Avaya WLAN 8100 Planning and Engineering

1.0.0.0
NN47251-200, 01.01

August 20, 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: About the WLAN 8100 Solution

The Avaya WLAN 8100 solution consists of two primary elements, the WLAN Controller 8180 and Access Point 8120. This section contains an overview of these items as well as other elements of the overall solution. This section contains the following topics:

Access points

The Avaya 8100 WLAN system supports a centralized WLAN architecture that consists of a large number of access points (AP) controlled and managed by one or more wireless controller switches (WCS). The WCS and AP communicate through a proprietary CAPWAP protocol.

This section describes the features provided by APs.

AP configuration profile

You can manage the configuration of controlled-APs through the use of configuration profiles. There can be several profiles defined on the Wireless Controller. You can apply each profile across multiple controlled-APs. A profile is configured in the same manner as a standalone AP. An existing profile and all of its configurations can be copied to another profile or used to create a new profile.

There are 16 virtual access points (VAP) available for each radio and each VAP is configured with a network. A new configuration profile has all of the VAPs configured on each radio interface assigned to the default network configurations. VAP1 is always assigned to the BSSID of the physical radio interface, it is enabled by default and you can modify its network assignment, but you cannot disable it. In order to disable VAP1, you must turn the radio off. VAP2 through VAP16 are disabled by default, you can enable and assign each of these to any network. You cannot assign the same network to more than one VAP on the same radio.

VAP network configuration

You can manage the networks available on the WLAN by modifying or adding network configurations. The network configuration includes SSID, VLAN, security, and tunneling parameters and can be applied to one or more VAPs within the AP configuration profiles.

Multiple networks can have the same SSID.

Default network configurations are applied to VAP0 through VAP31 when a new AP configuration profile is created (one default network configuration exists per VAP ID). The

default network configurations can be modified, but not deleted, and the user can add new network configurations. All of the default networks are configured with open authentication and assigned to the default VLAN 1. The default VLAN is used if Radius based authentication is not configured for the network or the Radius server does not return a VLAN for a specific client.

AP configuration changes

The administrator configures the wireless controller over the management plan. The wireless controller pushes the configuration to its APs.

The AP configuration profile is applied to a controlled AP (in other words, the entire configuration profile is sent to the AP) when the AP initially transitions to controlled mode, when the AP is reset, when the user requests an apply action for its associated profile through the UI, and when the health monitoring process initiates it. A configuration profile can always be edited, regardless of whether or not the profile is currently applied to one or more controlled-APs. Therefore the administrator must request a profile apply when ready to send the configuration changes to all controlled-APs associated with a modified profile. The administrator can also modify which profile is assigned to an AP.

AP firmware management

The Wireless Controller upgrades the AP application image. The AP operating system image is separated from the application image to reduce image size as well as to maintain stability of the system since most bug fixes and feature upgrades occur in the application code. The OS image shall be upgraded using the same procedure used for upgrading the application image

The Wireless Controller shall upgrade the AP boot loader image.

Fast BSS transition

Fast BSS Transition (FT), as described in IEEE 802.11r, reduces the length of time connectivity is lost between station transitions between APs within the same ESS and mobility domain.

The following FT protocols are defined for implementing the 802.11r functionality:

- FT protocol
- FT Resource Request Protocol

FT protocol is executed when the station makes a transition to a target AP and does not require a resource request prior to the transition.

The FT resource request protocol is executed when a station makes a transition to a target AP and requires resources to be available prior to transition.

Both protocols can be executed using the over the air method or the over the DSS method.

The fast BSS transition further defines a three level key hierarchy; PMK-R0, PMK-R1 and PTK. This key hierarchy allows a station to make transition between APs without the need to perform 802.1x authentication at every AP.

Two key holders, R0 Key Holder (R0KH) and R1 Key Holder (R1KH) are responsible for derivation of the different FT keys and key identifiers.

WEB and NNCLI interfaces can be used to configure the FT parameters such as FT protocols, FT methods, Mobility domain identifier, key lifetime, re-association deadline and key holder IDs.

Call admission control

The access category based call admission control (CAC) feature, as described in 802.11 and Wi-Fi Alliance WMM, makes decisions on whether a station request to create a traffic stream using ADDTS messages is admitted or rejected. The CAC supports access categories for voice, video, best effort and background.

The voice and video categories can be configured to be admission enforced. The Beacon of the AP advertises that the voice and video access categories are under admission control. Compliant stations note this and send an ADDTS message in order to gain admission for the sending and receiving of voice and video traffic. When an ADDTS message is received the network (AP and controller) evaluates the request based on the resources available and the request is either admitted or denied. A request is only admitted if its QoS constraints can be satisfied without jeopardizing the QoS constraints of existing calls in the network.

The network monitors the radio channel utilization on a per access category basis and uses this information to make the decision to admit a request or not. The user can configure a percentage of utilization reserved for voice traffic, a percentage of utilization reserved for video traffic, and a percentage of utilization that can be shared between voice and video.

Call admission control in a 802.11 network stops stations from overwhelming an AP, resulting in better quality for all users. With CAC, the system admits requests based on the measured real-time traffic load. If a large number of stations use very little bandwidth, additional requests may be admitted. Likewise, if only a few stations are using a lot of resources, the network cannot admit further requests.

Auto RF

To improve network performance of 802.11 radios the Wireless Switch can automatically adjust channel and power of the managed access points.

The administrator can also disable the channel and power algorithms and configure the AP to the desired channel and power.

Channel plan configuration is a global setting. Configuration is done separately for 2.4GHz and 5GHz bands. Channel plan adjustments can be either scheduled to run automatically or be administrator initiated.

Power adjustment configuration is a global setting. The WC enables the users to control AP power either manually or automatically.

AP profiles

The administrator provisions managed APs through AP profiles. Access point profiles are defined per AP Model taking into account the number of available radios.

An AP profile is a mapping of AP radio profiles to each AP radio for a given AP model.

Access point profiles are assigned to APs via the AP profile mapping table. There can be many defined AP profiles, and each profile can be applied across multiple managed APs.

There are AP models with one and two radios. Each radio in Access mode can service only one band at a time. Single radio APs can operate either in 2.4GHz or 5GHz band. Duald radio APs can service 2.4GHz and 5GHz bands; both radios can not operate in the same band. Radios can be individually disabled.

Access points are configured by applying AP profiles. AP profiles are defined on an AP model basis (per number of radios).

When an AP is discovered that does not have an AP profile mapping defined, it is assigned to the default AP profile. The default AP profile is always defined and cannot be deleted, but can be edited.

A profile configuration can be edited regardless of whether or not the profile is currently applied to one or more managed APs. The administrator requests a profile apply when ready to send the configuration changes to all managed APs associated with a modified profile.

The administrator can assign a different profile to an AP. This is done on an external RADIUS server, therefore the administrator resets the AP to apply the new profile. The AP can be reset through a command on the wireless switch or by power cycling the AP.

For configuration changes to the valid AP database to take effect for an AP that is actively being managed, the AP must be reset to reauthenticate to the WC.

AP profiles are used to define a common set of configuration parameters that can be defined and applied in bulk to multiple APs. Some parameters are intrinsically AP-specific and have to be applied individually to each AP. AP specific configuration depends on the AP model and includes the following:

- AP description and location string
- AP radio enabled/disable
- AP radio operating band and mode
- AP radio sentry mode setting
- AP radio WIPS countermeasures settings

AP configuration is defined for each individual AP. If Auto-RF is enabled so that AP power and channel settings are determined automatically, AP profiles can be applied to groups of APs instead of individually.

