While the demand for Wi-Fi access is increasing, more and more wireless Access Points (APs) are used in the network to ensure signal coverage in campuses, schools, or organization buildings, which makes the network operations & maintenance difficult for administrators.

An accesspoint was a standalone box which transmitted and received WiFi. These were configured individually. They were said to be automonous. When you had lots of these boxes you could roam across from one to another. There was a maximum of 32.

The idea of the WLC was a centralised administration which controlled all the access points and were said to be light weight.

All traffic would come back to the WLC before passing it the network. Over time other enhancements were added but that is the basics.

Wireless Access Controllers (WL[A]Cs) are running and administrating the multiple wireless access points. The wireless access point (AP) has lost the intelligent characteristic, while the wireless access controller turns into the new brain for WLAN.

In the case of the Wireless LAN network, also known as WLAN, you can use the WLC or Wireless LAN Controller, whose purpose is to centralize the control of Access Points (APs).

So that you can understand this better, let’s put it this way: what a wireless Access Point (AP) does for your network is similar to what an amplifier does for your home stereo. It takes the bandwidth coming from a router device and extends it so that multiple other devices can connect from farther distances away

What Is a Wireless LAN Controller (WLC)?

A Wireless LAN Controller (WLC) is a centralized device in the network which is used in combination with the Lightweight Access Point Protocol (LWAPP) to manage lightweight access points in large quantities by the network administrator or network operations center.

Also called “fat” access points, these access points on the network are managed, operated, and configured independently. The WLC automatically handles the configuration of wireless access points.

Because of its centralized position and brainpower, the Wireless LAN Controller is aware of the wireless LAN environment. It provides services that can lower the price of deployment, ease the management process, and provide several layers of security.

the WLC role is to : dynamic channel assignments. transmit power optimization. client roaming improvements. dynamic client load balance between 2 APs. RF and Security monitoring and ...

Does My Company Need Wireless LAN Controller (WLC)?

The Wireless LAN Controller (WLC) – Lightweight Access Point (LWAP) setup is commonly utilized in the company environment to stretch an individual wireless network in a vast geographical region. This setup lets users stroll the office premise, campus, or building and still be connected to the network.

When deploying enterprise WLANs, every single wireless access point is initially created and managed separately from other APs on the same network. In other words, each AP must run individually, which makes centralized management difficult to realize.

Unfortunately, technical problems and unstable network conditions can be caused by the lack of communication between these Access Points (APs). The solution? Wireless LAN Controllers (WLC) meant to solve the mentioned problems above once for all. Accompanied by fit mode APs, Wireless LAN Controllers (WLC) can help to realize efficient and simplified network management.

Functions of Wireless LAN Controller

As we said before, the major function of a wireless LAN controller (WLC) is to maintain the configuration of wireless Access Points (AP), but it carries out multiple other functionalities:
#1. Traffic aggregation and processing for wireless devices function

It is important to know that this function is not all the time performed inside the WLC, for this it will depend on the network architecture used. When all traffic from wireless devices is routed via the controller, you can use it to encode it or divide it so that is sent to different networks or to be filtered to prioritize it according to the established quality policies.
#2. Management and operation function

These two functions enable you to utilize and manage the wireless local network in a much simpler manner. This way you don’t have to repeat the same operations in every one of the APs within the local networks anymore. These tasks allow you to configure, observe and identify problems in the network and they also permit you to send and receive notifications when problems are noticed.

#3. Local wireless function

In the case of the radio features of wireless technology, it is preferable to utilize the coordination and protection mechanisms in the radio spectrum for more efficient use in a particular area.

The mechanisms aimed at optimizing the distribution of traffic between APs and wireless devices can recognize interference and by using radio triangulation mechanisms can locate geographically the devices.

Benefits of a Wireless LAN Controller

It is secure. With all the daily news about hacking and data breaches, security is an essential factor to have in mind for any organization. Wireless LAN Controller (WLC) fights against all kinds of threats to your organization based on user ID and location thanks to built-in security characteristics.
It is centralized. A centralized wireless controller provides malleability for deployment, which will lower the budget, planning instruments, and time spent organizing a wireless network in the business.
It is simple. Having a Wireless LAN Controller (WLC) will help you to administer and supervise your access points in the centralized hub.

A Wireless LAN Controller (WLC) gives the network administrators the ability to see all the data and information linked to the network. They are able to observe on the device the hardware status, the situation of the physical ports, and a summary of the Access Points (APs) connected anytime they want.

Does the size of a controller matter?

Simply put: yes. It's important to choose the right type of deployment and to make sure your controller matches the size of your organization.

Usually your choice of controller will depend on the number of devices that typically attach to a wireless network. A large office building that has hundreds of workers has different needs than a small business.

Some controllers, such as the Catalyst 9800-80 Wireless Controller, are built to handle the traffic of a large organization. That same controller would be overkill for a small business. Similarly, a controller like the Cisco 3504 Wireless Controller is intended for smaller business offices and manages a few access points--it would never be able to handle the day-to-day activity of a large enterprise.

Does my organization need a WLAN controller?

Not necessarily. If your business is a small to medium-sized, if you don't have a highly skilled IT manager, or if you are on a budget, Cisco Mobility Express may be the answer.

Mobility Express, unlike a typical network, is a controllerless device. What this means is that a WLAN controller is embedded in the access point. You are able to manage the entire Wi-Fi network through an access point.

