select a channel for the Access Point's 5GHz radio. All model Access Points support a second radio, with the exception of single radio model AP6511E and AP6521E Access Points. If using a dual radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the Smart option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 0 dBm, Smart RF, is the default value.

7 On supported devices select Enable RADIUS Server to enable the onboard RADIUS server. RADIUS settings can be configured on the RADIUS Screen.

8 Optionally, from the LAN IP Interface Settings section Add, Edit or Delete LAN Settings for the Access Point. When adding and editing settings specify the following:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Use the drop-down menu to select an Access Point interface to connect to the LAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description for each LAN interface configured to distinguish it from other LAN configurations with similar attributes.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter or edit the IP Address associated with each LAN interface. To edit the IP Address click the edit icon next to the corresponding interface.</td>
</tr>
</tbody>
</table>

9 To view more information about the Access Point, click Details.

10 To return to the Access Points screen click << Go Back.
The Event History screen displays historical Access Points events. Events can be filtered by using criteria in the search field.

In This Chapter

Event History ............................................................. 61

Event History

Events can be filtered by using criteria in the search field.

To review the event history:
1. Select Event History from the main menu.

2. Review the following event data to determine the severity of specific events and the devices reporting them:

<table>
<thead>
<tr>
<th>Time</th>
<th>Module</th>
<th>Message</th>
<th>Severity</th>
<th>Source</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-01-01</td>
<td>SYSTEM</td>
<td>User &quot;admin&quot; from 192.168.11.1 authenticated successfully</td>
<td>notice</td>
<td>FC-0A-01-42-89-6C</td>
<td>46521-42593C</td>
</tr>
<tr>
<td>2014-01-01</td>
<td>SYSTEM</td>
<td>User &quot;admin&quot; from 192.168.11.1 authentication failed</td>
<td>error</td>
<td>FC-0A-01-42-89-6C</td>
<td>46521-42593C</td>
</tr>
<tr>
<td>2014-01-01</td>
<td>SYSTEM</td>
<td>Successfully locked user &quot;admin&quot; with privilege &quot;superuser&quot; from fiber optic cable</td>
<td>notice</td>
<td>FC-0A-01-42-89-6C</td>
<td>46521-42593C</td>
</tr>
<tr>
<td>2014-01-01</td>
<td>SYSTEM</td>
<td>Failed Start/Stop/Recover, reset command issued from CLI (user admin)</td>
<td>notice</td>
<td>FC-0A-01-42-89-6C</td>
<td>46521-42593C</td>
</tr>
<tr>
<td><strong>Timestamp</strong></td>
<td>Displays the timestamp (time zone specific) when the displayed event message was generated. Use this information to help assess whether the listed timestamp coincides with any known issue impacting the network.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Module</strong></td>
<td>Displays the Access Point module (resource) detecting, reporting and tracking the event. Events detected by other modules are not tracked.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Message</strong></td>
<td>Displays error or status messages for each event listed. Use the message text as an additional means of assessing an event's potential impact to the Access Point.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>All Severities</em> – All events are displayed irrespective of their severity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Critical</em> – Only critical events are displayed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Error</em> – Only errors and above are displayed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Warning</em> – Only warnings and above are displayed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Informational</em> – Only informational and above events are displayed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Displays the hardware encoded MAC address of the source device tracked by the selected module.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>Displays the administrator assigned name of the source device tracked by the listed module.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Use the **Search** field as necessary to refine event history to specific criteria.
4. Select **Clear All** to erase the existing event logs.
5. Select **Stop** to stop automatic updating of the event history logs.
6. Select **Refresh** to manually update the event history logs. If you have selected **Stop** select refresh to re-enable automatic updating.
Support Center

If you have a problem with your equipment, contact support for your region. Support and issue resolution is provided for products under warranty or that are covered by a services agreement. Contact information and Web self-service is available by visiting www.zebra.com/support.

When contacting support, please provide the following information:
♦ Serial number of the unit
♦ Model number or product name
♦ Software type and version number

Support responds to calls by email or telephone within the time limits set forth in support agreements. If you purchased your product from a business partner, contact that business partner for support.

Customer Support Web Site

The Support Web site, located at www.zebra.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Manuals

www.zebra.com/docs