The AP-to-profile mappings can be defined either locally on a WC or on the RADIUS server. AP profile is assigned to an AP during initial AP association with the WC. You can assign a different profile to AP at run-time by an explicit admin command.

AP radio profiles

AP radio profiles group settings that can be applied to one of the AP radios. AP radio profiles are used to define global bulk AP radio configuration settings; they are not used to configure individual AP-specific parameters, such as radio power or channel. However, it is possible to define an AP radio profile that is only applied to a single radio.

The user assigns WNs to a radio profile. Up to 16 WNs can be assigned to a radio profile to match the maximum number of VAPs that one radio can expose. The default radio profile has only one WN assigned to it, which is the Default WN.

AP radio QoS

Enhanced Distributed Channel Access (EDCA) parameters of an AP affect downstream traffic from the AP to the client station. Station EDCA parameters affects upstream traffic from the client station to an AP. The user has control over enabling and disabling WMM mode. When it is disabled, QoS only applies to downstream traffic.

The following AP EDCA parameters can be configured for a radio interface per QoS Queue. These parameters affect downstream traffic from the AP to the client station:

- Queue 0 (voice), highest priority queue, minimum delay
- Queue 1 (video), highest priority queue, minimum delay
- Queue 2 (best effort), medium priority queue, medium throughput and delay
- Queue 3 (background), lowest priority queue, high throughput

The following station EDCA parameters can be configured for a radio interface per QoS Queue. When WMM mode is enabled, these parameters affect upstream traffic from the client station to the AP. The QoS Queues that can be configured are:

- Queue 0 (voice), highest priority queue, minimum delay
- Queue 1 (video), highest priority queue, minimum delay
- Queue 2 (best effort), medium priority queue, medium throughput and delay
- Queue 3 (background), lowest priority queue, high throughput

The administrator can configure the following scan operations modes on a radio:

- Access mode: Radio provides client access and monitors the RF activities on the operation channel. The scan results are reported to the managing WC. This is the Default mode.
- Access-WIDS mode: Radio provides client access and periodically leaves the operational channel to briefly scan other channels on its RF band of operation. The scan results are reported to the managing WC.
- WIDS Sentry mode: Radio does not provide client access, but is fully dedicated to RF environment scanning.
- WIPS Sentry mode: Radio does not provide client access, but is fully dedicated to RF environment scanning. It can also run RF countermeasure actions against the offending wireless units (both rogue APs and clients).

Wireless ARP suppression

Wireless ARP suppression enables the AP to reduce the number of broadcasted ARP requests on the wireless interface. AP supports the following mechanisms for reducing ARP broadcasts:

- ARP broadcast to unicast conversion
- ARP filtering

Image push to AP

The managing WCs distribute the AP images. The administrator manually initiates image updates to individual APs by specifying APs MAC address and the image name. The code images are stored on the WC flash.

WCS health monitoring at AP

A managed AP monitors the health of its primary WCS. Health monitoring guarantees the detection of the failure of the primary WCS within 5 seconds. Health monitoring is done over the TCP control connection. The AP also maintains a keep-alive timer for the WCS, which is reset every time it receives a message from the WCS.

Deployment site models

The WLAN Deployment Site Models comprise of the Site Model Designer, the RF Monitoring Tools and the Location Tracking tools. These tools are developed as self-sufficient services. The services expose Web Service interface to integrate with other management applications.

The tools provide adapters to tap into the EUM framework as service module as well as adapters to integrate with WMS. The following section describes these tools in further detail.

Site Model Designer

The Site Model Designer (SMD) GUI application is an out-of band pre-deployment tool that is used to model the targeted WLAN deployment environment. The SMD creates a structured hierarchical model that captures the physical properties and the layout of each floor in the buildings where WLAN is deployed. The SMD also captures the placements and physical configurations of APs and WCs across the deployment site floors.

The SMD provides both browsing and editing capabilities of the physical properties of the deployment site floor plans. Individual floor plans can be created with one of the following approaches:

- The AutoCAD drawing of the site is imported and edited to create the floor plan model.
- The raster image (gif, jpg, png) of the building floor plans is used as a background template and the Floor Plan Elements (FPE) are traced atop the image.
- The entire site model is imported from a third party RF modeling tool.

The model is structured in the following general hierarchical way:

- Building: to accommodate for multibuilding sites.
- Floor: captures physical RF attenuation properties and layout of one floor.
- AP: captures physical details of an AP on a floor such as location, model, serial number, MAC.
- WC: captures physical details of a WC on a floor suck as location, model, serial number, MAC.
- Location Zone: name and area of a part of a floor as defined and mapped by Location Tracking Services.

A Floor Plan (FP) is the main building block of the site model. It contains location information for APs and WCs on the floor. Each AP and WC on the model describe physical characteristics of the corresponding units (for example model, MAC, serial number). Buildings are primarily FP grouping concepts. A FP groups Floor Plan Elements (FPE) (such as walls, doors, windows) by the common attenuation material type into corresponding layers. Floor Plan Elements are represented as straight lines only. Composite shapes, including circles and arches are approximated by a set of FPEs.

The site models are defined in XML format. The XML model file reflects the model's hierarchical structure and contains all of the details of the deployment site.

To accommodate for aggregating multiple files into a single model file, the model is ultimately stored in a ZIP-archive format with the .SMX file extension.

Location Tracking

Location Tracking is used to pinpoint the positions of selected Mobile Units (MU) within the WLAN coverage boundaries. The MU location is presented graphically on a floor plan model.

During the initial Site Survey or Location Tracking Engine Training, the deployment site is surveyed to collect RF fingerprints of building location areas. These areas are then assigned a unique name which is later used to report the location of a detected wireless unit when it roams into that area.

To provide a visual indication of a users location inside a building the locations zones are mapped to the floor plan model. When the location tracking API returns the location name of a wireless unit the location zones corresponding floor plan diagram is found and the location zones area is colored to indicate the wireless units position.

The list of the location zones defined by Runtime Location Tracking Services is exported from the corresponding RTLS, imported to the SMD and accessed through drop-down combo box controls inside the SMD.

The WLAN management solution provides two types of location tracking; basic on-demand location services and overlay third-party location tools.

Basic on-demand location services uses on-demand tracking only. Location queries are issued by MAC address and invoke triangulation algorithm. MUs can be tracked by MAC, IP or the user. IP and the user are internally translated to a corresponding MAC address; all location queries are ultimately MAC-based. MUs are tracked by supported defined physical type (APs, sensors, clients, tags) and by logical type (rogue APs).

The WLAN management solution can be bundled with third-party Location Services in overlay mode. This provides a more sophisticated and robust solution over the basic tracking functionality offered by the WLAN RF Tools.

The overlay third-party location tools can track locations in real time, as opposed to the on-demand mode supported by the ODLS. The real-time mode is used for additional security features, such as providing location-based access control, or monitoring disallowed asset movements.

RF monitoring

The RF Monitoring Tool (RFMT) provides insights into the run-time WLAN performance. It is based on the RF site model defined with the SMD. This tool provides a heat map view of the site model based on the current AP state (power and channel). The heat map is a predictive simulation, but provides insights into the RF operations. It can be particularly useful in case of AutoRF mode, where RF parameters are not directly configured but automatically adjusted. The RFMT reads the current transmit power/channel values of the AP from the network and plugs them into the model. Clicking on any point on the floor’s heat mat produces a table listing the estimated receive power from all the APs audible at that point.

