

Wireless LAN Networks: Wireless Infrastructure Components

Vinh Ho (22 mins)

My topic is "Wireless Infrastructure Components" and that is regarding the wireless networks, which can provide clients mobility, ability to connect from any location, at any time, and the ability to roam while staying connected. A wireless LAN is a classification of wireless network that is commonly used in homes, offices and campus environment. Although it uses radio frequencies instead of cables, it is commonly implemented in the switch network environment and its frame format is similar to Ethernet.

After the lesson, you will be able to describe wireless technology and standards (revision), the components of a wireless infrastructure, as well as wireless technologies. So let's deal with that the wireless concept.

As you know that supporting mobility is one of the topic that you're already familiar with. And as you know productivity is no longer restricted to a fixed work location or defined time period anymore. People now expect to be connected at anytime, at any place from the office, to the airport, or to the home. And the user now expect to be able to roam wirelessly, and roaming enables a wireless device to maintain Internet access without losing connection.

You all know that the benefits of wireless are tremendous. It increases flexibility, productivity, reduces the cost, and is also provide the ability to grow and adapt to a changing environment, and wireless networking can do all of that.

Another thing that you already are familiar with is the wireless technologies. Wireless communication, as you know are used in a variety of professions. Although the mix of wireless technology is continually expanding, the focus of the discussions is on wireless networks that allow user to be mobile.

Broadly speaking, wireless networks can be classify as you can see on the screen: Wireless Personal Area Network, Wireless LAN, Wireless Wide Area Network, Bluetooth, Wi-Fi Wireless LAN, Worldwide Interoperability for Microwave Access, Cellular Broadband, Satellite Broadband. All these networks - wireless networks and really brings great mobility to the user.

Wi-Fi certification, what is it? Wi-Fi certification provides the standard and ensures interoperability between devices make by different manufacturers. Internationally the three organisations influencing Wireless LAN standards are:

- ITU-R that regulates the allocation of the radio frequency spectrum and satellite orbits.
- IEEE specifies how radio frequency is modulated to carry information. It maintains the standards for Local and Metropolitan Area Networks.

- Wi-Fi Alliance is a global, non-profit industry trade association devoted to promoting the growth and acceptance of WLANs. It is an association of vendors whose objective is to improve the interoperability of products that are based on the 802.11 standard by certifying vendors to conformance to industry norms and adherence to the standard.

And as you can see that - a lot of standards for the product compatibility:

- IEEE 802.11a/b/g/n/ac/ad compatible,
- IEEE 802.11i secure using WPA2, and
- Extensible Authentication Protocol (EAP),
- Wi-Fi Protected Setup (WPS) is to simplify device connections.
- Wi-Fi Direct to share media between devices,
- Wi-Fi Passpoint to simplify securely connecting to Wi-Fi hotspot networks,
- Wi-Fi Miracast to seamlessly display video between devices.

Wireless NICs - this is a vital and most important component in the wireless infrastructure. Without a wireless NIC, you cannot access the wireless network, and the wireless deployment requires end devices with wireless NICs, and the infrastructure devices, and Wireless Router, and Wireless Access Point. All of these form very important components in the wireless network.

Wireless home router - a home user typically interconnects wireless devices using a small, integrated Wireless Router. These routers can serve as an Access Point, Ethernet switch or router. And I believe you are very much familiar with all these devices at home.

Business Wireless Solutions

Organizations providing wireless connectivity to their users require wireless LAN infrastructure to provide additional connectivity options. The IEEE 802.11 refers to a wireless client as a station. Most of the small business network you can see in Figure 1 is an 802.3 Ethernet LAN. Each client (ie. PC1) connects to a switch using a network cable, and then switch is the point where the clients gain access to the network. Noticed that the Wireless Access Point also connects to the switch. In this example, either the Cisco WAP4410N Access Point, or the WAP131 AP could be used to provide wireless network connectivity.

Wireless clients use their wireless NICs to discover nearby Access Points by advertising their Service Set ID, SSID. Clients then attempt to associate and authenticate with the AP, as shown in Figure 2 - you can see that the two laptops using wireless cards (NICs) and connect to Wireless Access Point. After being authenticated, wireless users have access to the network resources.

Remember, wireless needs of a small organization differ from those of a large organisation. Large wireless deployments require additional wireless hardware to simplify the installation and management of a wireless network.

Wireless Access Point

The Wireless Access Points can be categorized as either Autonomous APs or Controller-based APs.

