Wireless Concepts

80.11b

This is an older wireless standard that enables a maximum data rate of 11 Mbps using the 2.4 GHz unlicensed band. There are well-known sources of interference from commercial devices in that frequency band. Some common examples include microwave, cordless phone, Bluetooth and other wireless devices. Channel allocation is limited with only three non-overlapping channels of 1, 6 and 11. The only selectable channel width available is 20 MHz. There are four available data rates of 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps.

802.11g

This is an enhancement to 802.11b wireless standard that supports a maximum data rate of 54 Mbps using the same 2.4 GHz frequency band. 802.11g wireless standard has higher throughput and increased cell coverage. There are the same interference problems however within that 2.4 GHz band. The same non-overlapping channels 1, 6 and 11 are assignable and channel width of 20 MHz. The modulation enable higher data rates of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 and 48 Mbps.

802.11a

This wireless standard is based on 5 GHz frequency band where there is much less interference. The wider frequency spectrum enables up to 23 non-overlapping channels with the same native channel width of 20 MHz. There is support for a maximum data rate of 54 Mbps. The number of non-overlapping channels and less interference enables higher average throughput. The disadvantage however is that higher frequency creates smaller cells and less coverage. Deploy additional access points for extended cell coverage available.

802.11n

802.11n wireless standard was approved as a paradigm shift in wireless infrastructure. There is support for dual-band operation in both 2.4 GHz and 5 GHz bands. New features such as MIMO and channel bonding have increased data rates from 300+ Mbps to 900 Mbps. The wired-side uplink is Gigabit Ethernet speed now from access point to network switch. Channel bonding creates a single 40 MHz channel from adjacent 20 MHz channels for additional bandwidth.

802.11ac

This wireless standard is an extension to the current 802.11n with higher data rates. It has native support for 5 GHz band and that is where highest data rates are available. Channel bonding width of 80 MHz and 160 MHz are available along with more MIMO spatial streams. 802.11ac does have backward compatibility with 2.4 GHz band however at lower data rates. Wireless operation within 2.4 GHz band is equivalent to an 802.11n access point. From a practical perspective, 802.11ac is the first access point to approach Gigabit Ethernet performance.

Table 1 Wireless Network Standards

Standard	Band	Data Rate	*Channels	Channel Width
802.11b	2.4 GHz	11 Mbps	1,6,11	20 MHz
802.11g	2.4 GHz	54 Mbps	1,6,11	20 MHz
802.11a	5 GHz	54 Mbps	23	20 MHz
802.11n	2.4 GHz	300 Mbps	1,6,11	20 MHz, 40 MHz
	5 GHz	450 Mbps	23	
802.11ac	5 GHz	900+ Mbps	23	20 MHz, 40 MHz 80 MHz, 160 MHz

* Non-overlapping channels represents the number of assignable channels based on minimum channel width selected.

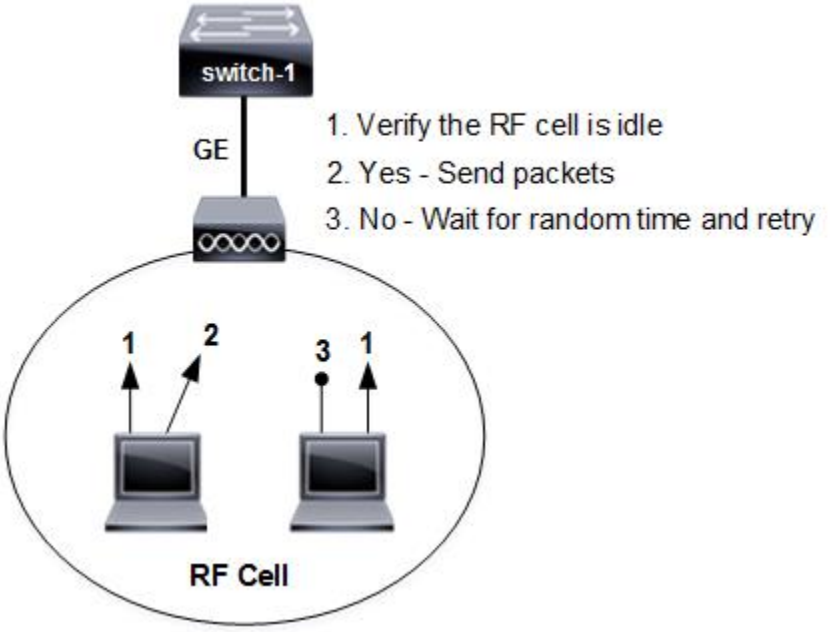
RF Cell Characteristics

There are significant differences between wired and wireless network media. RF wireless cells are shared media with only half-duplex data transmission. Half-duplex mode decreases throughput by 50% compared with wired switch port full-duplex mode. Collisions are eliminated on Gigabit interfaces where there is a collision domain created per port.