The RFMT provides the following views on the predicted coverage:

- single AP coverage view
- multiple APs on a single floor
- multiple APs on multiple floors

Configuration and management interfaces

The following section describes the configuration and management interfaces associated with the WLAN Controller 8180 (WC 8180). These interfaces are:

- Enterprise Device Manager (EDM)
- Wireless Management Server (WMS)
- Command Line Interface (CLI)

Enterprise Device Manager

The Enterprise Device Manager (EDM) is a graphical user interface (GUI) application used for the management of individual WC 8180 units.

WLAN Management Server

The WLAN Management Server (WMS) is a browser-based server management solution. WMS is used to manage multiple WC 8180 devices, whether individually or grouped into Mobility Domains. WMS is installed on a network server and can be accessed by a distributed group of network administrators. Unlike the EDM solution, WMS does not ship with the controller and must be purchased and downloaded separately.

Command Line Interface

The Command Line Interface (CLI) is a text based management system used for the management of individual WC 8180 units. The CLI is accessed locally through a connection to the Console port on the front of the device or remotely through Telnet or SSH.

The following sections detail the usage of the CLI and the navigation of the interface.

Command modes

The CLI is divided into five command modes. Each command mode has different levels of access to the device and is used for different aspects of configuration and management. The following command modes are available:

- User Execution

  This is the default command mode. This is the most restrictive command mode. Only basic management commands are available.

- Privileged Execution

  This command mode is used to perform basic switch level management tasks. Downloading software images, setting passwords, and restarting the switch are some examples of the tasks performed. All commands available in User Execution mode are also available in this mode.

- Global Configuration

  This command mode provides commands for general switch configuration. Commands in this mode can be used to configure the device IP address, SNMP parameters, Telnet access, and VLANs. Commands from User and Privileged Execution modes are also available in this mode.

- Interface Configuration

  This command mode provides commands for the configuration of port and VLAN parameters. Parameters include speed, duplex, and rate limiting.

- Wireless Configuration

  This command mode provides commands for the configuration of wireless operations. Operations include access point configuration, access point profile configuration, network profile configuration, and configuration of the wireless controller itself.

The following table lists the commands for entering and exiting each command mode.

Command Mode	Example Prompt	Entrance Command	Exit Command
User Execution	**WC8180>**	N/A	**exit** or **logout**
Privileged Execution	**WC8180#**	**enable**	**exit**
Global Configuration	**WC8180(config)#**	**configure**	**exit**
Interface Configuration	**WC8180(config-if)#**	**interface**	**exit**
Wireless Configuration	**WC8180(config-wireless)#**	**wireless**	**exit**

DHCP Option 43 configuration

The WLAN 8100 solution requires configuration of DHCP Option 43 to ensure proper operation of access points and the solution overall. This configuration should be performed before attempting any operations that require network connectivity between the controller and access points.

Configuration is dependent on the type of DHCP server in use in the network environment. Avaya recommends the use of either a Windows 2003 Server or Linux-based DHCP server. If a Windows 2003 DHCP server is in use, perform the following actions:

1. Open the DHCP Server Manager.
2. Select DHCP > <your-DHCP-server> > Scope > Scope Option > Option 043.
3. Configure Sub-Option 8 as AVAYA AP with hexadecimal values for domain controller IP addresses. A UDP port for communications can also be optionally specified.
4. Click OK.

If a Linux DHCP server is in use, perform the following actions:

1. Edit dhcpd.conf (/root/dhcp.conf).
2. Configure Sub-Option 8 as AVAYA AP with hexadecimal values for domain controller IP addresses. A UDP port for communications can also be optionally specified.
3. Restart dhcpd.

For example, a Linux entry for Option 43 with controller addresses 192.168.11.2 and 192.168.11.3 and using port 61000 would break down as follows:

option vendor-encapsulated-options 08:08:41:56:41:59:41:20:41:50 = "AVAYA AP"

:01:04:c0:a8:0b:02 = "192.168.11.2"

:01:04:c0:a8:0b:03 = "192.168.11.3"

:03:02:EE:48 = "61000"

The total Option 43 entry would be:

08:08:41:56:41:59:41:20:41:50:01:04:c0:a8:0b:02:01:04:c0:a8:0b:03:03:02:EE:48

The access point will use UDP port 61000 by default if Option 43 does not include the UDP port number.

WLAN Controller 8180

The WLAN Controller 8180 (WC 8180) is the scalable controller element of the WLAN 8100 solution. Individual WC 8180 devices have the capability to support up to 256 AP 8120 access points with the option of grouping devices into clusters of up to 32 controllers. The WC 8180 features 12 copper Gigabit Ethernet ports, 12 Fiber Optic ports, and 2 10Gig ports. This coupled with dual redundant power supplies makes the WC 8180 an always-on solution for today's WLAN environment.

Additionally, the WC 8180 has the following features:

- FIPS 140–2 ready
- Layer 2 and Layer 3 secure seamless roaming
- RADIUS integration
- LDAP integration
- Configuration and monitoring through Enterprise Device Manager, Command Line Interface, WLAN Management System, and SNMPv3

The WC 8180 is available with the capability to support 16 or 64 access points out of the box. Additional access point support is available in 64 access point increments.

Access Point 8120

The Access Point 8120 (AP 8120) is a dual radio 802.11n access point. The AP 8120 features industry-leading Voice Over WLAN capabilities with 3 antenna MIMO, 2 spatial streams, and up to 300Mbps bandwidth. The AP 8120 supports both legacy 802.11 a/b/g and 802.11n network devices.

Additionally, the AP 8120 has the following features:

- 802.11e, 802.11r, CAC, 802.1p, DSCP
- GigE interface with 802.3af POE
- WMM, UAPSD, TSPEC Certified
- 802.11i/WPA2 Security
- Internal & External MIMO Antenna arrays
- FIPS 140-2 ready
- Distributed Forwarding

Related topics:

Unpacking the access point on page 17

Unpacking the access point

The shipping carton for an AP contains the following items:

- one AP
- mounting kit
  - one universal mounting bracket (attached to the AP)
  - one dual size (15/16 and 5/8 inch) T-bar clamp
  - one mounting bracket that attaches to the T-bar clamp and AP
  - four adhesive rubber feet
- Avaya WLAN 8100 - Regulatory Information - AP 8120 document

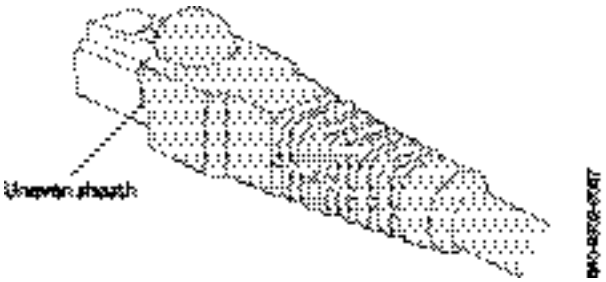
Verify that the items removed from the shipping carton correspond to the provided list. If an item is missing or damaged, contact Avaya.

Cabling requirements

The AP 8120 access point has one RJ-45 port. This port provides a 10/100/1000BASE-TX Ethernet connection to a Wireless Controller 8180. This port is used to indirectly connect an access point to a WC 8180 through an intermediate Layer 2 or Layer 3 network.