Autonomous APs, sometimes referred to as heavy APs, are standalone devices configured using the Cisco CLI or a GUI (Graphical User Interface). Autonomous APs are useful in situations where only a couple of APs are required in the network. Optionally, multiple Access Points can be controlled using Wireless Domain Services (WDS) and managed using CiscoWorks Wireless LAN Solution Engine (WLSE). A home router is an example of an autonomous Access Points because the entire Access Point configuration resides on the device, and you can see it in the first Figure there – (showing) an autonomous Access Point in a small network.

If the wireless demands increase, more Access Points would be required. Each Access Point would operate independently of the other Access Points, and require manual configuration and management.

In contrast to the Autonomous Access Point, if you use Controller-based AP, it's more server-dependent devices and requires no initial configuration. Cisco offers two controller-based solutions. They are useful in situations where many APs are required. As more Access Points are added, each AP is automatically configured and managed by a wireless LAN controller

The second Figure shows you the picture of a Controller –based Access Point in a smaller network. Noticed how the WLAN controller is now required to manage the APs. The benefit of the controller is that it can be used to manage many, many APs.


Small Wireless Deployment Solutions

With the basic concept of the wireless Access Point there, now we talk about the small wireless deployment solutions. Cisco offers the following wireless Autonomous AP solutions:

- Cisco WAP4410N Access Point. This AP is ideal for a small organization requiring two Access Points supporting a small group of users. As you can see that the Cisco WAP4410N can be powered using AC or PoE ('Power over Ethernet'). You can configure them using GUI (Graphical User Interface).
- Another solution is Cisco WAP121 and WPA321. They are mid-level small business Access Points, and can be powered using AC or PoE.
- And then you have the Cisco AP541N. This is a mid-level small business Access Point. It is ideal for small- to medium-sized organizations that want robust and an easily manageable cluster of Access Points.

Most enterprise-level Access Points support Power over Ethernet.

Each WAP4410N Access Point can be configured and managed individually. However, in this small wireless deployment solution, only two WAP4410N are required. But when you need more Access Points, then it become a problem.



In order to provide a better solution in that situation, Cisco provides WAP121, WAP 321, AP541N Access Points to support what we call the clustering of APs without the use of a controller. The cluster provides a single point of administration and enables administrator to view the deployment of APs as a single wireless network, rather than a series of separate wireless devices. The clustering capability makes it easy to set up, configure, and manage a growing wireless network. Multiple APs can be deployed and push a single configuration to all the devices within the cluster, managing the wireless network as a single system without worrying about interference between Access Points, and without configuring each AP as a separate device.

Specifically, the WAP121 and WAP321 support Single Point Setup (SPS), which makes AP deployment easier and faster. It helps to enable the wireless LAN to scale up to four WAP121 and up to eight WAP321 devices to provide broader coverage and support additional users as business needs change and grow.

Cisco AP541N AP can cluster up to ten APs together and can support multiple clusters. A cluster can be formed between two APs if the following conditions are met:

- Clustering mode is enabled on the APs.
- The APs joining the cluster must have the same Cluster Name.
- The APs are connected on the same network segment.
- The APs use the same radio mode, for example, both use 802.11n.

Large Wireless Deployment Solutions

What happened to the large wireless deployment solutions? What can the large wireless deployment solutions offer?

For larger organization with many Access Points, Cisco provides Controller-based managed solutions, including the Cisco Meraki Cloud Managed Architecture and the Cisco Unified Wireless Network Architecture.

Cisco Meraki Cloud Managed Architecture is a management solution used to simplify the wireless deployment. Using this architecture, APs are managed centrally from a controller in the cloud.

Cloud networking and management provides centralized management, visibility, and control without the cost and complexity of controller appliances or overlay management software. This process reduces costs and complexity. The controller pushes management settings, such as firmware updates, security settings, wireless network, SSIDs settings to the Meraki APs.

Cisco MR (Meraki) Cloud Managed Wireless APs, Meraki Cloud Controller (MCC), Web-based Dashboard - all of these provide a better solution for the large wireless organisations.

Wireless Antennas

Talking about wireless antennas, which are also essential components of a wireless infrastructure. Wireless antennas - most business required by using the external antennas to make them fully functional unit.

Cisco has developed antennas specifically designed for use with 802.11 APs, while accommodating specific deployment conditions, including physical layout, distance, and aesthetics.

You can see that Cisco Aironet APs can use Omnidirectional Wi-Fi antennas. Factory Wi-Fi gear often uses basic dipole antennas similar to those used on walkie-talkie radios. Omnidirectional antennas provide 360-degree coverage, and are ideal in open office areas, hallways, conference rooms, and outside areas.

Directional Wi-Fi Antennas focus the radio signal in a given direction, that's why we call a directional. This enhances the signal to and from the AP in the direction the antenna is pointing. Therefore, it provides stronger signal strength in one direction, but less signal strength in other directions.

