TOPICS COVERED:

WIRELESS

- WIRED vs WIRELESS
- BASIC SERVICE SET (BSS)
- RADIO FREQUENCY (RF)
- WIRELESS BANDS & CHANNELS
- WIRELESS ENCRYPTION
- CISCO WLC DEPLOYMENT MODELS
- WIRELESS LAN 802.11 SERVICE SET
- CISCO WLC BASIC CONFIGURATION (GNS3 LAB)
- CISCO WIRELESS AP MODES

WIRELESS TECHNOLOGIES

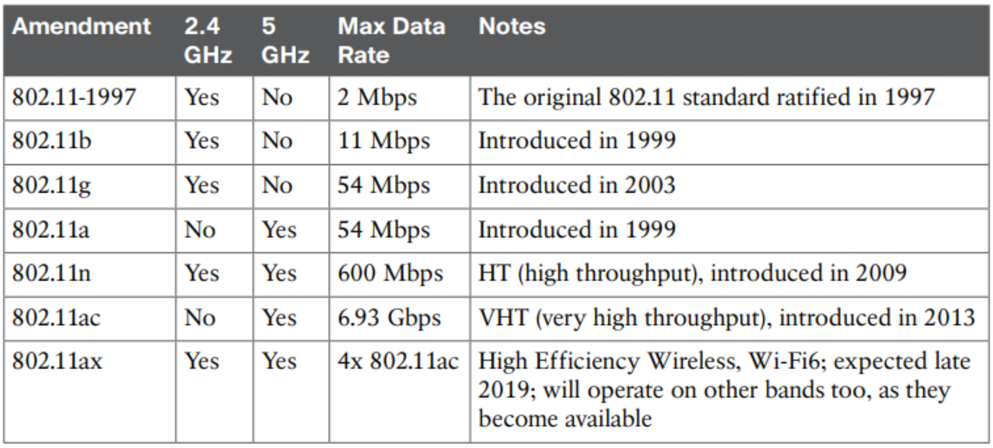
WIRED

1. In a wired network, any two devices that need to communicate with each other must be connected by a wire.
2. In a wired network, any two devices that need to communicate with each other must be connected by a wire.
3. Data that passes over the wire is bounded by the physical properties of the wire.
4. The IEEE 802.3 set of standards defines strict guidelines for the Ethernet wire itself, in addition to how devices may connect, send, and receive data over the wire.
5. Wired connections have been engineered with tight constraints and have few variables that might prevent successful communication. Even the type and size of the wire strands, the number of twists the strands must make around each other over a distance, and the maximum length of the wire must adhere to the standard.
6. Therefore, a wired network is essentially a bounded medium; data must travel over whatever path the wire or cable takes between two devices
7. If the cable goes around a corner or lies in a coil, the electrical signals used to carry the data must also go around a corner or around a coil.

WIRELESS

1. A wireless network removes the need to be tethered to a wire or cable.
2. Convenience and mobility become paramount, enabling users to move around at will while staying connected to the network.
3. A user can (and often does) bring along many different wireless devices that can all connect to the network easily and seamlessly.
4. Wireless data must travel through free space, without the constraints and protection of a wire.
5. In the free space environment, many variables can affect the data and its delivery. To minimize the variables, wireless engineering efforts must focus on two things:
   ■ Wireless devices must adhere to a common standard (IEEE 802.11).
   ■ Wireless coverage must exist in the area where devices are expected to use it

Table 26-3 Basic Characteristics of Some IEEE 802.11 Amendments



Amendment	2.4 GHz	5 GHz	Max Data Rate	Notes
802.11-1997	Yes	No	2 Mbps	The original 802.11 standard ratified in 1997
802.11b	Yes	No	11 Mbps	Introduced in 1999
802.11g	Yes	No	54 Mbps	Introduced in 2003
802.11a	No	Yes	54 Mbps	Introduced in 1999
802.11n	Yes	Yes	600 Mbps	HT (high throughput), introduced in 2009
802.11ac	No	Yes	6.93 Gbps	VHT (very high throughput), introduced in 2013
802.11ax	Yes	Yes	4x 802.11ac	High Efficiency Wireless, Wi-Fi6; expected late 2019; will operate on other bands too, as they become available

Wireless LAN Topologies

1. Wireless communication takes place over free space through the use of radio frequency (RF) signals.

2. The transmitter can contact the receiver at any and all times, as long as both devices are tuned to the same
frequency (or channel) and use the same scheme to carry the data between them.

3. To fully leverage wireless communication, data should travel in both directions, as shown in Figure 26-2. Sometimes Device A needs to send data to Device B, while Device B would like to take a turn to send at other times.

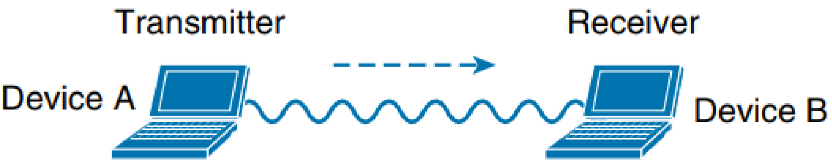


Figure 26-1 *Unidirectional Communication*

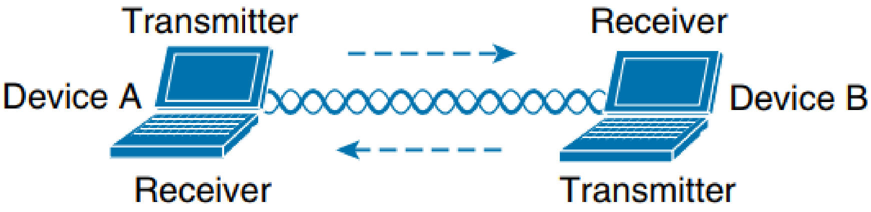


Figure 26-2 *Bidirectional Communication*

Basic Service Set (BSS)

1. The solution is to make every wireless service area a closed group of mobile devices that forms around a fixed device; before a device can participate, it must advertise its capabilities and then be granted permission to join. The 802.11 standard calls this a basic service set (BSS).
2. At the heart of every BSS is a wireless access point (AP).
3. The AP operates in infrastructure mode, which means it offers the services that are necessary to form the infrastructure of a wireless network.
4. The AP also establishes its BSS over a single wireless channel. The AP and the members of the must all use the same channel to communicate properly.
5. In addition, the AP advertises the wireless network with a Service Set Identifier (SSID), which is a text string containing a logical name.
6. Think of the BSSID as a machine-readable name tag that uniquely identifies the BSS ambassador (the AP), and the SSID as a nonunique, human-readable name tag that identifies the wireless service.

7. Membership with the BSS is called an association.
8. A wireless device must send an association request to the AP and the AP must either grant or deny the request. Once associated, a device becomes a client, or an 802.11 station (STA), of the BSS.
9. As long as a wireless client remains associated with a BSS, most communications to and from the client must pass through the AP.

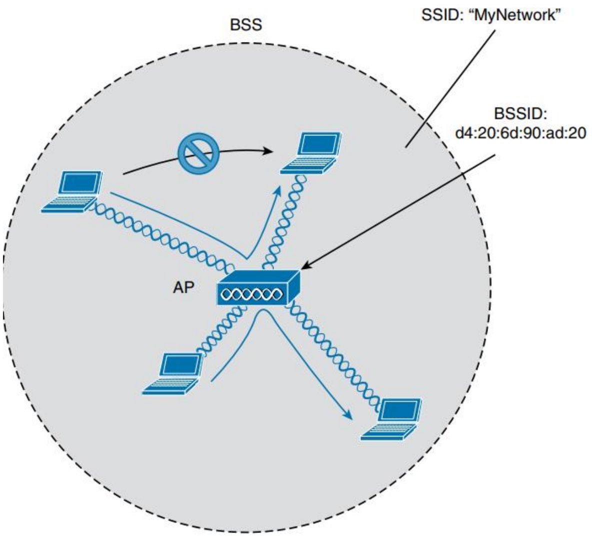
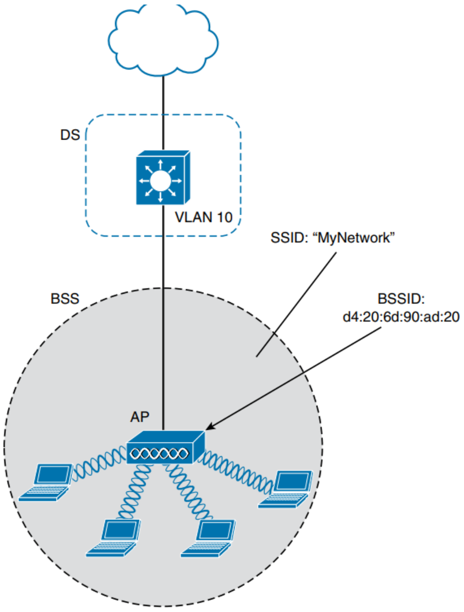


Figure 26-5 *Traffic Flows Within a BSS*



Radio Frequency (RF)

To send data across a wired link, an electrical signal is applied at one end and carried to the other end. The wire itself is continuous and conductive, so the signal can propagate rather easily.

A wireless link has no physical strands of anything to carry the signal along.

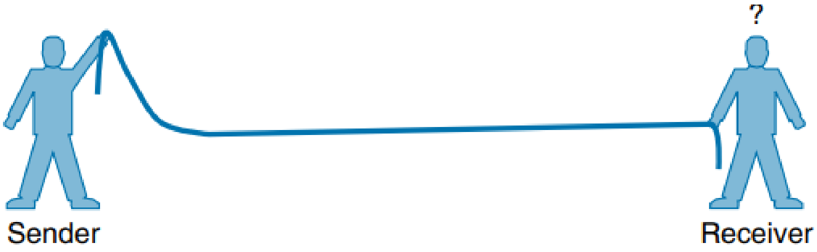


Figure 26-15 *Failed Attempt to Pass a Message Down a Rope*

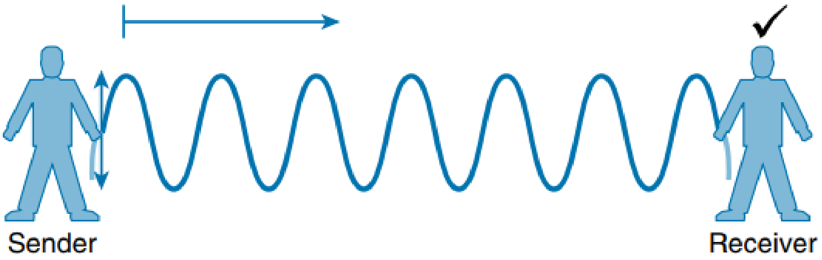
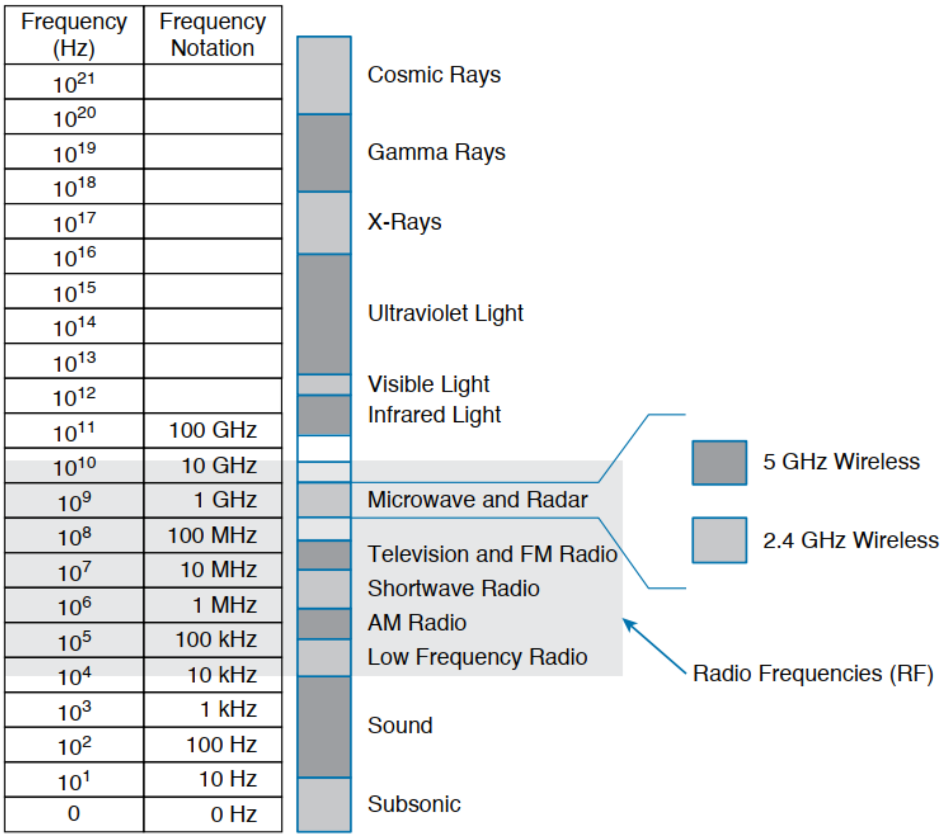