Wireless CSMA/CA

This is the wireless media contention protocol that controls when a desktop can send and receive data. It is designed to detect collisions for half-duplex connectivity to the access point. When a collision is detected there is a random wait time assigned before retransmission.

Figure 1 Wireless CSMA/CA



Wireless LAN (WLAN) employs an older less effective carrier sense multiple access with collision avoidance (CSMA/CA). It is required to manage wireless client access to RF cells. Figure 1 shows CSMA/CA operation when multiple clients want to transmit packets. The effect of shared media is collisions, lower throughput, and retransmission.

Data Rate, Distance and Frequency

The average data rate will decrease as wireless clients move further from an access point. The solution is to increase coverage with more access points so that maximum bandwidth is available. The network range will decrease as well for 5 GHz when compared with 2.4 GHz radios. That is a characteristic of higher frequency signals that do not pass through building structure as easy as lower frequencies.

Increasing transmit power on an access point radio will actually decrease range at higher data rates. The effective range is extended although with lower data rates. That does not apply to wireless clients where transmit power should be set at maximum for best results. The network length or maximum distance is 100 meters from access point to switch. Mixed environments such as 802.11b and 802.11g will decrease throughput for both clients as well on the same WLAN assigned.

Channel Assignment

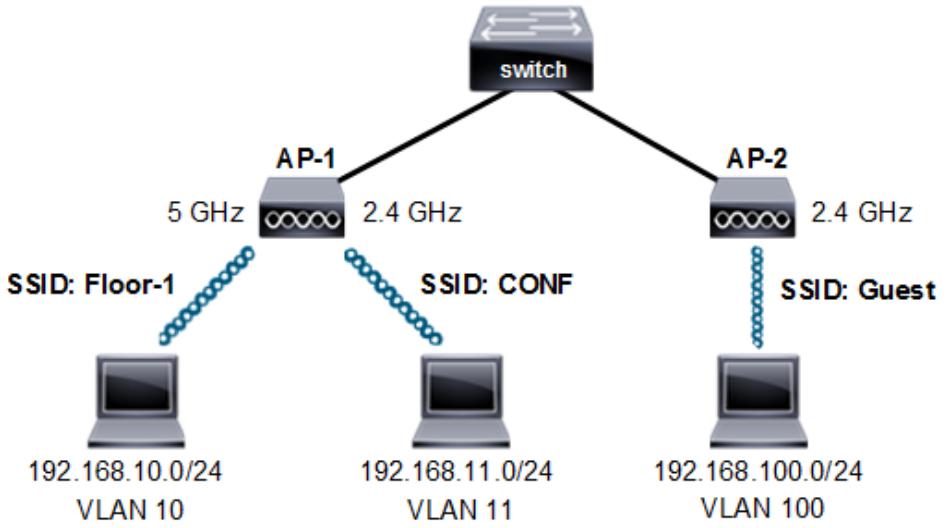
Cisco wireless infrastructure supports both automatic and manual channel assignment. Select Dynamic Channel Assignment (DCA) on wireless controllers for best results. Configuration of a radio policy assigns a frequency band to an RF cell.

As mentioned there are only three (1,6,11) non-overlapping channels assignable from 2.4 GHz band. Channel separation of 20 MHz is required to avoid channel overlap interference. Selecting the wider 5 GHz band will allow more channels for assignment. 5 GHz enables channel bonding of adjacent channels for higher bandwidth (data rate). That reduces the number of non-overlapping channels assignable.

Service Set Identifier (SSID)

Network addressing is a key CCNA topic that extends to wireless infrastructure. The concept of a wireless LAN (WLAN) is defined with a network name called SSID. It advertises an access point presence over a wireless cell to clients. Any wireless clients that are compatible with the access point and know the SSID can associate.

Figure 2 Service Set Identifier (SSID)



Typically there is a wired VLAN that is mapped to an SSID. For example, guest users from Figure 2 would associate to AP-2 using SSID Guest. That same SSID is then mapped to wired VLAN 100 on the wired switch. There is support as well for mapping multiple SSID to a single VLAN.

Anytime you first assign an SSID, there is Basic SSID (BSSID) assigned to that SSID. It is the base MAC address of an access point. The purpose of BSSID is to identify wireless clients with a physical access point. There are often multiple access points and SSID within a wireless domain. Each additional SSID is also associated with a unique BSSID that is calculated by incrementing the base MAC address by one. Cisco supports 32 SSID and 32 BSSID per radio.

Wireless Security

There has been considerable improvements to wireless security with newer authentication and encryption protocols. Wireless access points enable access to network services on the private network. Cisco access points are configurable for various security levels based on requirements. The purpose of wireless security is authentication of user credentials. In addition, data privacy and integrity is enabled across the wireless network with encryption.