Finally, the Yagi antennas, this type of directional radio antenna that can be used for long-distance Wi-Fi networking. These antennas are typically used to extend the range of outdoor hotspots in a specific direction, or to reach an out building.

You can see that the figure displays various Cisco indoor and outdoor antennas.

IEEE 802.11n/ac/ad use MIMO technology to increase the availability of the bandwidth. MIMO means Multiple-Inputs Multiple-Outputs technology. Specifically, MIMO uses multiple antennas to exchange more data than it would be possible using a single antenna. Up to four antennas can be used to increase throughput.

Remember, not all wireless routers are the same. For instance, entry level 802.11n routers support 150 Mbps bandwidth using one Wi-Fi radio, and one antenna attached to the unit. To support the higher data rates, an 802.11n router requires more radios antennas to manage more channels of data in parallel. For example, two radios and two antennas to an 802.11n router support up to 300 Mbps, while 450Mbps and 600 Mbps require three and four radios and antennas, respectively.

802.11 Wireless Topology Modes

Now we come to the essential of the topic at the moment, that is, the 802.11 wireless topology mode. 802.11 wireless technology identifies two main wireless topology modes. One is Ad hoc, and the other is Infrastructure Mode

On your screen you can see the Ad hoc Mode. The Ad hoc Mode is used when two devices connect wirelessly without the aid of an infrastructure devices, such a wireless router or Access Points, for example, using Bluetooth or Wi-Fi Direct connect to each other. You can see that between the two devices, there's no AP, no wireless router, and we call that mode is Ad hoc Mode.

The second mode is the 802.11 Wireless Infrastructure Mode. The Infrastructure Mode is used when wireless clients interconnect via a wireless router or AP, such as in WLANs. APs connect to the network infrastructure using the Wired Distribution System (DS), such as Ethernet.

You can see on the screen there, the wireless Access Point connect to the LAN switch – the distribution system there, and it provides wireless network to the wireless clients. In this topology, we call it Infrastructure Mode.

Let's go into a bit more detail with the Ad hoc Mode. So with Ad hoc Mode, wireless network is when two wireless devices communicate in a peer-to-peer (P2P) manner without using access point wireless router. For example, a client workstation with wireless capability can be configured to operate in Ad hoc Mode enabling another device to connect to it using Bluetooth or Wi-Fi Direct.


Remember, IEEE 802.11 standard refers to an Ad hoc Mode network as an Independent Basic Service Set (IBSS). You can see the figure display a summary of the Ad hoc Mode. A variation of the Ad hoc topology is when a smartphone or tablet with cellular data access is enabled to create a personal hotspot. This feature is sometimes referred to as Tethering, a temporary quick solution that enables a smartphone to provide the wireless services to a Wi-Fi router. Other devices can associate and authenticate with the smartphone to use the Internet connection. The Apple iPhone refers to this as the Personal Hotspot feature, while Android devices refer to as either Tethering or Portable Hotspot.

Infrastructure mode. The IEEE 802.11 architecture consists of several components, that interacts in a WLAN that supports clients. It defines two Infrastructure Mode topology building blocks. One is call Basic Service Set (BSS), and the other is Extended Service Set (ESS).

On the screen you can see that is the Basic Service Set topology. BSS consists of a single AP interconnecting all the associated wireless clients. In the figure, two Basic Service Sets are displayed. The circles depict the coverage area within which the wireless clients of the BSS may remain in communication. This area is called the Basic Service Area (BSA). If a wireless client moves out of its BSA, it can no longer directly communicate with the other wireless clients within the BSA. The BSS is the topology building block while the BSA is the actual coverage area. The terms BSA and BSS are often used interchangeably.

The Layer 2 MAC address of the AP is used to uniquely identify each BSS, which is called the Basic Service Set Identifier (BSSID). Therefore, the BSSID is the formal name of the BSS and is always associated with only one AP.

The second topology is Extended Service Set. When a single BSS provides insufficient RF coverage, two or more BSSs can be joined through a common distribution system (DS) into an ESS. An ESS is the union of two or more BSSs interconnected by a wired distribution system. Wireless clients in one BSA can now communicate with wireless clients in another BSA within



the same Extended Service Set. Roaming mobile wireless clients can now move from one BSA to another and seamlessly connect.

The rectangular area depicts the coverage area within which members of an ESS may communicate. This area is called the Extended Service Area (ESA). An ESA typically involves several BSSs in overlapping and/or separated configurations.

Each ESS is identified by an SSID. For security reasons, additional SSIDs can be propagated through the ESS to segregate the level of network access. Remember, the 802.11 standard refers to Ad hoc Mode as an IBSS.