The access point can receive power and data through the RJ-45 port. Use a Category 5 (CAT-5) cable with straight-through signaling and standard RJ-45 connectors to connect to a network device. The AP 8120 supports 802.3af. An Avaya-approved power injectors must be used to provide the access point with power over the Ethernet cable. The WC 8180 has no PoE capabilities.

The Ethernet port on the access point cannot accept a CAT-5 cable that has an uneven sheath as shown below. The RJ-45 connector on the cable will not seat properly in the receptacle on the access point. Use a CAT-5 cable with an even sheath instead.



You must operate the access point with a CAT-5 Ethernet cable installed on the Ethernet port to ensure compliance with the Class B emissions standards. Failure to comply with this installation requirement can cause the device to operate in excess of the allowable emissions limits.

Important:

The AP 8120 access point is intended for indoor use only. Do not install the device or operate it outdoors.

Important:

To reduce the possibility of connection interference caused by dust, clean the CAT-5 connector pins before inserting a cable into an AP.

The following table lists the pin signals for the 10/100/1000 Ethernet straight-through wiring. Pins 4, 5, 7, and 8 are used when Avaya Power over Ethernet (PoE) is enabled on the port.

Wireless Controller 8180	
Pin	**Function**
1	Bidirectional pair +A
2	Bidirectional pair -A
3	Bidirectional pair +B
4	Bidirectional pair +C
5	Bidirectional pair -C
6	Bidirectional pair -B
7	Bidirectional pair +D
8	Bidirectional pair -D

Wall installation recommendations

If you plan to install an AP on a partial wall or other vertical surface, orient the top of the access point (the side with the LEDs) toward the intended coverage area. The radio antennas transmit through the top of the access point but not through the bottom (where the bracket is located).

Radio safety advisories

When you enable the AP radios as part of a configuration, the radios can receive and transmit radio frequency energy as soon as you connect the AP to the WC 8180, either directly or through the network.

Radio frequency advisories

Federal Communications Commission (FCC) Docket 96-8 for Spread Spectrum Transmitters specifies a safety standard for human exposure to radio frequency electromagnetic energy emitted by FCC-certified equipment. The Avaya Access Point 8120 product meets the uncontrolled environmental limits found in OET-65 and ANSI C95.1-1991, if proper installation procedures are followed. To ensure compliance with these exposure requirements, you must install this device in such a manner as to maintain a minimum of 20 cm separation distance between the radiating elements and all persons.

Additional radio safety advisories

Warning:

Install this device in such a manner as to maintain a minimum of 20 cm (7.9 inches) separation distance between the radiating elements and all persons. This safety warning conforms with FCC radio frequency exposure limits.

Warning:

Do not operate the AP near unshielded blasting caps or in an otherwise explosive environment unless the device has been modified for such use by qualified personnel.

Warning:

Do not touch or move the AP when the antennas are transmitting or receiving.

Warning:

Before using a wireless device in a hazardous location, consult the local codes, national codes, and safety directors of the location for usage constraints.

Chapter 2: Roadmap

This section lists and describes the documentation available for the Avaya WLAN 8100 product suite.

Product fundamentals

Product fundamentals documentation includes overview and reference information about the product and product documentation. The following table lists the product fundamentals documents in the Avaya WLAN 8100 documentation suite.

Title	Description
Avaya WLAN 8100 Regulatory Information (WC 8180) (NN47251-101)	This document provides regulatory information for the Avaya WLAN 8100 WLAN Controller 8180.
Avaya WLAN 8100 Fundamentals (NN47251-102)	This document provides an overview of the technologies and products used in the Avaya WLAN 8100 product suite.
Avaya WLAN 8100 Terminology (NN47251-103)	This document provides a dictionary of terms and acronyms used in the Avaya WLAN 8100 documentation suite.
Avaya WLAN 8100 Regulatory Information (AP 8120) (NN47251-104)	This document provides regulatory information for the Avaya WLAN 8100 Access Point 8120.
Avaya WLAN 8100 Planning and Engineering (NN47251-200)	This document provides information on network planning and integration.

Installation and commissioning

Installation and commissioning documentation describes the installation of Avaya WLAN 8100 hardware and how to perform initial configuration.

Title	Description
Avaya WLAN 8100 Quick Start Guide (NN47251-106)	This document provides the information and procedures necessary to quickly install the WC 8180 and AP 8120.

Title	Description
Avaya WLAN 8100 Installation - AP 8120 (NN47251-302)	This document provides information and procedures for the physical installation of the AP 8120.
Avaya WLAN 8100 Installation - WC8180 (NN47251-303)	This document provides information and procedures for the physical installation of the WC 8180.
Avaya WLAN 8100 Commissioning (NN47251-304)	This document provides information and procedures on the initial configuration of the WC 8180 and AP 8120.

Upgrades and patches

Upgrade and patch documentation describes the software upgrade process.

Title	Description
Avaya WLAN 8100 Release Notes (NN47251-400)	This document provides the latest information on the Avaya WLAN 8100 product and documentation suites as well as information on the installation of software upgrades.

Operations

Operations documentation describes the configuration and management of Avaya WLAN 8100 devices.

Title	Description
Avaya WLAN 8100 Configuration - WC 8180 (CLI) (NN47251-500)	This document provides information and procedures for the configuration and management of the WLAN Controller 8180 using the command line interface.
Avaya WLAN 8100 Configuration - WC 8180 (GUI) (NN47251-501)	This document provides information and procedures for the configuration and management of the WLAN Controller 8180 using the WMS management software.

Fault and performance management

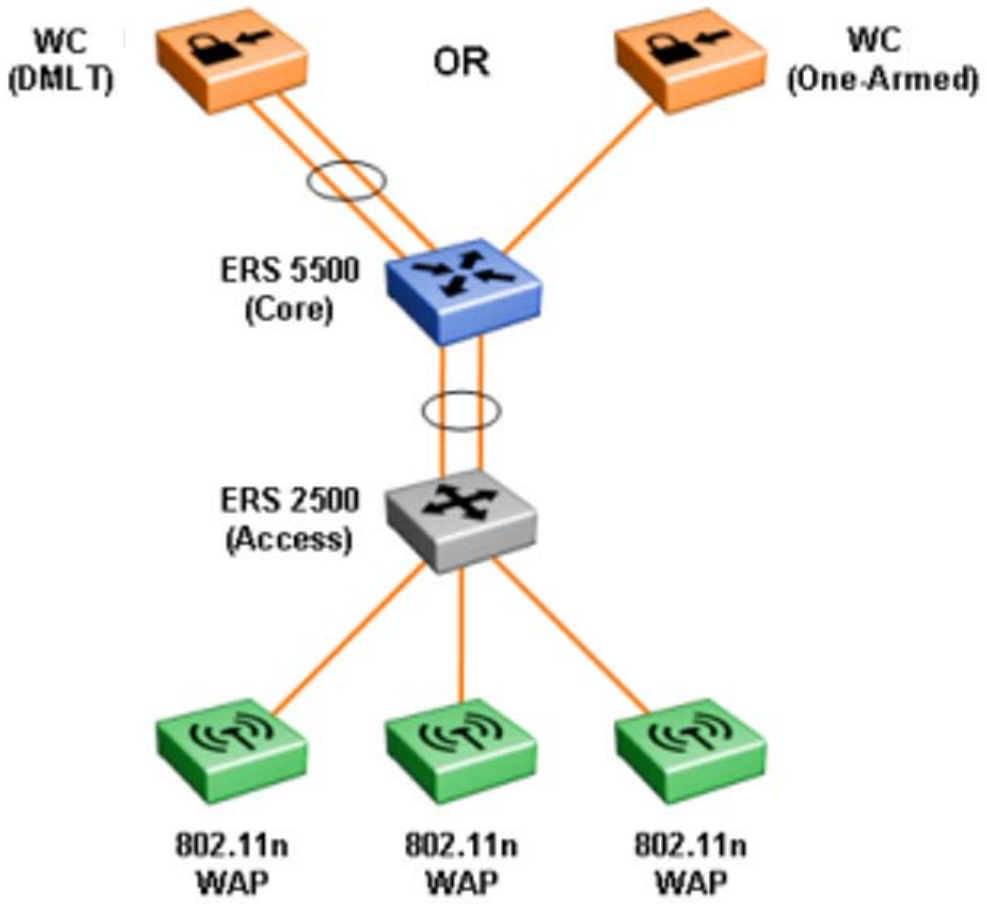
Fault and performance management documentation describes fault and performance management techniques.