Figure 26-16 *Sending a Continuous Wave Down a Rope*



Frequency (Hz)	Frequency Notation
10^{21}	
10^{20}	
10^{19}	
10^{18}	
10^{17}	
10^{16}	
10^{15}	
10^{14}	
10^{13}	
10^{12}	
10^{11}	100 GHz
10^{10}	10 GHz
10^{9}	1 GHz
10^{8}	100 MHz
10^{7}	10 MHz
10^{6}	1 MHz
10^{5}	100 kHz
10^{4}	10 kHz
10^{3}	1 kHz
10^{2}	100 Hz
10^{1}	10 Hz
0	0 Hz

Figure 26-20 *Continuous Frequency Spectrum*

Electromagnetic waves do not travel in a straight line. Instead, they travel by expanding in all directions away from the antenna.

To get a visual image, think of dropping a pebble into a pond when the surface is still. Where it drops in, the pebble sets the water's surface into a cyclic motion.

The waves that result begin small and expand outward, only to be replaced by new waves. In free space, the electromagnetic waves expand outward in all three dimensions.

At the receiving end of a wireless link, the process is reversed. As the electromagnetic waves reach the receiver's antenna, they induce an electrical signal. If everything works right, the received signal will be a reasonable copy of the original transmitted signal.

The electromagnetic waves involved in a wireless link can be measured and described in several ways.

One fundamental property is the frequency of the wave, or the number of times the signal makes one complete up and down cycle in 1 second.

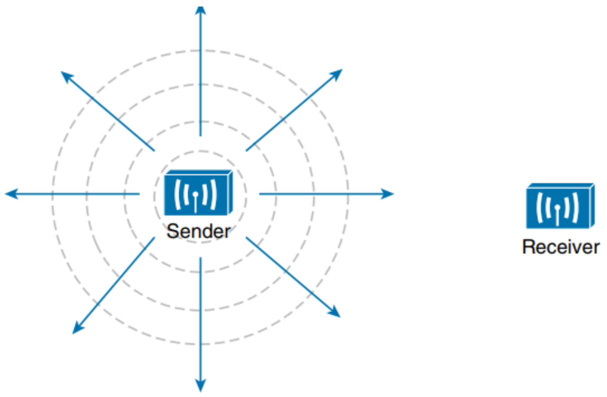


Figure 26-18 *Wave Propagation with an Idealistic Antenna*

Table 26-2 Frequency Unit Names

Unit	Abbreviation	Meaning
Hertz	Hz	Cycles per second
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1,000,000 Hz
Gigahertz	GHz	1,000,000,000 Hz

The frequency range from around 3 kHz to 300 GHz is commonly called radio frequency (RF).

It includes many different types of radio communication, including low-frequency radio, AM radio, shortwave radio, television, FM radio, microwave, and radar.

The microwave category also contains the two main frequency ranges that are used for wireless LAN communication: 2.4 GHz and 5 GHz.

Wireless Bands and Channels

1. Because a range of frequencies might be used for the same purpose, it is customary to refer to the range as a band of frequencies.

2. For example, the range from 530 kHz to around 1710 kHz is used by AM radio stations; therefore, it is commonly called the AM band or the AM broadcast band.

3. One of the two main frequency ranges used for wireless LAN communication lies between 2.400 and 2.4835 GHz. This is usually called the 2.4-GHz band, even though it does not encompass the entire range between 2.4 and 2.5 GHz. It is much more convenient to refer to the band name instead of the specific range of frequencies included.

4. The other wireless LAN range is usually called the 5-GHz band because it lies between 5.150 and 5.825 GHz. The 5-GHz band actually contains the following four separate and distinct bands:

5.150 to 5.250 GHz
5.250 to 5.350 GHz
5.470 to 5.725 GHz

5.725 to 5.825 GHz

> **TIP** You might have noticed that most of the 5-GHz bands are contiguous except for a gap between 5.350 and 5.470. At the time of this writing, this gap exists and cannot be used for wireless LANs. However, some governmental agencies have moved to reclaim the frequencies and repurpose them for wireless LANs. Efforts are also underway to add 5.825 through 5.925 GHz.

5. CHANNELS

A. frequency band contains a continuous range of frequencies. If two devices require a single frequency for a wireless link between them, which frequency can they use?

B. Beyond that, how many unique frequencies can be used within a band?

c. To keep everything orderly and compatible, bands are usually divided into a number of distinct channels.

d. Each channel is known by a channel number and is assigned to a specific frequency.

e. As long as the channels are defined by a national or international standards body, they can be used consistently in all locations.

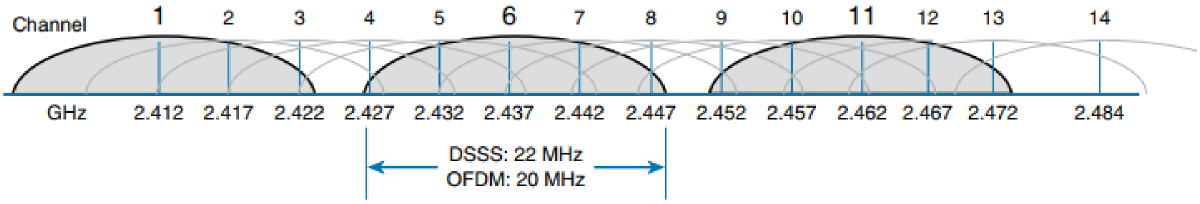


Figure 26-21 *Channel Layout in the 2.4-GHz Band*

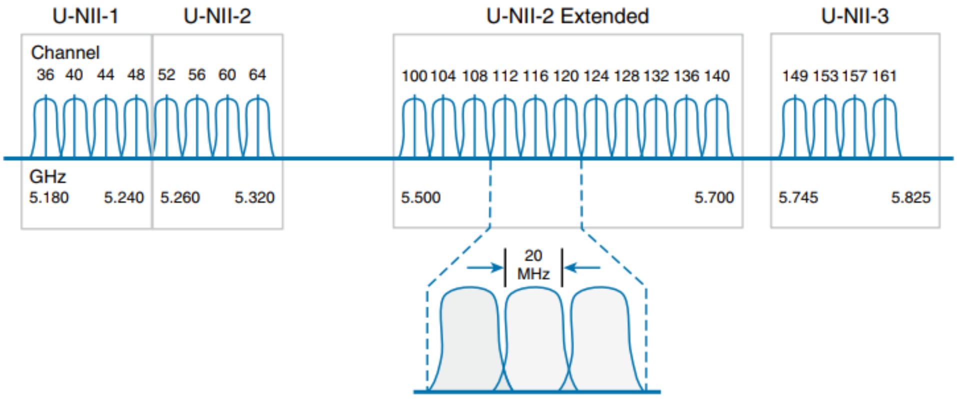


Figure 26-22 *Channel Layout in the 5-GHz Band*

In the 5-GHz band, this is the case because each channel is allocated a frequency range that does not encroach on or overlap the frequencies allocated for any other channel. In other words, the 5-GHz band consists of nonoverlapping channels.

The same is not true of the 2.4-GHz band. Each of its channels is much too wide to avoid overlapping the next lower or upper channel number.

In fact, each channel covers the frequency range that is allocated to more than four consecutive channels!

Notice the width of the channel spacing in Figure 26-21 as compared to the width of one of the shaded signals centered on channels 1, 6, and 11.

The only way to avoid any overlap between adjacent channels is to configure APs to use only channels 1, 6, and 11.

Even though there are 14 channels available to use, you should always strive for nonoverlapping channels in your network.

2.4 GHz vz 5 Ghz???

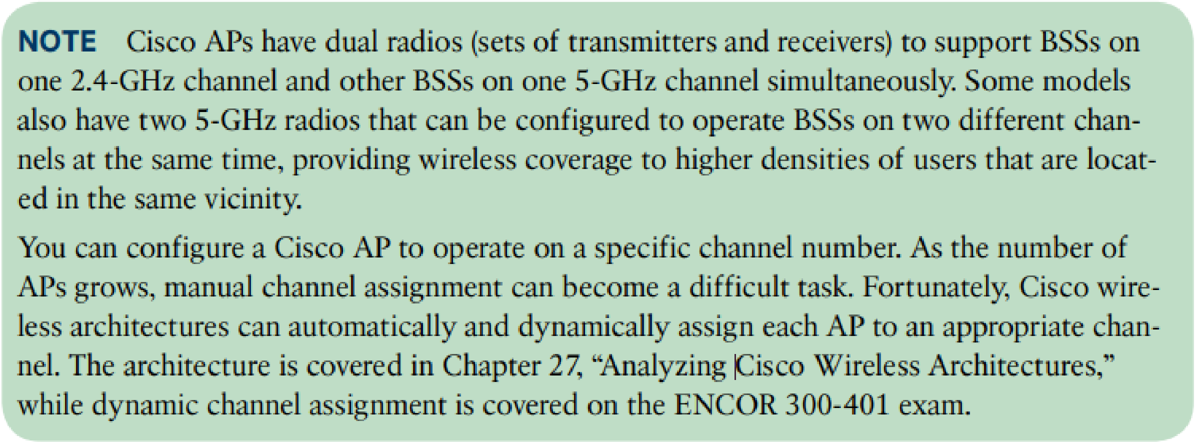
In open space, RF signals propagate or reach further on the 2.4-GHz band than on the 5-GHz band.

They also tend to penetrate indoor walls and objects easier at 2.4 GHz than 5 GHz.

However, the 2.4-GHz band is commonly more crowded with wireless devices.

Remember that only three nonoverlapping channels are available, so the chances of other neighboring APs using the same channels is greater.

In contrast, the 5-GHz band has many more channels available to use, making channels less crowded and experiencing less interference.



NOTE Cisco APs have dual radios (sets of transmitters and receivers) to support BSSs on one 2.4-GHz channel and other BSSs on one 5-GHz channel simultaneously. Some models also have two 5-GHz radios that can be configured to operate BSSs on two different channels at the same time, providing wireless coverage to higher densities of users that are located in the same vicinity.

You can configure a Cisco AP to operate on a specific channel number. As the number of APs grows, manual channel assignment can become a difficult task. Fortunately, Cisco wireless architectures can automatically and dynamically assign each AP to an appropriate channel. The architecture is covered in Chapter 27, "Analyzing Cisco Wireless Architectures," while dynamic channel assignment is covered on the ENCOR 300-401 exam.

Wireless Encryption

1. Open Authentication: Open authentication is true to its name; it offers open access to a WLAN. The only requirement is that a client must use an 802.11 authentication request before it attempts to associate with an AP. No other credentials are needed.

2. WEP: WEP uses the RC4 cipher algorithm to make every wireless data frame private and hidden from eavesdroppers. The algorithm uses a string of bits as a key, commonly called a WEP key, to derive other encryption keys—one per wireless frame. As long as the sender and receiver have an identical key, one can decrypt what the other encrypts.