SSID Association

Initial communication from wireless client to access point is with SSID. Configuration of any access point starts with creating one or multiple WLANs and assigning a unique SSID to each. There is the option to broadcast SSID name from an access point or select to disable SSID broadcasts. Clients must be configured with the SSID name to associate with an access point. The association of client to an access point is not considered part of any effective security solution. You are permitted access to the wired network unless additional security is enabled.

Open Authentication

This type of authentication security is based on null authentication algorithm. There is essentially no device authentication or user authentication. In fact, wireless clients are granted network access if they know the access point SSID only. Open authentication has an option for configuring static WEP keys as well. The wireless client and access point are configured with the same key string for device authentication. It provides only authentication of client endpoint devices. WEP keys must match between access point and wireless client for network access to be granted. The WEP key is used to encrypt and decrypt client data.

WPA2-PSK (WPA Personal)

The minimum recommended wireless security today is pre-shared keys. Cisco pre-shared key security is branded as WPA2-PSK and available on newer access points. It is wireless security based on a static passphrase configured on an access point and clients. The static passphrase authenticates client devices through a request/response challenge. The passphrase is used as well to generate encryption session keys via AES to encrypt user data. Passphrases should be at least 27 characters to defend against dictionary attacks. Cisco recommends WPA2-PSK for small office/home office (SOHO) only.

Local Authentication (WPA2)

In the wireless domain, Cisco supports wireless client authentication based on local authentication or external RADIUS server. 802.1x EAP authentication protocols are used to manage user authentication. There is Local EAP option on wireless controllers to authenticate wireless clients when a RADIUS server is not deployed or available. If you have selected **Local Authentication** when configuring the controller, then Local EAP is the default. There is an EAP type selected as well for communication between controller and wireless client. Common EAP types include LEAP, EAP-FAST, EAP-TLS or PEAP.

The controller local database is configured with username/password accounts for credentials. This security option is only available with Cisco WPA-Enterprise. Security control is extended to permit or deny specific individuals and/or groups. Client data is still encrypted with dynamic (WPA2) session keys based on AES after user credentials are confirmed. TKIP is no longer supported with Cisco wireless for WPA2 security.

RADIUS Authentication (WPA2)

This is a preferred alternative to local authentication with the most stringent security available. Clients authenticate to an external RADIUS server where user accounts are configured. This security option is only available with Cisco WPA-Enterprise. RADIUS server is configured with EAP authentication and an EAP type selected from LEAP, EAP-FAST, EAP-TLS or PEAP. In addition, there is a secret shared key configured on wireless controller and RADIUS server for device authentication. The following describes how a wireless client authenticates to an external RADIUS server with EAP-TLS.

RADIUS Server Authentication

1. Client associates with access point SSID.
2. Client authenticates RADIUS server certificate.
3. RADIUS server authenticates client certificate.
4. RADIUS sends username and encrypted password request to client.
5. Client sends username and encrypted password to RADIUS server.
6. RADIUS server and wireless client derive dynamic session key.
7. RADIUS server sends dynamic session key to controller.
8. Controller encrypts broadcast key with session key sent to client.
9. Client and access point use session key to encrypt/decrypt packets.

Network access requests sent from host endpoints are forwarded from wireless controller to RADIUS server. There is mutual authentication of client and server based on digital certificates or PAC (shared secret) credentials. Digital certificates are associated with endpoints. Table 1 describes some of the differences between EAP authentication types.