Title	Description
Avaya WLAN 8100 Troubleshooting (NN47251-700)	This document provides troubleshooting information and procedures for the WLAN Controller 8180 and Access Point 8120.

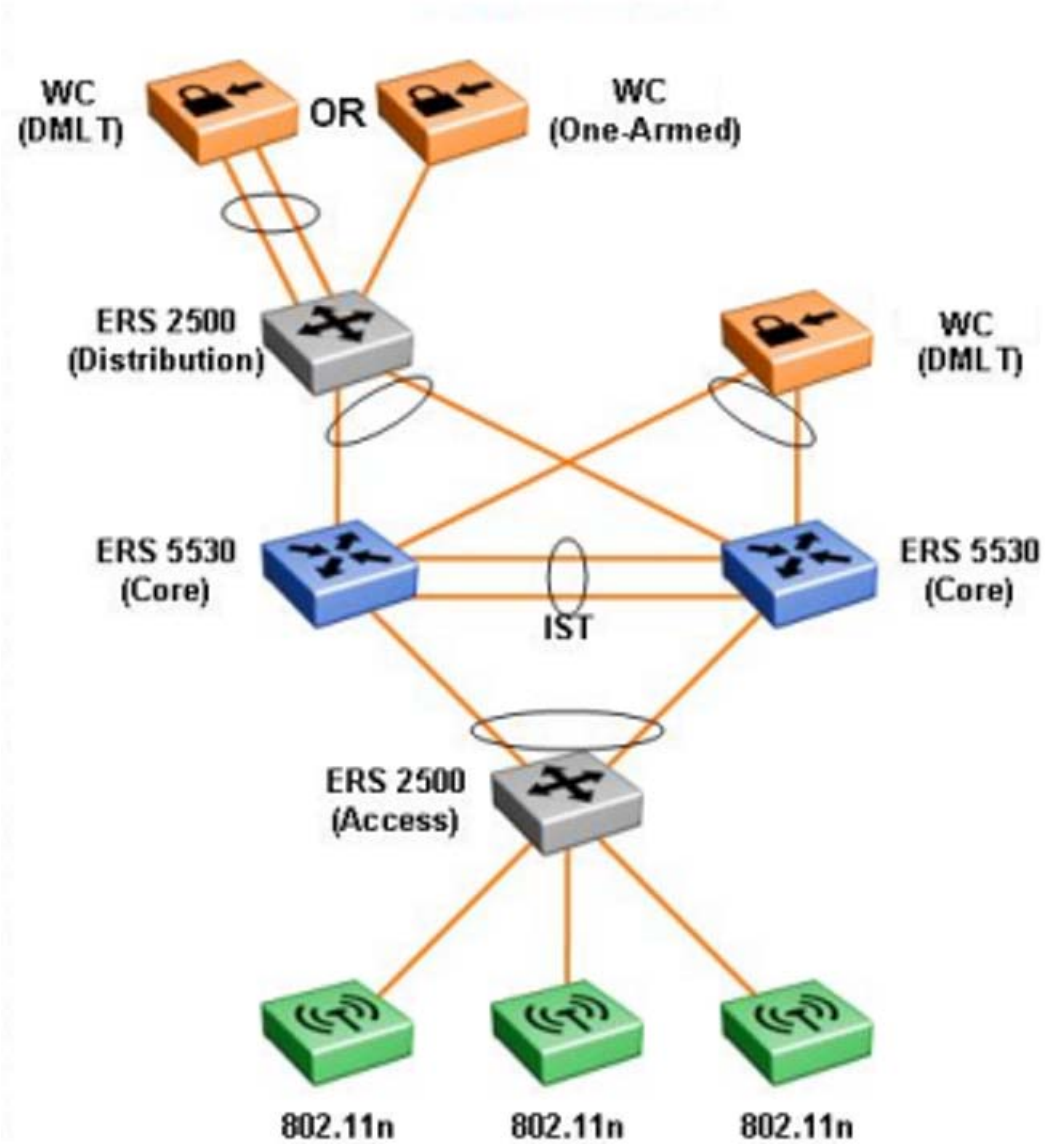
Chapter 3: Common WLAN 8100 Topologies

This section demonstrates some common topologies used to implement the WLAN 8100 series in a network environment.