3. 802.1x/EAP:

* Supplicant: The client device that is requesting access
* Authenticator: The network device that provides access to the network (usually a wireless LAN controller [WLC])
* Authentication server (AS): The device that takes user or client credentials and permits or denies network access based on a user database and policies (usually a RADIUS server)

WPA,WPA2,WPA3

The Wi-Fi Alliance (http://wi-fi.org), a nonprofit wireless industry association, has worked out straightforward ways to do that through its Wi-Fi Protected Access (WPA) industry certifications. To date, there are three different versions: WPA, WPA2, and WPA3. Wireless products are tested in authorized testing labs against stringent criteria that represent correct implementation of a standard. As long as the Wi-Fi Alliance has certified a wireless client device and an AP and its associated WLC for the same WPA version, they should be compatible and offer the same security components.

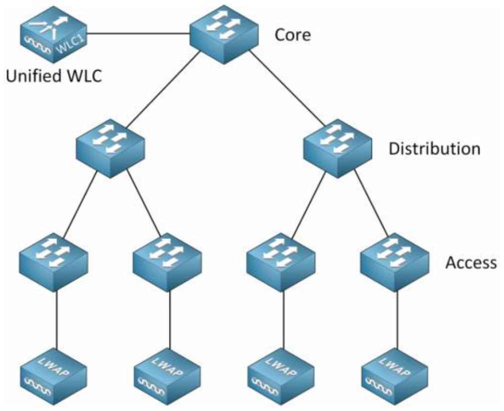
Cisco WLC Deployment Models

Let's say you want to deploy a WLC with multiple lightweight APs in your network. Where do you connect the WLC? In the core layer? The distribution or access layer? Or perhaps in the data center?

The **Split-MAC architecture** with the WLC and APs supports multiple deployment models. What is essential to understand is that all data from wireless clients goes through the CAPWAP tunnel to the WLC.

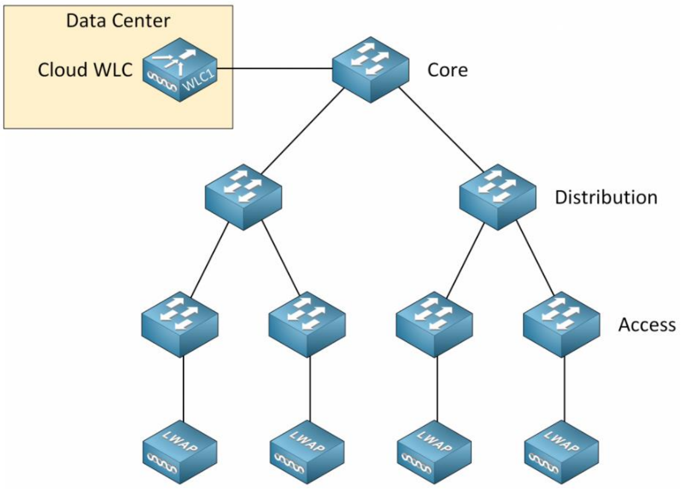
1. Unified WLC Deployment

With the centralized WLC deployment model, the WLC is a hardware appliance in a central location in the network. This deployment is a good choice if the majority of your wireless traffic is destined to the edge of your network, like the Internet or a data center. It's easy to enforce security policies because all traffic ends up in a central location. Another name for this deployment is centralized WLC deployment.



2. Cloud-based WLC Deployment

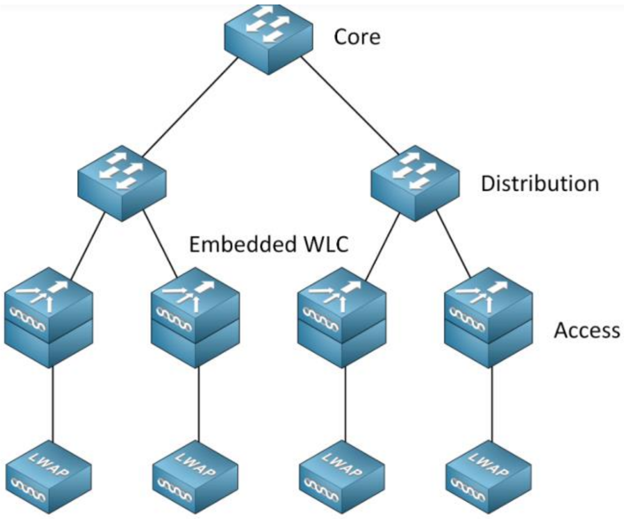
With the cloud-based WLC deployment model, we add the WLC to the data center in a private cloud. With this deployment model, the WLC is a virtual machine, not a physical appliance. It supports up to 3000 APs, so if you need more, you create a second virtual machine.



3. Embedded WLC Deployment

If you have a small number of APs, like in a small campus or branch location, then you can use an embedded WLC in switch stacks. This deployment option is a switch with an integrated WLC, and it supports up to 200 APs.

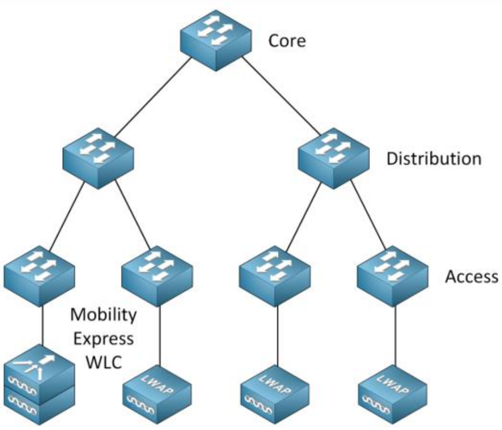
The APs don't have to be physically connected to the switch that hosts the WLC. APs connected to other switches can join the WLC as well. When the number of APs increases, you can add additional switches with embedded WLCs.



4. Cisco Mobility Express WLC Deployment

For small branch offices with only a few APs, even an embedded WLC deployment might be too much. For this situation, you can use a Cisco mobility express WLC deployment.

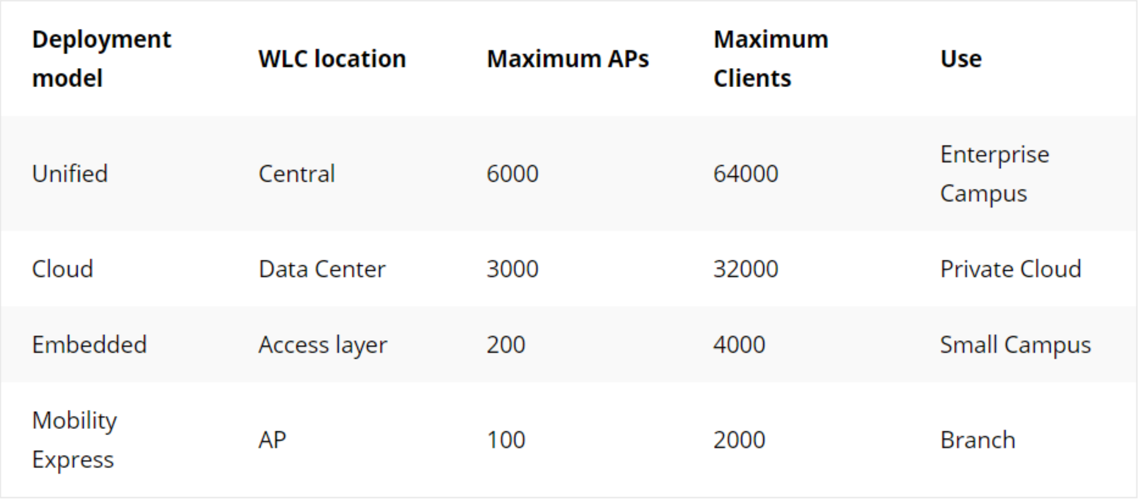
This is a virtual WLC integrated into the AP and supports up to 100 APs. It doesn't support all features that a "normal" WLC supports, but for a small branch network, it might be the right choice.



Conclusions (summary):

Cisco offers different deployment models for WLCs:

- Centralized WLC deployment: Hardware appliance in a central location of the network, like the core layer. Supports up to 6000 APs and is also known as unified WLC deployment.
- Cloud-based WLC deployment: Virtual WLC that runs in a virtual machine, supports up to 3000 APs and is usually deployed in a private cloud at the data center.
- Embedded WLC deployment: An embedded WLC in a switch stack. Useful for smaller sites and supports up to 200 APs.
- Cisco Mobility Express WLC deployment: Virtual WLC that runs on APs. Supports fewer features compared to the full-blown WLC. Supports up to 100 APs.



Deployment model	WLC location	Maximum APs	Maximum Clients	Use
Unified	Central	6000	64000	Enterprise Campus
Cloud	Data Center	3000	32000	Private Cloud
Embedded	Access layer	200	4000	Small Campus
Mobility Express	AP	100	2000	Branch

Wireless LAN 802.11 Service Set

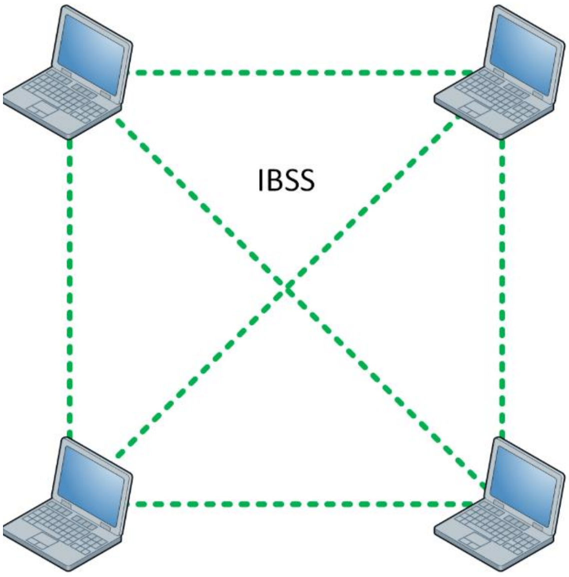
Like wired networks, wireless networks have different physical and logical topologies. The 802.11 standard describes different service sets. A service set describes how a group of wireless devices communicate with each other.

Each service set uses the Same Service Set Identifier (SSID). The SSID is the "friendly" name of the wireless network. It's the wireless network name you see when you look at available wireless networks on your wireless device.

1. IBSS

With an Independent Basic Service Set (IBSS), two or more wireless devices connect directly without an access point (AP). We also call this an ad hoc network. One of the devices has to start and advertise an SSID, similar to what an AP would do. Other devices can then join the network.

An IBSS is not a popular solution. You could use this if you want to transfer files between two or more laptops, smartphones, or tablets without connecting to the wireless network that an AP provides.



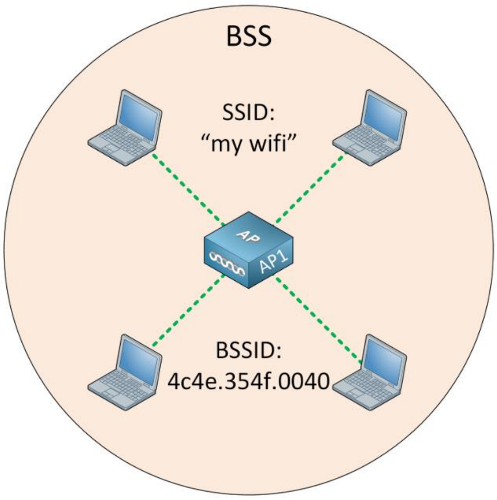
2. Infrastructure Mode

With infrastructure mode, we connect all wireless devices to a central device, the AP. All data goes through the AP. The 802.11 standard describes different service sets. Let's take a look.

2.1 Basic Service Set (BSS)

With a Basic Service Set (BSS), wireless clients connect to a wireless network through an AP. A BSS is what we use for most wireless networks. The idea behind a BSS is that the AP is responsible for the wireless network.