Figure 3 RADIUS Authentication

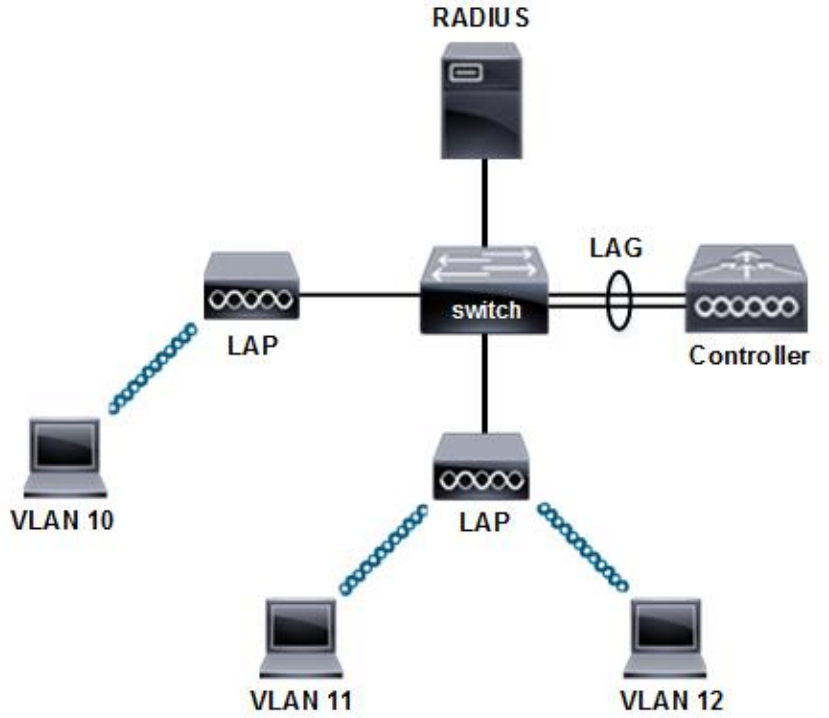


Table 2 EAP Authentication Types

Feature	LEAP	PEAP	EAP-FAST	EAP-TLS
mutual authenticate	yes	yes	yes	yes
digital certificates	no	server-side	PAC	client/server
tunneling	no	yes	yes	no
security level	low	medium	high	high

- LEAP is older, easy to deploy, no certificates.
- PEAP only has server-side certificate.
- EAP-FAST is faster than PEAP and replaces LEAP.
- EAP-TLS certificate management is a disadvantage.

WPA Security Protocols

There are significant differences between wired and wireless media that affect network security. For example, wireless is an open, public, shared media. There is the problem of signal overrun as well where a signal extends beyond the building. Open, shared media is vulnerable to rogue access points as well that advertise SSID to endpoints. Any connection to a rogue server would expose user credentials and data. It is important to have the same unified consistent security from network edge to internet routers. Some of the well-known security attacks include man-in-the middle, and dictionary attacks.

Wi-Fi Protected Access (WPA)

The current wireless standards provide authentication, privacy and message integrity with enhanced security protocols. Cisco enables a variety of different options based on your design. Consider as well that each WLAN (SSID) is assigned a specific security protocol and configuration. You could have for example multiple different security protocol configurations and radio policies for each SSID.

- Authentication of user and endpoint device
- Encryption of security credentials and data
- Message authenticity and integrity

Wi-Fi Protected Access (WPA)

Older security protocol that improved on 64-bit/128-bit static WEP keys. It was the first wireless security protocol to enable user authentication via EAP methods. In addition, dynamic session keys are used instead of static keys. TKIP dynamically generates 128-bit encryption key for each packet. There is message integrity check (MIC) as well to detect and prevent any changes to packet content.

Wi-Fi Protected Access 2 (WPA2)

The WPA protocol standard is backward compatible with older versions. This newer standard improves upon the original WPA with advanced encryption and message integrity check. AES-CCMP (encryption mode) is a single protocol that replaces TKIP for WPA2. There is support for 802.1x EAP authentication of user and wireless endpoints. WPA2 is the current standard for all Cisco wireless equipment.

WPA2 Pre-Shared Keys (WPA2-PSK)

Cisco wireless infrastructure is primarily for most enterprise deployment, however small office/home office (SOHO) is supported as well. It includes remote users, hotspots and small branch. There are less stringent security requirements for SOHO deployments. As a result, pre-shared keys were developed as part of the WPA standard.

Table 3 WPA Certification Standards

Feature	WPA	WPA2	WPA2-PSK	WPA3
Device authentication	EAP	EAP	PSK	EAP
User authentication	EAP	EAP	-	EAP
Encryption mode	TKIP	AES-CCMP	AES-CCMP	CGMP-256
Encryption key	128-bit	128-bit	128-bit	256-bit
Key management	dynamic	dynamic	dynamic	dynamic
Message integrity	MIC	AES-CCMP	AES-CCMP	SHA-2

WPA2-PSK is based on a static passphrase key that must be configured on wireless clients and access points. There is 128-bit dynamic session key generated from the 256-bit shared key. That is used to encrypt session data from wireless clients.

Static passphrase rules permit 8-63 ACII characters. Only wireless device (endpoint) authentication is enabled with pre-shared keys. The same AES encryption is supported since it is WPA2 however it is only client machine authentication. All clients with the same passphrase generate the same session encryption keys as opposed to WPA2 dynamic rotating keys.

Wi-Fi Protected Access 3 (WPA3)

The current wireless standard is WPA3 with improved encryption, message integrity (SHA-2) and replacement of pre-shared keys. There is a newer 192-bit session keys available to counter increased hacker attacks. Data encryption is now 256-bit and based on GCMP-256. In addition, SAE protocol replaces pre-shared keys for SOHO deployments. WPA3 is designed to make dictionary attacks much more difficult along with other well-known hacker attacks. There is a maximum login attempts feature that prevents Cisco is currently in the process of WPA3 certification for wireless hardware.