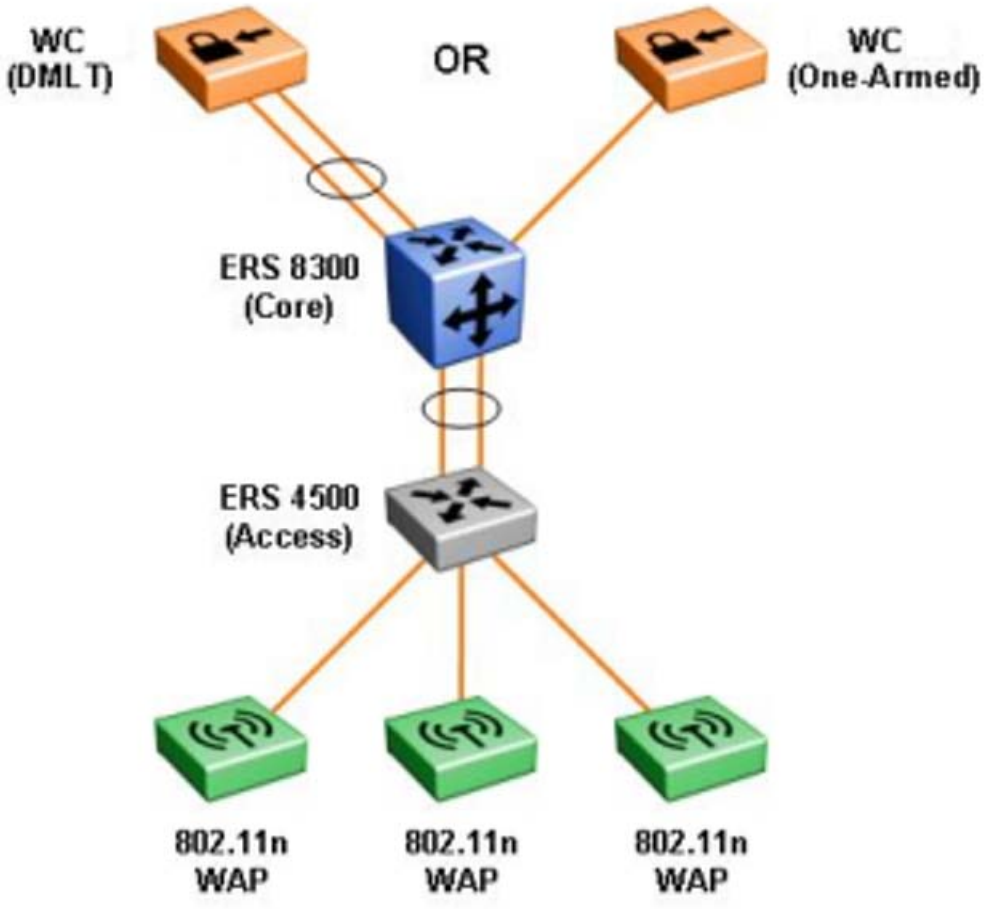
Small Campus Single Core



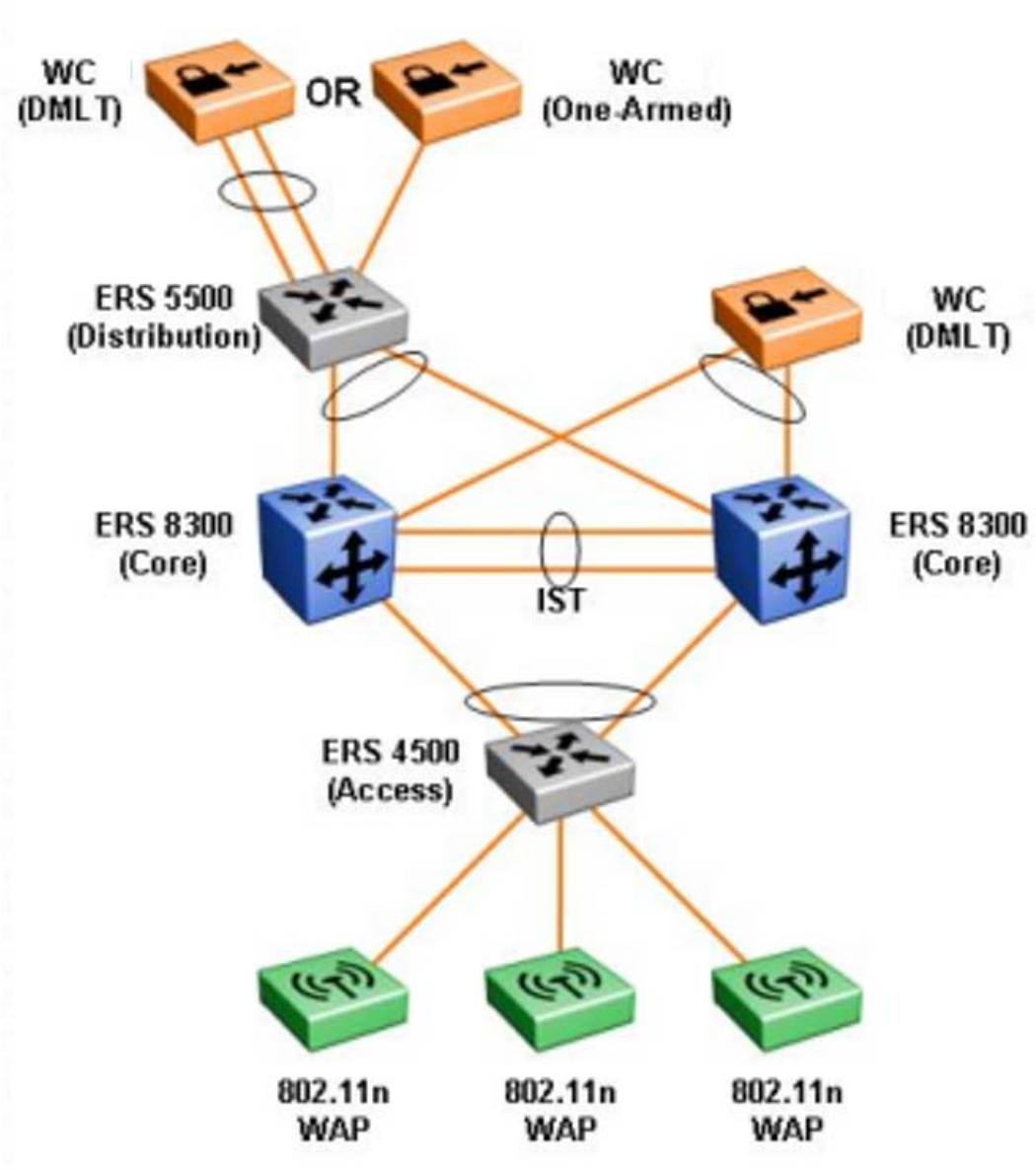
Small Campus SMLT Core



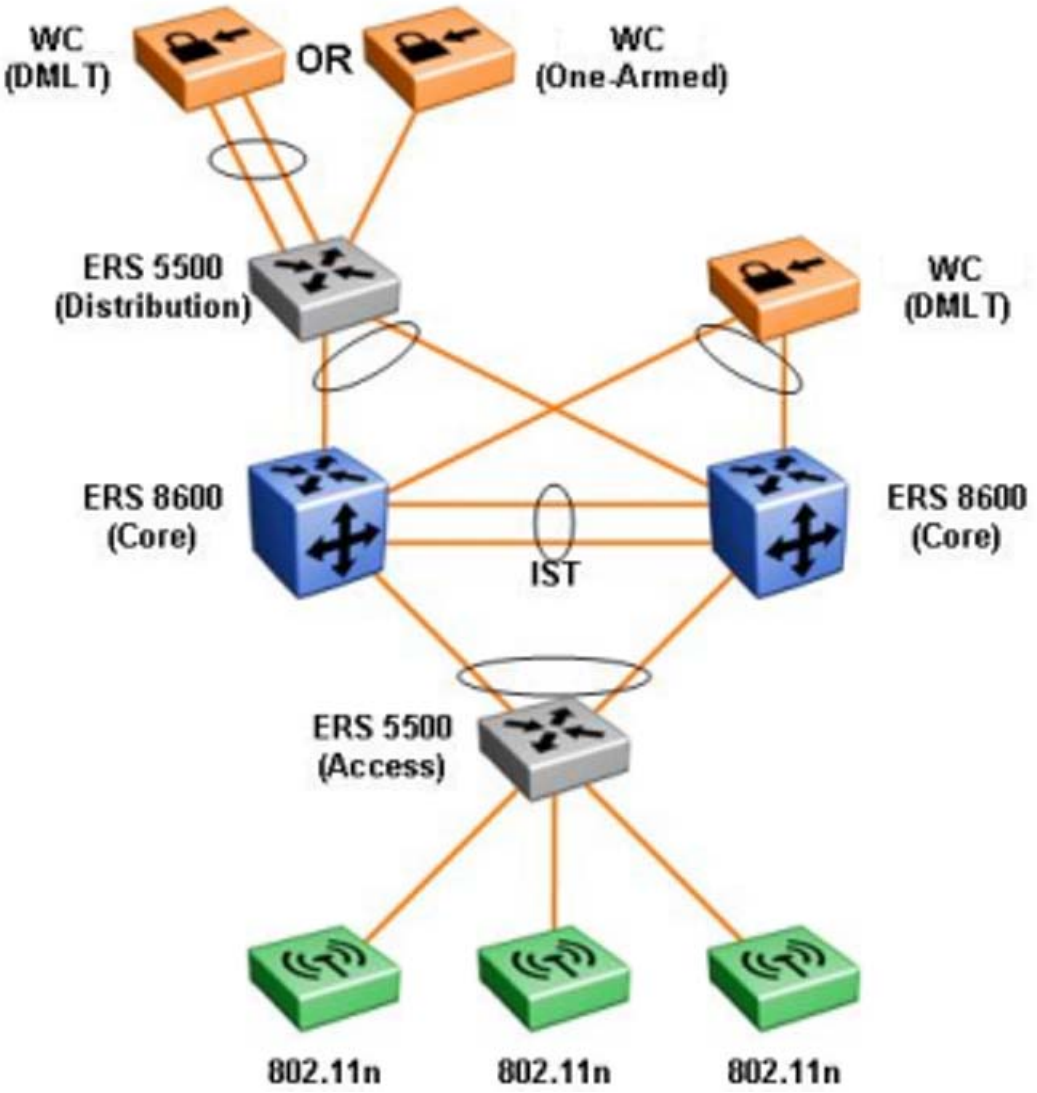
Medium Campus Single Core



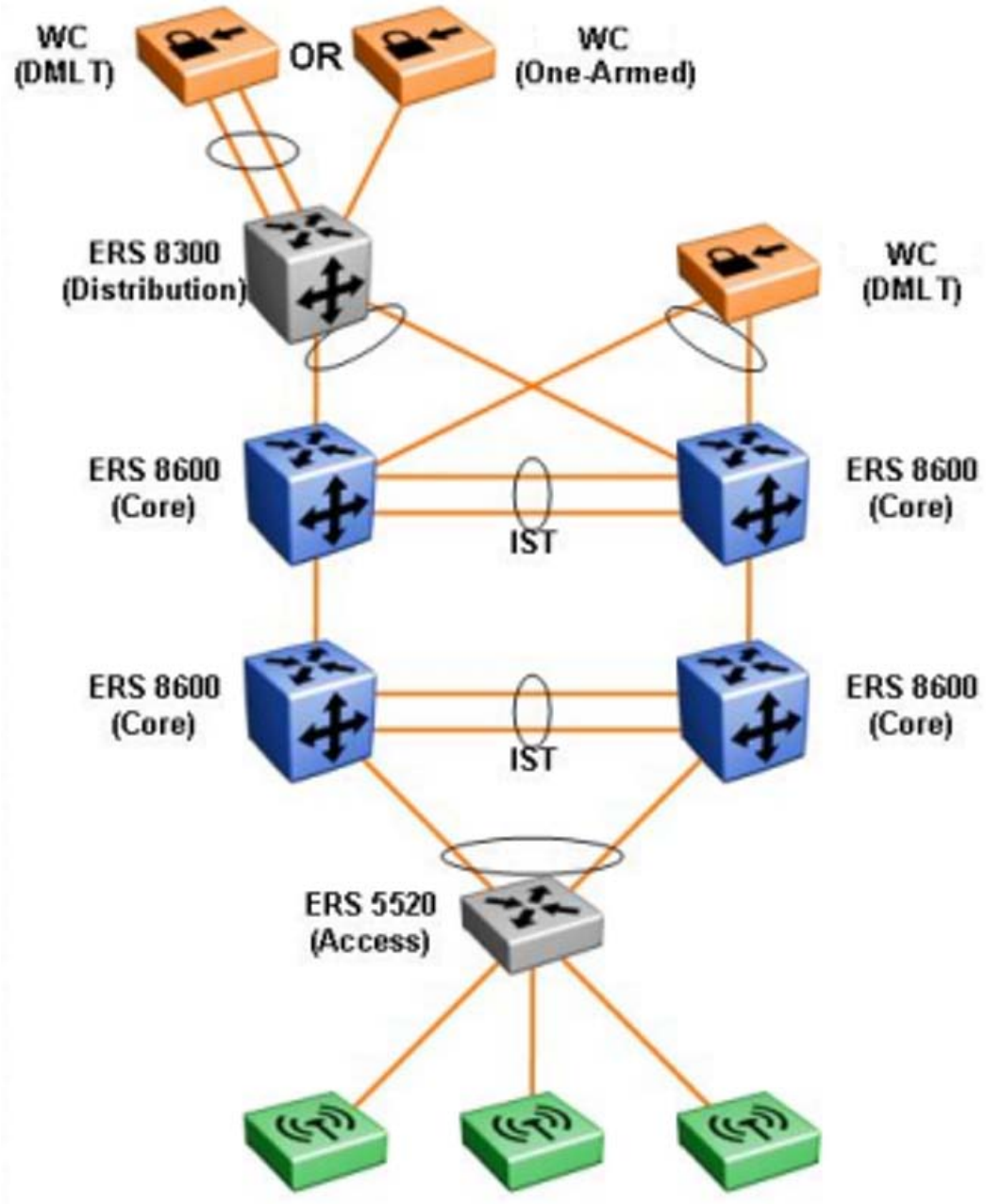
Medium Campus SMLT Core



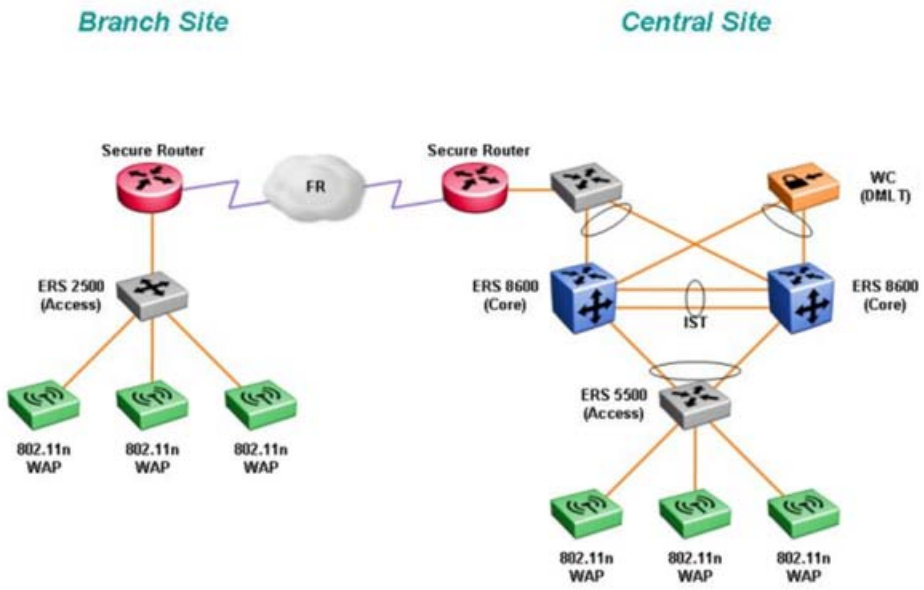
Large Campus SMLT Core



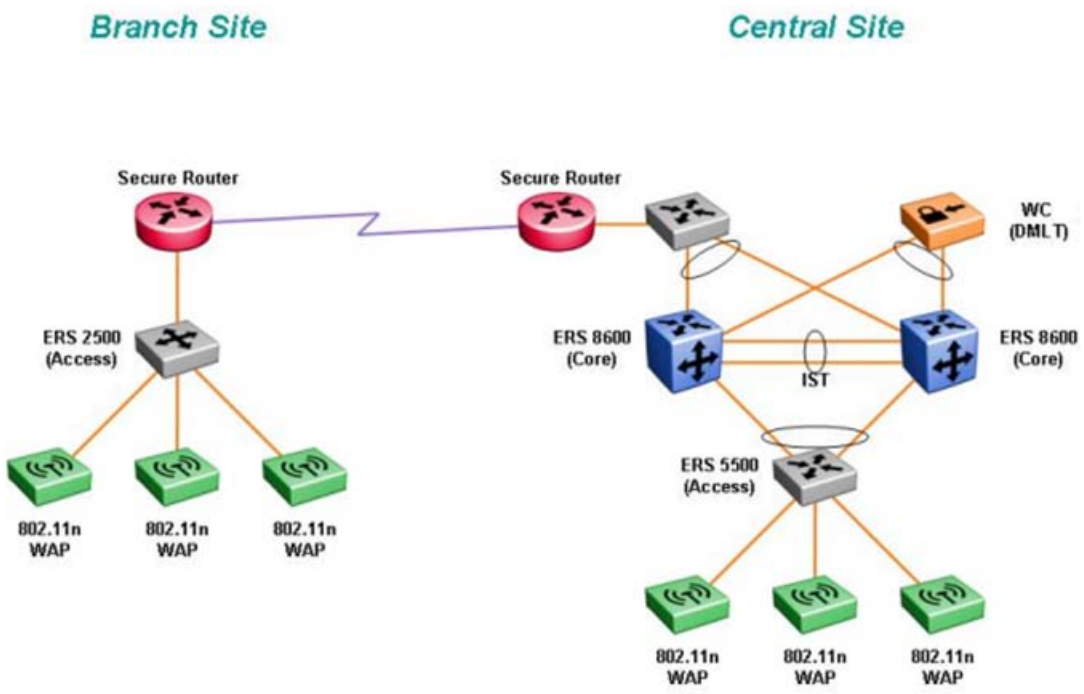
Large Campus SMLT / RSMLT Core



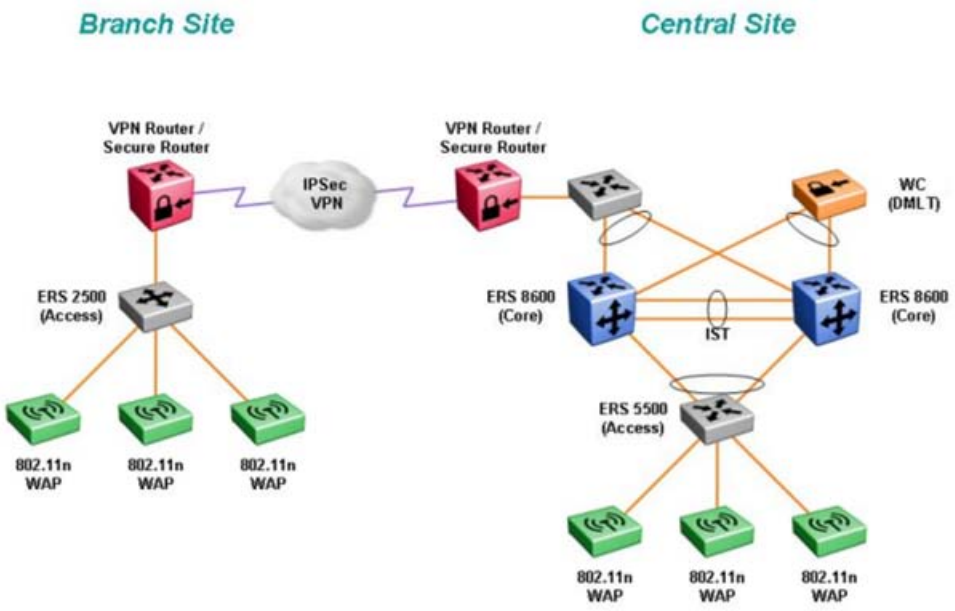
Frame-Relay WAN



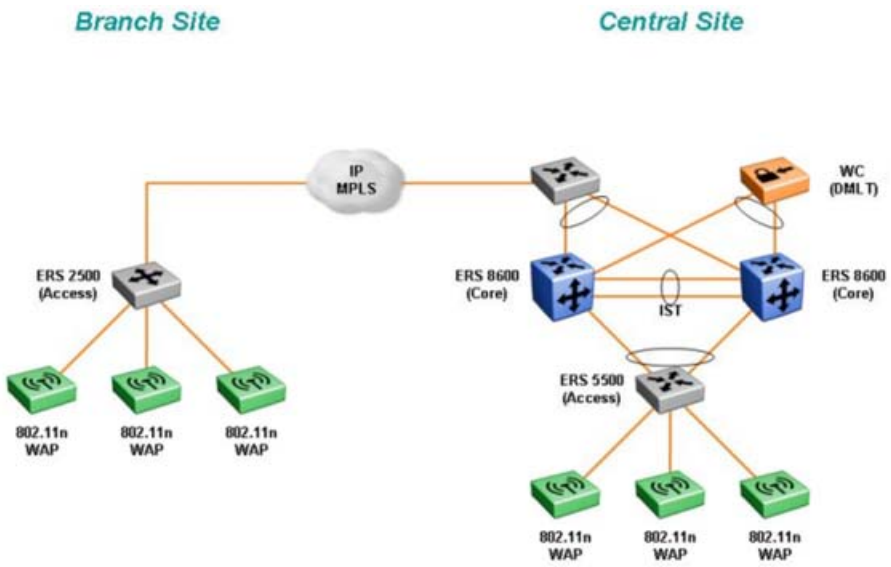
PPP WAN


Branch Site
Central Site
Secure Router
Secure Router
WC
(DMLT)
ERS 2500
(Access)
ERS 8600
(Core)
IST
ERS 8600
(Core)
ERS 5500
(Access)
802.11n
WAP
802.11n
WAP
802.11n
WAP
802.11n
WAP