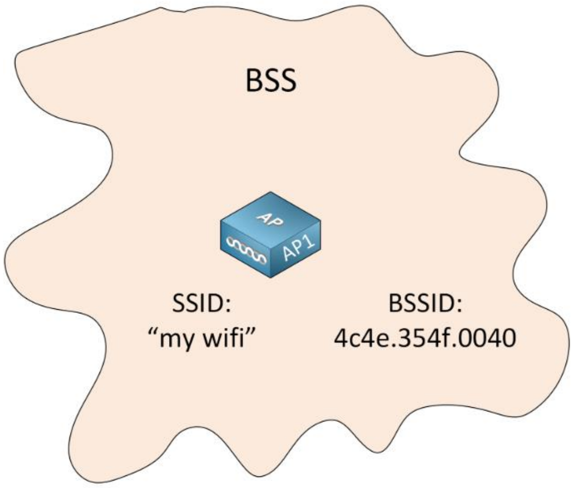
Each wireless client advertises its capabilities to the AP, and the AP grants or denies permission to join the network. The BSS uses a single channel for all communication. The AP and its wireless clients use the same channel to transmit and receive.



The SSID is the "nice" name of the wireless network, and it doesn't have to be unique.

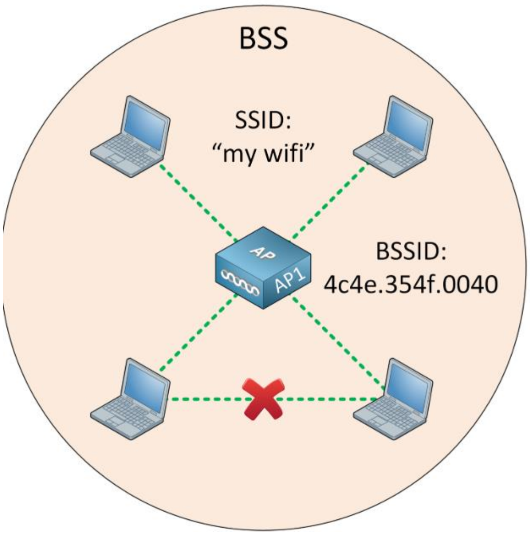
The AP also advertises the **Basic Service Set Identifier (BSSID).** This is the MAC address of the AP's radio, a unique address that identifies the AP. All wireless clients have to connect to the AP. This means the AP's signal range defines the size of the BSS. We call this the **Basic Service Area (BSA).**

In the picture above, the BSA is a beautiful circle. This might be the case if you install your AP somewhere in the middle of a meadow with nothing around the AP. In a building, the BSA probably looks more like this:



When a wireless device wants to join the BSS, it sends an association request to the AP. The AP either permits or denies the request. When the wireless device has joined the BSS, we call it a wireless client or 802.11 station (STA).

All traffic from a wireless client has to go through the AP even if it is destined for another wireless client.



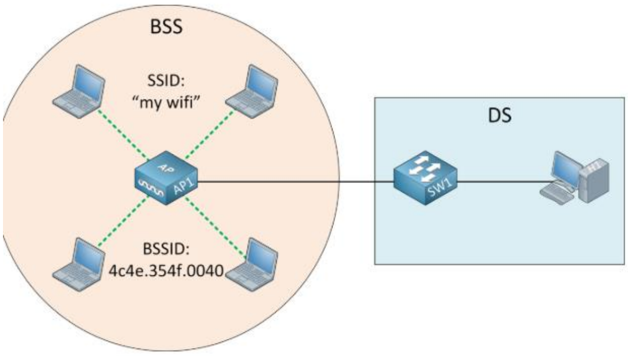
Everything has to go through the AP because the AP is our central point for management, and it limits the size of the BSS. The AP's signal range defines the boundary of the BSS.

2.1.1 Distribution System (DS)

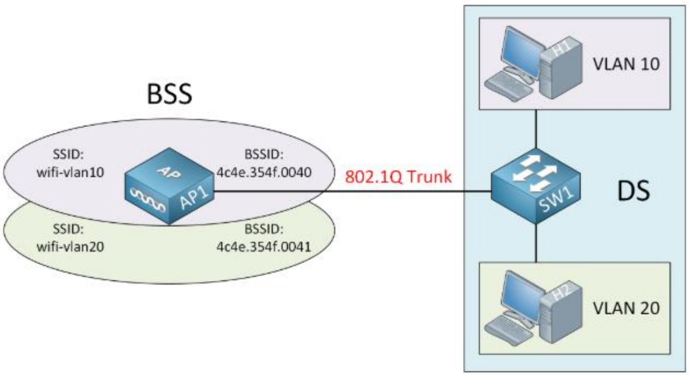
A BSS is a standalone network with a single AP. In the pictures above, there is no connection with a wired network.

Most wireless networks, however, are an extension of the wired network. An AP supports both wired and wireless connections. The 802.11 standard calls the upstream wired network the distribution system (DS).

The AP bridges the wireless and wired L2 Ethernet frames, allowing traffic to flow from the wired to the wireless network and vice versa.



We can also do this with VLANs. The AP connects to the switch with an 802.1Q trunk. Each SSID maps to a different VLAN:



Each wireless network has a unique BSSID. The BSSID is based on the MAC address, so most vendors (including Cisco) increment the last digit of the MAC address to create a unique BSSID.

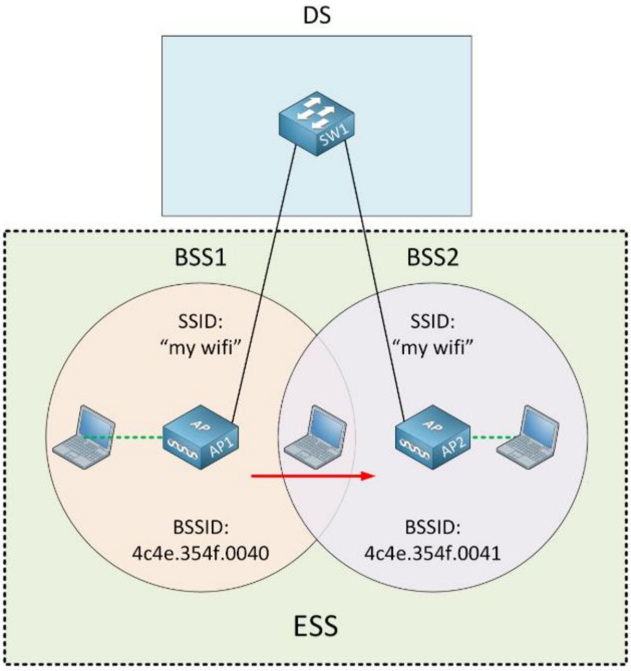
Even though we have multiple wireless networks, they all use the same underlying hardware, radios, and channels. If you have an AP with multiple radios, then it's possible to assign wireless networks to different radios. For example, you could use one wireless network on the 2.4 GHz radio and another one on the 5 GHz radio.

2.2 Extended Service Set (ESS)

A BSS uses a single AP. This might not be enough because of two reasons:

- Coverage: A single AP's signal can't cover an entire floor or building. You need multiple APs if you want wireless everywhere.
- Bandwidth: An AP uses a single channel, and wireless is half-duplex. The more active wireless clients you have, the lower your throughput will be. This also depends on the data rates you support. A wireless client that sits on the border of your BSA might still be able to reach the AP, but can only use low data rates. A wireless client that sits close to the AP can use high data rates. The distant wireless client will claim more "airtime," reducing bandwidth for everyone.

To create a larger wireless network, we use multiple APs and connect all of them to the wired network. The APs work together to create a large wireless network that spans an entire floor or building. The user only sees a single SSID, so they won't notice whether we use one or multiple APs. Each AP uses a different BSSID, so behind the scenes, the wireless client sees multiple APs it can connect to. We call this topology with multiple APs, an **Extended Service Set (ESS).**



APs work together. For example, if you associate with one AP and you walk around the building, you won't disconnect. The wireless client will automatically "jump" from one AP to another AP. We call this roaming. To make this a seamless experience, we need an overlap between APs.

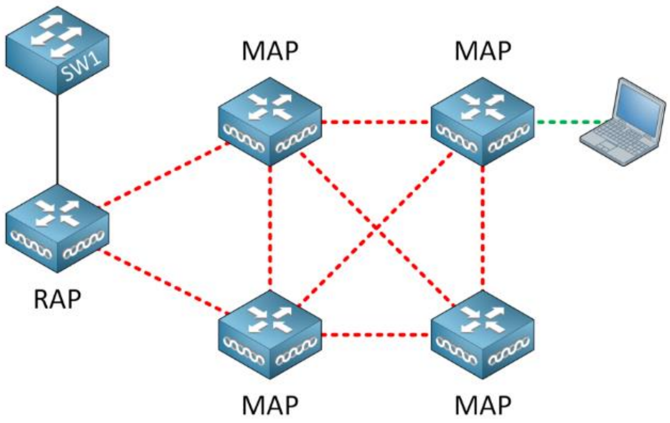
Each AP offers its own BSS and uses a different channel to prevent interference between APs.

2.3 Mesh Basic Service Set (MBSS)

If you want to provide a wireless network for a large area, like a city, then it's not easy to connect each AP to a wired network.

Instead, you could build a mesh network, also known as a Mesh Basic Service Set (MBSS). With a mesh network, we bridge wireless traffic from one AP to another. Mesh APs usually have multiple radios. One radio is for backhaul traffic of the mesh network between APs; the other radio is to maintain a BSS for wireless clients on another channel.

At least one AP is connected to the wired network; we call this the Root AP (RAP). The other APs are Mesh APs (MAP) and are only connected through the wireless backhaul.



There are multiple paths for a MAP to reach the wired network through the RAP, so we need a protocol that finds the best loop-free path. Similar to how spanning-tree works for L2 or routing protocols for L3, there are different wireless solutions. IEEE has the 802.11s standard for mesh networks. Vendors sometimes also use proprietary solutions. For example, Cisco has the Adaptive Wireless Path Protocol (AWPP).

Cisco APs support both indoor and outdoor mesh networks.

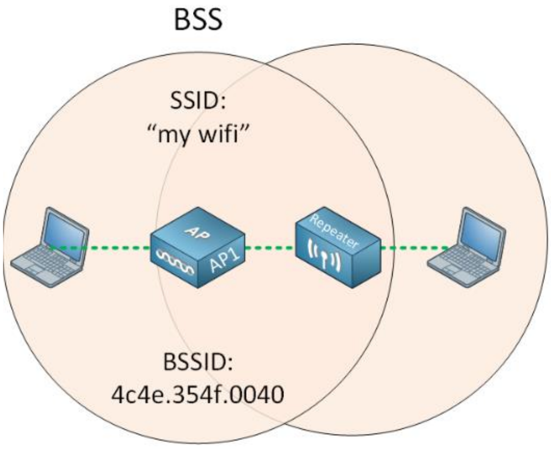
3. AP Modes

Thus far, we have only talked about service sets. Some APs also support different non-infrastructure modes. I'll explain the most common AP modes below.

3.1 Repeater

If you need to cover a large area with your wireless network, you usually create an ESS. An ESS, however, requires wired connections. If it's impossible to connect your AP with a wire, you could configure an AP in repeater mode.

A wireless repeater receives a signal and retransmits it. This allows wireless devices that are not close enough to the AP to join the network.

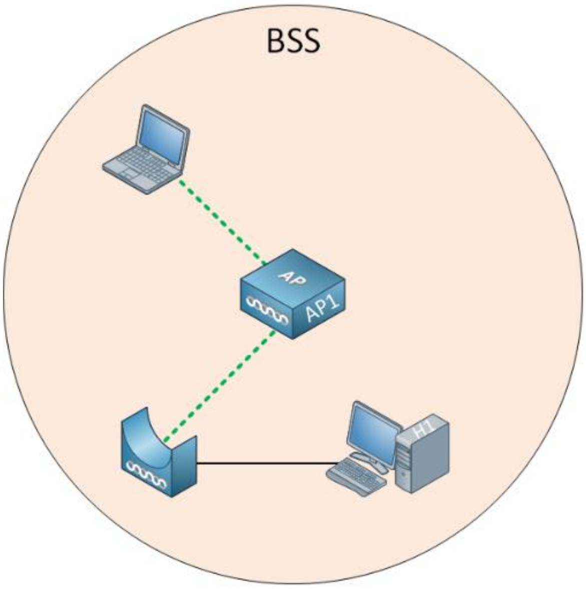


There must be an overlap between the cell size of the AP and the repeater. For optimal performance, it should be about 50%. If the repeater has a single radio, then it will receive and transmit on the same signal as the AP. In this case, the AP will also receive the retransmitted signal. Since wireless is half-duplex, adding a repeater will reduce your available throughput by about 50%.

To work around this, some repeaters have two or more radios. They receive on one channel (same as the AP) and retransmit on another.

3.2 Workgroup Bridge

What if you have a wired device that needs to connect to a wireless network but doesn't have a radio? For example, older printers, computers, or point of sale (PoS) systems. In this case, you can use a workgroup bridge (WGB). The WGB has a wired connection you connect to the wired device and a wireless connection, which it uses to act as a wireless client of a BSS.



There are two types of WGBs:

- Universal workgroup bridge (uWGB): Universal WGB only supports a single wired client. This is based on the 802.11 standards.
- Workgroup Bridge (WGB): WGB (or Workgroup Bridge Mode) is a Cisco proprietary extension to the 802.11 standards and supports multiple wired clients.

3.3 Outdoor Bridge

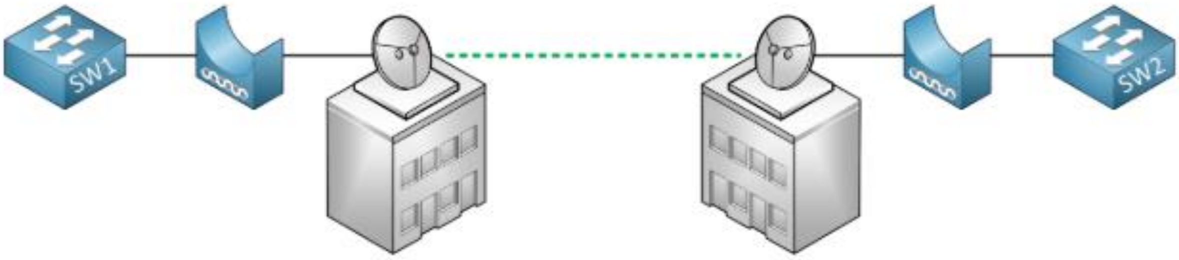
What if you want to connect two buildings, but there is no cable in between, and you don't want to use a WAN? You could use an outdoor wireless bridge. You can configure two APs to create a wireless bridge between two LANs over a longer distance. Wireless bridges between two buildings, and even between two cities are possible.

There are two options:

1. Point-to-point
2. Point-to-multipoint

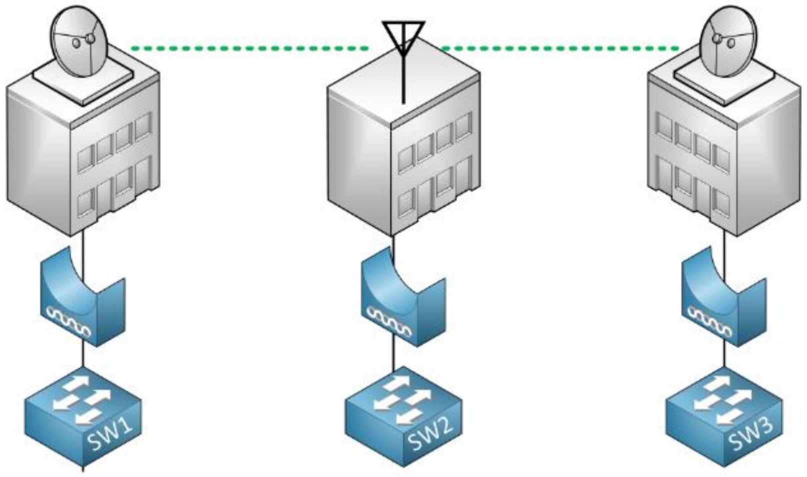
1. Point-to-point

We have two buildings, each with a LAN. The APs are in bridge mode and use directional antennas that focus their signal in one direction, towards the AP on the other side.



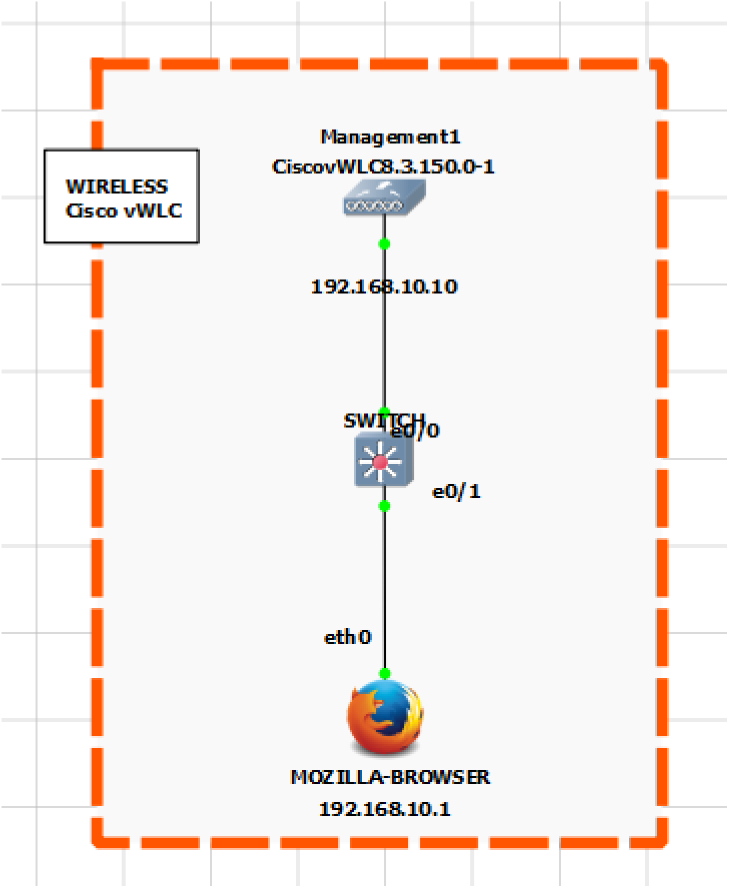
2. Point-to-multipoint

If you want to bridge more than two LANs, you could use a point-to-multipoint bridge.



Cisco Wireless LAN Controller (WLC) Basic Configuration

GNS3 cntr+alt+F5



Let’s take a look at our WLC. When you power it, you see the following boot messages:

```
(Cisco Controller)
```

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:
```

The WLC supports an autoinstall feature that lets you download a configuration file from a TFTP server automatically. We don't need this, so hit enter to select the default option, which is to terminate autoinstall.

We now get a wizard that asks a bunch of questions. If you see anything between brackets, then you can hit enter, and it will select the default option.

First, we set a system name, user name, and password:

```
System Name [Cisco_e0:4e:85] (31 characters max): WIRELESSLC1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): Wireless@1234
Re-enter Administrative Password              : Wireless@1234
```

We don't need link aggregation so we'll hit enter for the next question:

```
Enable Link Aggregation (LAG) [yes][NO]:
```

Now, we need to configure the management interface:

```
Management Interface IP Address: 192.168.10.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.10.254
Management Interface VLAN Identifier (0 = untagged): 10
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 192.168.10.254
```

Our management interface uses VLAN 10 and connects to interface one on the WLC. The following two options are less obvious:

```
Virtual Gateway IP Address: 192.0.2.1

Multicast IP Address: 239.1.1.1
```

Let me explain these two options:

- **Virtual Gateway IP Address:** The WLC has a virtual interface that it uses for mobility management. This includes DHCP relay, guest web authentication, VPN termination, and some other features. The WLC only uses this IP address in communication between the WLC and wireless clients. It has to be a valid IP address but shouldn't be an IP address that is in use on the Internet or your LAN. The 192.0.2.0/24 network is assigned as "TEST-NET-1," so it's a safe choice.

- **Multicast IP Address**: The WLC uses the multicast IP address to forward traffic to APs. You have to make sure you don't use an address that is already in use somewhere else on your network. The 239.1.1.1 multicast address is in the administratively scoped IPv4 multicast space (239.0.0.0/8), so it's safe to use.

We also need to configure a mobility and RF group name:

```
Mobility/RF Group Name: mobility
```

The mobility and RF group names are for WLCs that want to work together. WLCs with the same mobility group name support client roaming and redundancy between WLCs. If you use the same RF group name, WLCs can do Radio Resource Management (RRM) calculations for the entire group.

The next question is to configure an SSID:

```
Network Name (SSID): CCNPENCOR
```

It doesn't matter what you configure here since we are not going to use it anyway.

The WLC sits in between the DHCP server (SW1) and the wireless client, and DHCP bridging mode can make the WLC entirely transparent to the client. We don't need this so we'll leave it disabled:

```
Configure DHCP Bridging Mode [yes][NO]:
```

By default, the WLC permits static IP addresses for clients which is fine:

```
Allow Static IP Addresses [YES][no]:
```

We also can configure a RADIUS server now if we want:

```
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

If you don't, it will give us a warning that the default security policy requires a RADIUS server. Don't worry about this. We can always configure one later.

The next questions are about the country and which wireless standards you want to enable:

```
Enter Country Code list (enter 'help' for a list of countries) [US]: IN

Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
```

Auto-RF lets the WLC figure out which channels and how much power to use. Best to leave it enabled:

```
Enable Auto-RF [YES][no]:
```

Configuring an NTP server is a good idea, but I don't have one in my lab, so I'll manually set the date and time:

```
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: YES
Enter the date in MM/DD/YY format: 10/20/19
Enter the time in HH:MM:SS format: 13:28:00
```

I don't need IPv6 so I'll skip it for now:

```
Would you like to configure IPv6 parameters[YES][no]: no
```

Everything is correct, so make sure you type yes as the final answer:

```
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

The WLC now reboots:

```
Configuration saved!
Resetting system with new configuration...
```

You'll see the entire boot process again:

```
WLCNG Boot Loader Version 1.0.20 (Built on Jan  9 2014 at 19:02:44 by cisco)
Board Revision 0.0 (SN: PSZ18411Q1S, Type: AIR-CT2504-K9) (P)

Verifying boot loader integrity... OK.