802.11n
WAP
802.11n
WAP

IPSEC WAN


Branch Site
Central Site
VPN Router / Secure Router
IPSec VPN
VPN Router / Secure Router
WC (DMLT)
ERS 2500 (Access)
ERS 8600 (Core)
IST
ERS 8600 (Core)
ERS 5500 (Access)
802.11n WAP
802.11n WAP
802.11n WAP
802.11n WAP
802.11n WAP
802.11n WAP

MPLS


Branch Site
Central Site
IP
MPLS
WC
(DMLT)
ERS 2500
(Access)
ERS 8600
(Core)
IST
ERS 8600
(Core)
ERS 5500
(Access)
802.11n
WAP
802.11n
WAP
802.11n
WAP
802.11n
WAP
802.11n
WAP
802.11n
WAP

Appendix A: Detailed Feature List

The following sections present detailed feature lists for the components of the WLAN 8100 solution.

WLAN Controller 8180

Table 1: Hardware Features

Feature	Description
Gigabit Ethernet Ports	12 Copper and 12 Fiber
10 Gigabit Ethernet Ports	2
Access Points per Controller	256 maximum
Power Supply	Dual redundant
Clustering	32 controllers per cluster

Table 2: Software Features

Feature
Layer 2 and Layer 3 secure seamless roaming
Captive portal
RADIUS/LDAP Integration
Web UI, CLI, and SNMPv3 management
Clustering

Access Point 8120

Table 3: Hardware Features

Feature	Description
Wireless	Dual radio 802.11n
Antennas	3 antenna MIMO with 2 spatial streams and up to 300Mbps bandwidth
Network Connectivity	1 Gigabit Ethernet with 802.3af PoE

Table 4: Software Features

Feature
WMM, UAPSD, Wi-Fi Certified
802.11i/WPA2 Security
Basic WIDS/WIPS Support
Control plane encryption
802.11e, CAC, 802.11p, DSCP