[output omitted]
```

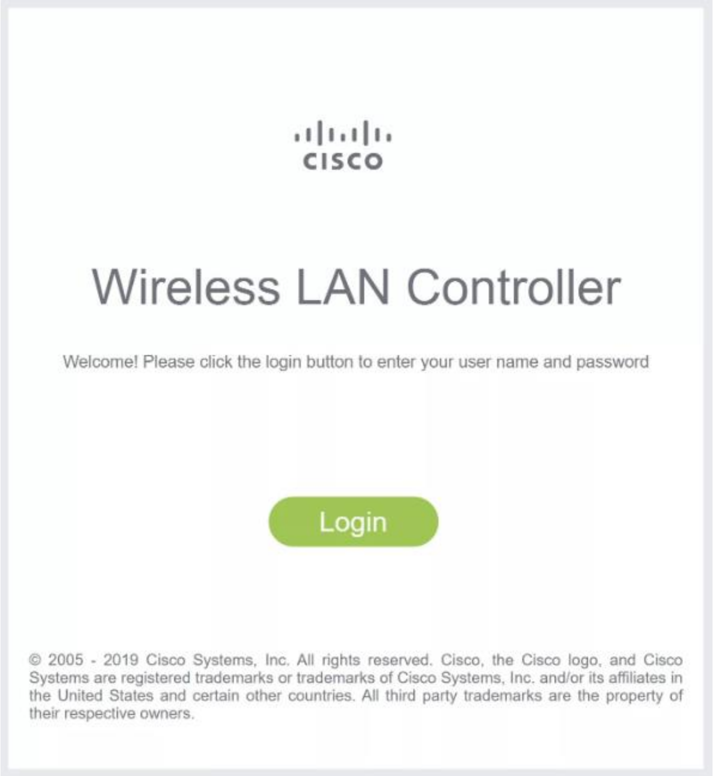
When it's ready, you'll see the prompt, and we can log in:

```
(Cisco Controller)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration to factory defaults)

User:  admin
Password:********
(Cisco Controller) >
```

You can now configure the WLC with the CLI or GUI.

Let's make use of GUI.

Now open your browser and go to http://192.168.10.10. You'll see the following screen:

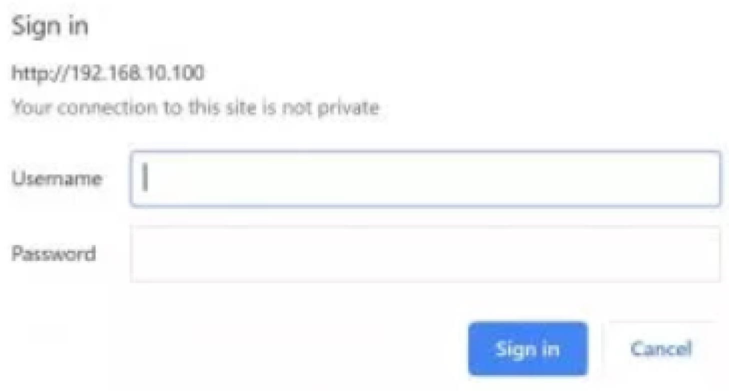


Wireless LAN Controller

Welcome! Please click the login button to enter your user name and password

© 2005 - 2019 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

Enter the username and password we configured with the wizard:

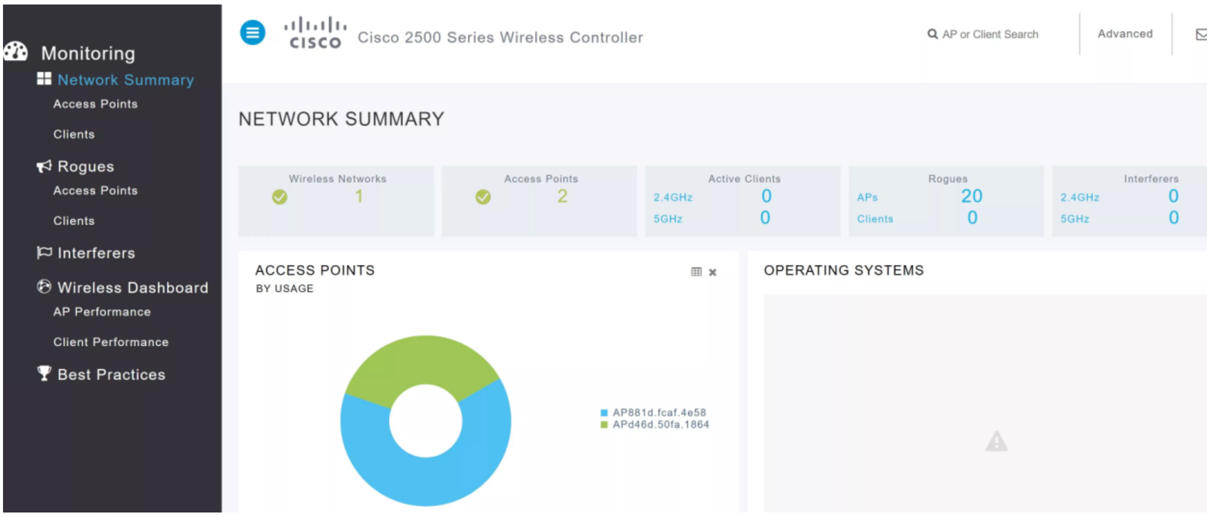


Sign in

http://192.168.10.100

Your connection to this site is not private

You'll now see the monitoring dashboard:



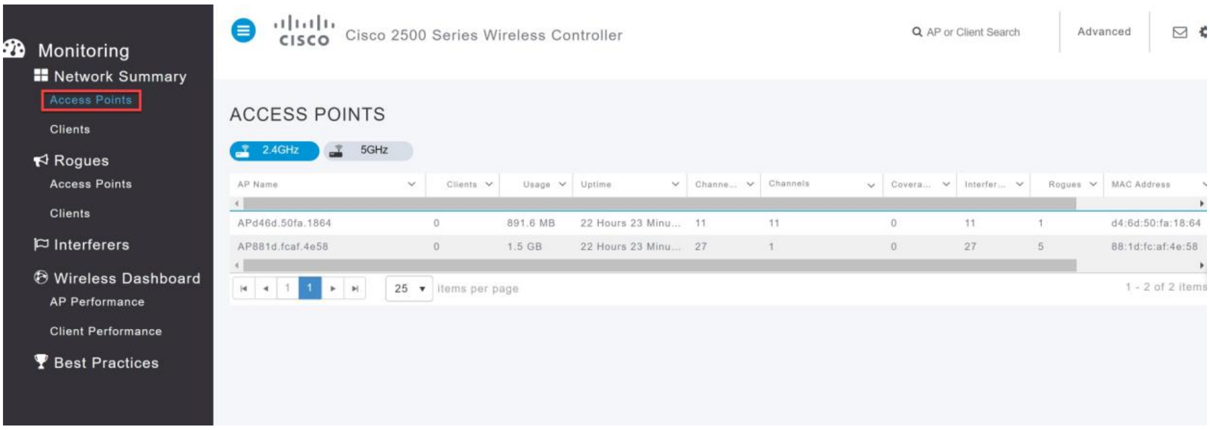
NETWORK SUMMARY

Wireless Networks	Access Points	Active Clients	Rogues	Interferers
✓ 1	✓ 2	2.4GHz 0	APs 20	2.4GHz 0
		5GHz 0	Clients 0	5GHz 0

ACCESS POINTS
BY USAGE

OPERATING SYSTEMS

This dashboard only gives you a basic overview. You'll see the wireless networks, the access points, active clients, etc. For example, here we can find our APs:

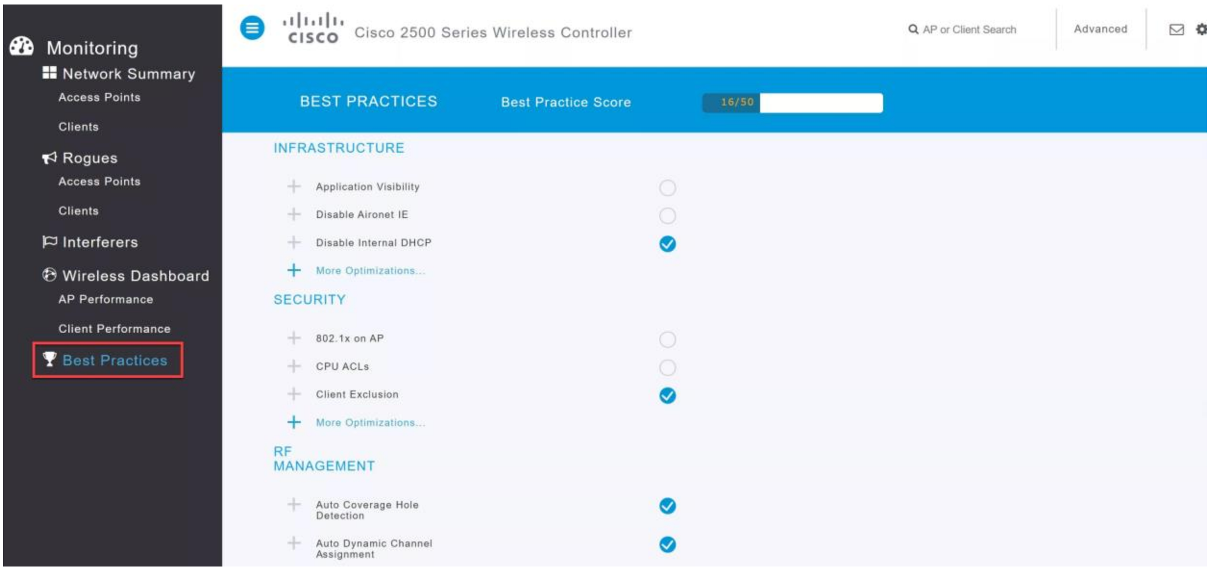


ACCESS POINTS

AP Name	Clients	Usage	Uptime	Channe...	Channels	Covera...	Interfer...	Rogues	MAC Address
APd46d.50fa.1864	0	891.6 MB	22 Hours 23 Minu...	11	11	0	11	1	d4:6d:50:fa:18:64
AP881d.fcaf.4e58	0	1.5 GB	22 Hours 23 Minu...	27	1	0	27	5	88:1d:fc:af:4e:58

25 items per page   1 - 2 of 2 items

At least we know that our APs have joined the WLC. The best practices tab gives you a nice overview of items we should configure:



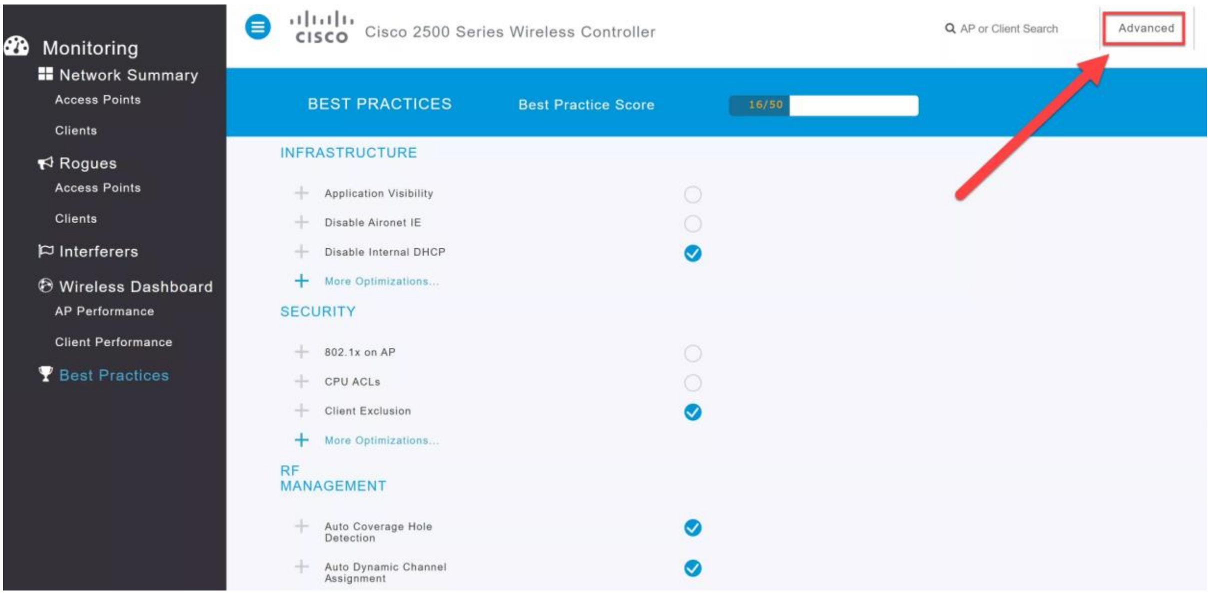
BEST PRACTICES   Best Practice Score 16/50

INFRASTRUCTURE
- Application Visibility ○
- Disable Aironet IE ○
- Disable Internal DHCP ✓
- More Optimizations...

SECURITY
- 802.1x on AP ○
- CPU ACLs ○
- Client Exclusion ✓
- More Optimizations...

RF MANAGEMENT
- Auto Coverage Hole Detection ✓
- Auto Dynamic Channel Assignment ✓

The monitoring dashboard gives you an overview, but if we want to configure anything, we have to use the **advanced mode**. You can find it on the top right:



INFRASTRUCTURE

- Application Visibility ○
- Disable Aironet IE ○
- Disable Internal DHCP ✓
- More Optimizations...

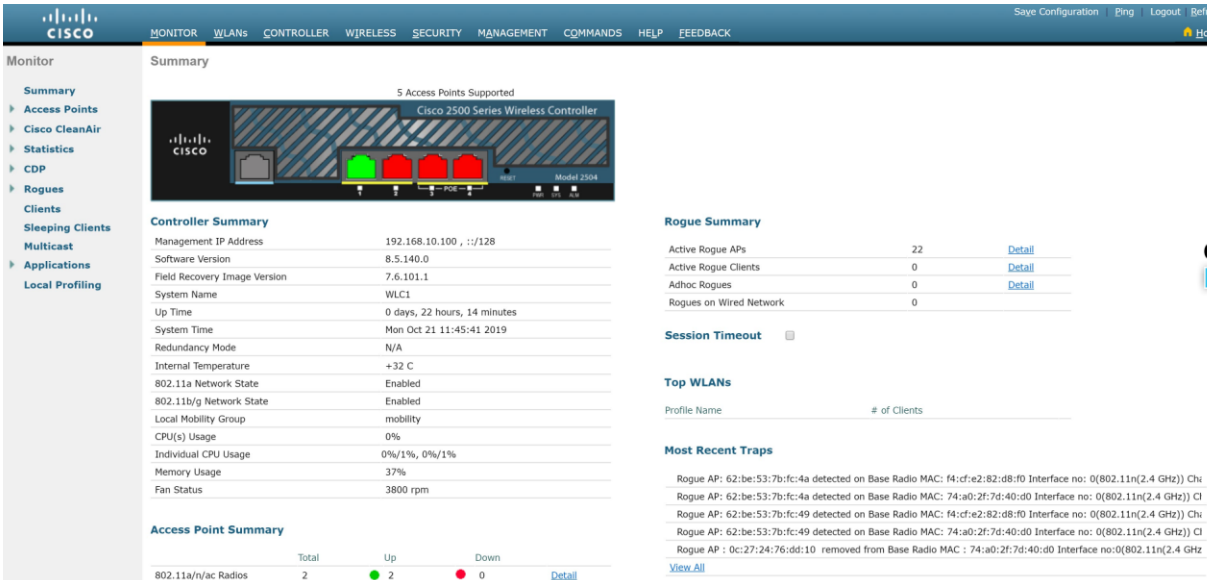
SECURITY

- 802.1x on AP ○
- CPU ACLs ○
- Client Exclusion ✓
- More Optimizations...

RF MANAGEMENT

- Auto Coverage Hole Detection ✓
- Auto Dynamic Channel Assignment ✓

Here’s what advanced mode looks like:



Controller Summary

Management IP Address	192.168.10.100 , ::/128
Software Version	8.5.140.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	0 days, 22 hours, 14 minutes
System Time	Mon Oct 21 11:45:41 2019
Redundancy Mode	N/A
Internal Temperature	+32 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	mobility
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/1%
Memory Usage	37%
Fan Status	3800 rpm

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail

Rogue Summary

Active Rogue APs	22	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Session Timeout □

Top WLANs

Profile Name	# of Clients

Most Recent Traps

```
Rogue AP: 62:be:53:7b:fc:4a detected on Base Radio MAC: f4:cf:e2:82:d8:f0 Interface no: 0(802.11n(2.4 GHz)) Cha
Rogue AP: 62:be:53:7b:fc:4a detected on Base Radio MAC: 74:a0:2f:7d:40:d0 Interface no: 0(802.11n(2.4 GHz)) Cl
Rogue AP: 62:be:53:7b:fc:49 detected on Base Radio MAC: f4:cf:e2:82:d8:f0 Interface no: 0(802.11n(2.4 GHz)) Cha
Rogue AP: 62:be:53:7b:fc:49 detected on Base Radio MAC: 74:a0:2f:7d:40:d0 Interface no: 0(802.11n(2.4 GHz)) Cl
Rogue AP : 0c:27:24:76:dd:10  removed from Base Radio MAC : 74:a0:2f:7d:40:d0 Interface no:0(802.11n(2.4 GHz
```

View All

Cisco Wireless AP Modes

Many Cisco APs can operate in autonomous or lightweight mode; this depends on the image that you run.

An AP that serves wireless clients is in local mode. Besides local mode, there are other AP modes. In this lesson, we'll take a look at each AP mode.

1. AP Modes

1.1 Local

Local mode is the default mode; it offers a BSS on a specific channel. When the AP doesn't transmit wireless client frame, it's still doing something behind the scenes. The AP scans other channels to:

- Measure noise
- Measure interference
- Discover rogue devices
- Check for matches against IDS events

1.2 Monitor

An AP in monitor mode doesn't transmit at all. It's a dedicated sensor that:

- Checks Intrusion Detection System (IDS) events
- Detects rogue APs
- Determines the position of wireless stations

1.3 FlexConnect

It's possible to connect a local mode AP at a remote branch to the HQ's WLC. This works, but it's not a good idea. First of all, the AP encapsulates all wireless client data through the CAPWAP tunnel over the WAN link. Secondly, when the WAN link is down, your wireless network at the branch site is offline too.

FlexConnect is an AP mode for situations like the one above. The AP can locally switch traffic between a VLAN and SSID when the CAPWAP tunnel to the WLC is down.

1.4 Sniffer

An AP in sniffer mode dedicates its time to receive 802.11 wireless frames. The AP becomes a remote wireless sniffer; you can connect to it from your PC with an application like Wildpackets Omnipeek or Wireshark. This can be useful if you want to troubleshoot a problem and you can't be on-site.

1.5 Rogue Detector

Rogue detector mode makes the AP detect rogue devices full-time. The AP checks for MAC addresses it sees in the air and on the wired network.

1.6 Bridge/Mesh

The AP becomes a dedicated point-to-point or point-to-multipoint bridge. Two APs in bridge mode can connect two remote sites. Multiple APs can also form an indoor or outdoor mesh.

1.7 Flex plus Bridge

The AP can operate in either FlexConnect or Bridge/Mesh mode. This AP mode combines the two; it allows APs in mesh mode to use FlexConnect capabilities.

1.8 SE-Connect

An AP in SE-Connect mode dedicates its radios to spectrum analysis on all wifi channels. You can connect to the AP from your PC with applications like MetaGeek Chanalyzer or Cisco Spectrum Expert. This is useful if you want to remotely discover interference sources that you can’t solve with a sniffer.

WIRELESS SECURITY FEATURES

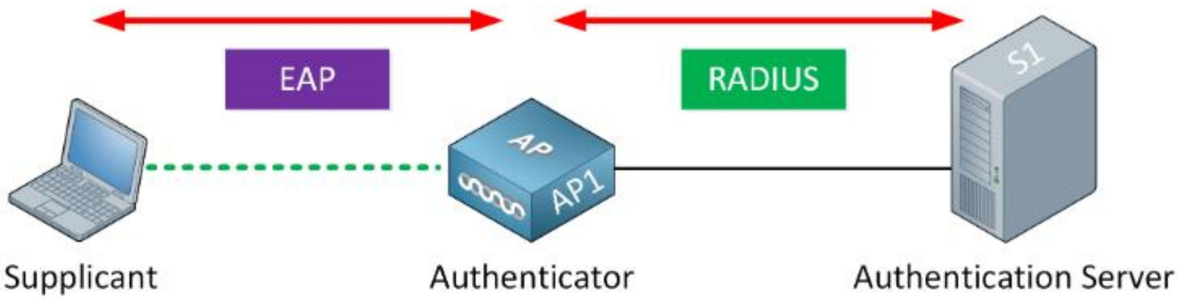
1. 802.1X/EAP

- The original 802.11 standard **only supported open authentication and WEP**. It was time for more secure authentication methods.

- Instead of adding new authentication methods into the 802.11 standard, IEEE chose the **Extensible Authentication Protocol (EAP) framework** to add new authentication options. EAP has functions that multiple authentication methods can use, and it **integrates with 802.1X port-based access control**.

- An 802.1X-enabled port **limits access to the network** until the client successfully authenticates. For wireless networks, it means that a wireless client can associate with an AP, but it won't be able to do anything else until authentication succeeds.

- Here's what 802.1X EAP authentication looks like:



There are three device roles:

- **Supplicant**
- **Authenticator**
- **Authentication Server**

The supplicant (wireless client) uses **open authentication** and associates with the AP. It doesn't end there, though; the supplicant communicates with an external authentication server to authenticate itself. The authentication server is usually a **RADIUS server**. The authenticator in the middle is the AP or WLC, which blocks all traffic, except for authentication traffic. When the authentication server verifies the credentials of the end user, the authenticator unblocks the traffic and permits all wireless traffic.

Now you understand the basics of 802.1X/EAP, let's take a look at some popular EAP authentication methods.

- **LEAP**

Cisco developed a proprietary wireless authentication method called **Lightweight EAP (LEAP)** as an attempt to create a more secure authentication method than WEP (Wired Equivalent Privacy).

- **EAP-FAST**

Cisco developed another EAP method called **EAP Flexible Authentication by Secure Tunneling (EAP-FAST)**.

EAP-FAST protects credentials by exchanging a shared secret generated by the authentication server. This shared secret is called a **protected access credential (PAC) and used for mutual authenticatio**n.

- **PEAP**

Similar to EAP-FAST, **Protected EAP (PEAP)** uses inner and outer authentication. However, instead of a secret, the authentication server presents a **digital certificate** to the supplicant for the outer authentication.

- **EAP-TLS**

PEAP uses a digital certificate to authenticate the authentication server, but clients need to authenticate themselves through MSCHAPv2 or 2GTC.

EAP-TLS goes one step further and requires a **certificate on the authentication server and a certificate on every client.** The authentication server and supplicant authenticate each other using these certificates.

Once authentication is successful, encryption key material is exchanged through the TLS tunnel.

2. Web Authentication on WLAN Controller

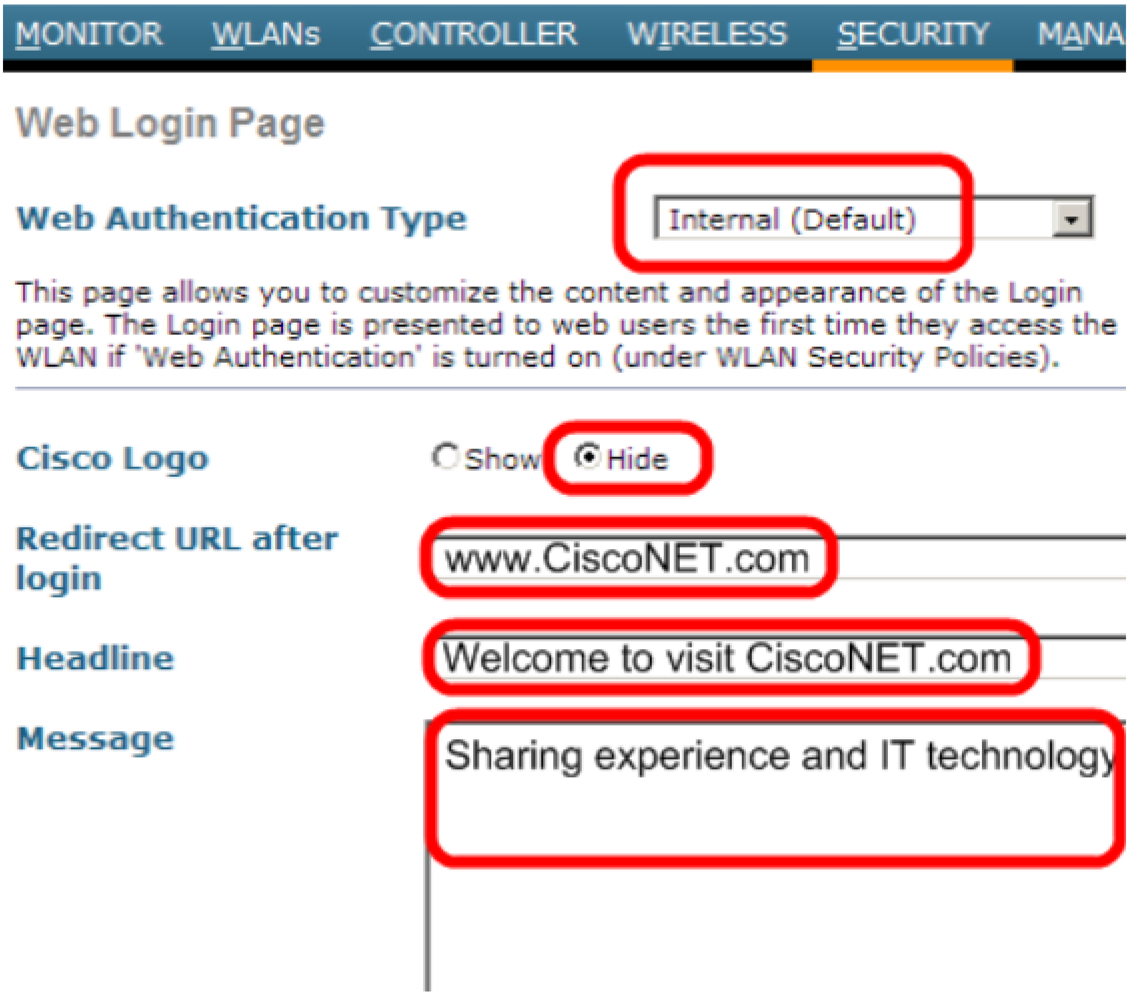
Web authentication (WebAuth) is Layer 3 security. It allows for user-friendly security that works on any station that runs a browser. It can also be combined with any pre-shared key (PSK) security (Layer 2 security policy). Although the combination of WebAuth and PSK reduces the user-friendly portion significantly and is not used often, it still has the advantage to encrypt client traffic. WebAuth is an authentication method without encryption.

WebAuth cannot be configured with 802.1x/RADIUS (Remote Authentication Dial-In User Service) until the WLC Software Release 7.4 is installed where it can be configured at the same time. However, be aware that clients must go through both dot1x and web authentication. It is not meant for guest, but for the addition of a web portal for employees (who use 802.1x). There is not an all-in-one service set identifier (SSID) for dot1x for employees or web portal for guests.

How WebAuth Works

The 802.11 authentication process is open, so you can authenticate and associate without any problems. After that, you are associated, but not in the WLC **RUN** state. With web authentication enabled, you are kept in **WEBAUTH_REQD** where you cannot access any network resource (no ping, and so on). You must receive a DHCP IP address with the address of the DNS server in the options.

You must type a valid URL in your browser. The client resolves the URL through the DNS protocol. The client then sends its HTTP request to the IP address of the website. The WLC intercepts that request and returns the **webauth** login page, which spoofs the website IP address. In the case of an external WebAuth, the WLC replies with an HTTP response that includes your website IP address and states that the page has moved. The page was moved to the external web server used by the WLC. When you are authenticated, you gain access to all of the network resources and are redirected to the URL originally requested, by default (unless a forced redirect was configured on the WLC). In summary, the WLC allows the client to resolve the DNS and get an IP address automatically in **WEBAUTH_REQD** state.



Web Login Page

Web Authentication Type: Internal (Default)

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

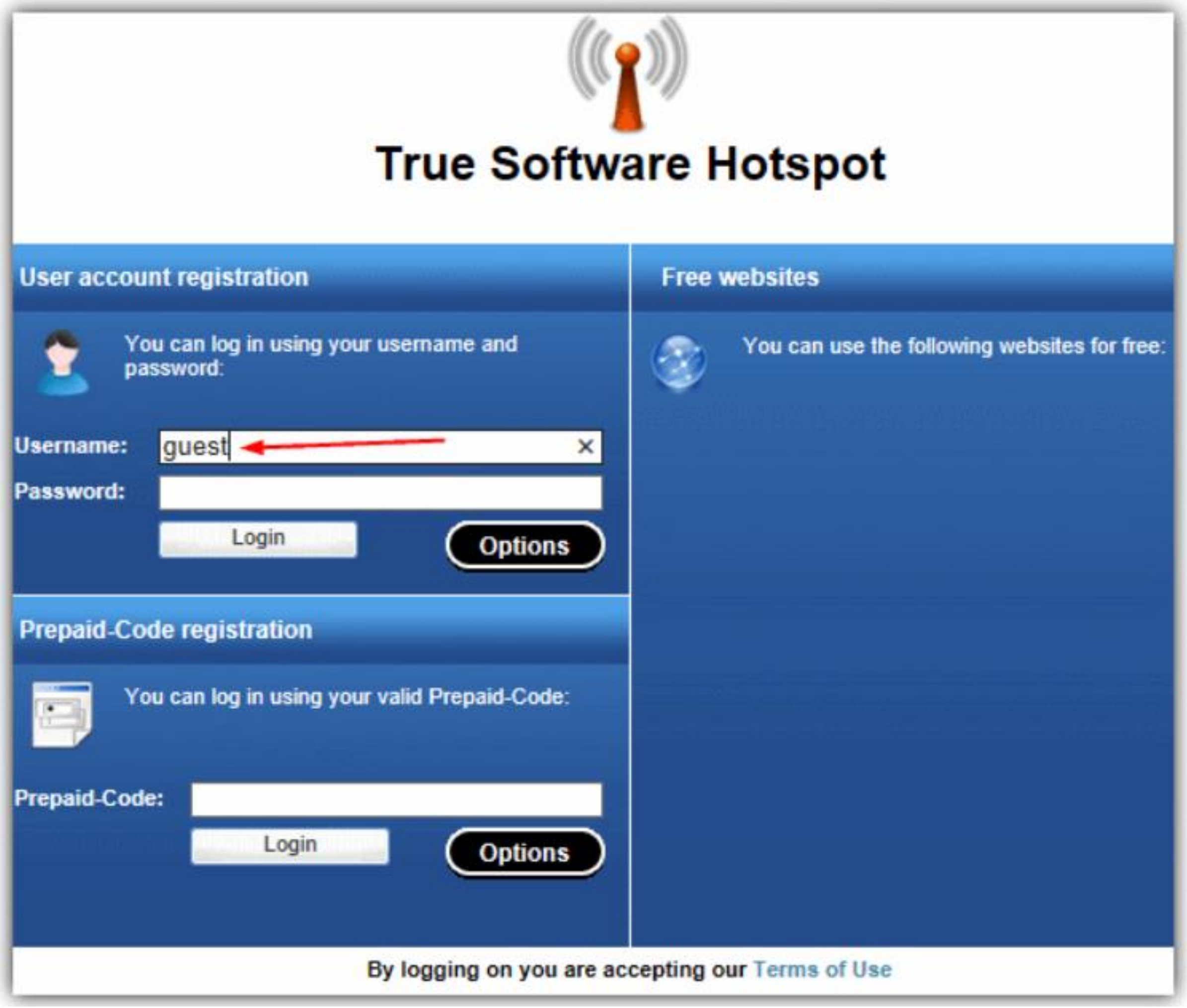
Cisco Logo: ○ Show ● Hide

Redirect URL after login: www.CiscoNET.com

Headline: Welcome to visit CiscoNET.com

Message: Sharing experience and IT technology

EXAMPLE:



True Software Hotspot

User account registration

You can log in using your username and password:

Username: guest

Password:

Prepaid-Code registration

You can log in using your valid Prepaid-Code:

Prepaid-Code:

Free websites

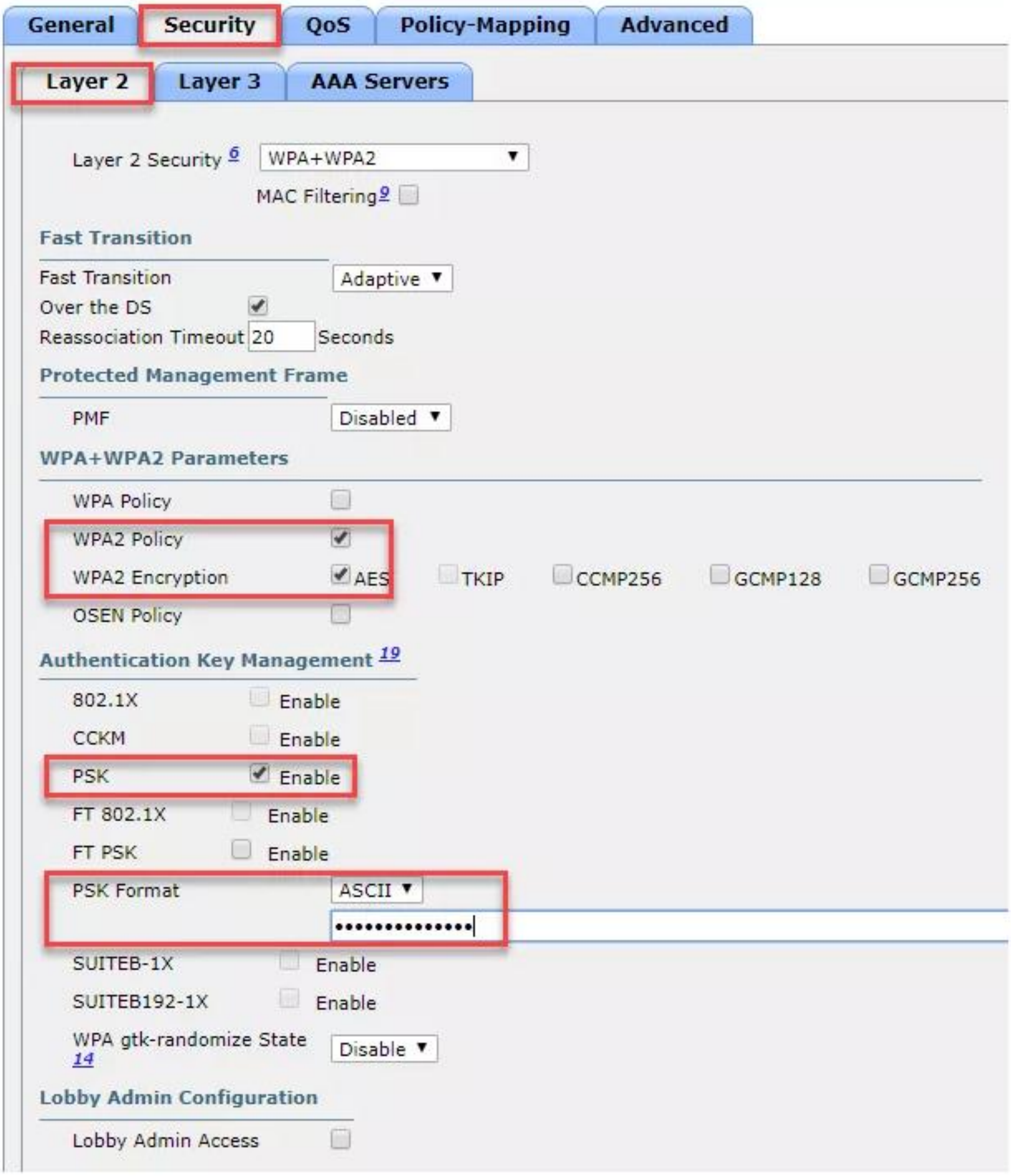
You can use the following websites for free:

By logging on you are accepting our Terms of Use

3. PSK Authentication

You will learn how to configure a basic wireless network that uses **WPA2 Pre-Shared Key (PSK)** authentication.

PSK—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the pairwise master key (PMK) between the clients and the authentication server.



Layer 2 Security 6: WPA+WPA2

MAC Filtering 9 □

Fast Transition

Fast Transition: Adaptive

Over the DS ☑

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP □ CCMP256 □ GCMP128 □ GCMP256

OSEN Policy □

Authentication Key Management 19

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

FT PSK □ Enable

PSK Format: ASCII

••••••••••••••

SUITEB-1X □ Enable

SUITEB192-1X □ Enable

WPA gtk-randomize State 14: Disable

Lobby Admin Configuration

Lobby Admin Access □