Mobility Express is easy to manage but also easy to deploy on your wireless network, including guest access. It takes under 10 minutes to deploy.

How do WLAN controllers fit into intent-based network?

Cisco's wireless controllers are a key component of intent-based networking. This means that with an intent-based network from Cisco, your network grows more intuitive every day, because it is informed by context and powered by design.

Benefits of a Cisco WLAN controller

Cisco WLAN controllers are state-of-the-art. They all adhere to the 802.11ac Wave 2 standard and the Catalyst controllers are ready for the upcoming standard. All controllers have fast, optimized network performance.

Flexible

Flexibility is also paramount. Cisco can help scale a small, medium-sized, or large enterprise network, whether your solution involves a cloud-based controller, or an on-premises controller designed to handle your organization's needs. Catalyst cloud controllers are able to be deployed in either the public or private setting.

Secure

Security is another important consideration for any organization, with hacking and data breaches in the news every day. Cisco WLAN controllers battle all kinds of threats to your business based on user ID and location thanks to built-in security features.

Always on

Cisco Catalyst controllers are always on meaning that they limit your network’s downtime and allow for upgrades and patches to be deployed while the network is still running.

Simple

Finally, Cisco provides simplicity. With a Cisco WLAN controller, your network has a centralized hub where you can manage and control your access points.

Access Points and Wireless LAN Controllers Explained

This tutorial explains the functionalities of the Access points and the Wireless LAN controllers in detail. Learn what the Access points and the Wireless LAN controllers are and how they work in the wireless network.

This tutorial is the part of the CCNA Study Guide. It explains the following CCNA topic.

Describe the impact of infrastructure components in an enterprise network.

- Access points
- Wireless controllers

Access point

An access point is the device that allows multiple wireless devices to connect with each other. Just like a HUB or switch connects multiple devices together in a single or multiple wired LAN networks, an access point connects multiple wireless devices together in a single wireless or multiple wireless networks. An access point can also be used to extend the wired network to the wireless devices.

access point in wireless and in wired network

Based on the functionalities, we can categorize the access point in three types; standalone access point, multifunction access point and controlled access point. Let’s understand each type in detail.
Standalone access point

A standalone access point provides the same functionality in wireless network which a switch or hub provides in the wired network. It provides connectivity between the different wireless devices. It accepts frame from the connected device and, based on its physical address, forwards it to the destination device.

Both the wired network and the wireless network use the different networking standards. Wired network uses the Ethernet standards while the wireless network uses the IEEE802.11 or Wi-Fi standards.

A device which only understands and supports the one type of standards from the Ethernet standards and the Wi-Fi standards cannot process the frame that is formatted in the other type of standards. For example a regular Ethernet switch neither understands the frame formatted in Wi-Fi standards nor processes it.

Access point supports both standards. Based on the destination device, it converts the received frame before forwarding it. For example if it receives a frame that is formatted with the Wi-Fi standards and have a destination address that uses Ethernet standards, it formats that frame with Ethernet standards before forwarding it to the destination.

how access point forward frames

Access point uses radio signals for connectivity. Any device which falls in its signal range can connect with it. This feature makes it more flexible but less secure in comparison with the regular Ethernet switch.

To enhance the security and stop the unauthorized access, the Access point uses authorization feature. Based on the security and the flexibility requirements, it can be configured to allow all users or to the selected users.

Multifunction Access Point

A multifunction access point is the combination of two or more devices. In this combination an additional device or devices are merged with the access point to provide the additional functionalities along with existing functionality of the access point. A wireless router which ISP uses to provide to the Internet connection is the perfect example of the multifunction access point. It consist of three devices; an access point, a regular Ethernet switch and a router.

Controlled Access Point

A controlled access point works as the client of the Wireless LAN Controller (WLC). Technically a controlled access point is known as the Lightweight Access Point (LWAP). LWAP doesn’t take any forwarding decision. Upon receiving a frame from the connected device, instead of forwarding it to the destination device, it forwards that frame to the WLC. The WLC, based on the security configuration, makes decision whether the received frame should be forwarded or discarded. If the frame needs to be forwarded, then it sends that frame to that LWAP, to which the destination device is connected. Then that LWAP sends this frame to the destination device.

The WLC - LWAP setup is usually used in the company environment to span a single wireless network in large geographical area. This setup allows users to roam around the office premise, campus or building and stay connected to the network.

In this setup, it doesn’t make any difference which LWAP a user uses to send and receive the frames as long as that LWAP is controlled by the same WLC. Since all forwarding decisions are taken by the WLC, an LWAP does not allow direct communication between the two devices, even if they both are connected with it.

wireless lan controller and lightweight access point
Key points

- Access point connects multiple wireless devices together in a single wireless network.
- Access point supports both type of standards; Ethernet and Wi-Fi.
- Access point uses radio signals to provide the connectivity.
- Based on functionality an access point can be categorized in three types; standalone, multifunction and client.
- A standalone access point works in the wireless network exactly as the switch works in the wired network.
- To control the unauthorized access, Access point uses authorization.
- To extend the coverage area, multiple access points are used together under a Wireless LAN Controller.
- An access point which works under the WLC is known as the LWAP (Lightweight Access Point).
- In WLC-LWAPs setup, the WLC controls and manages all LWAPs.
- A LWAP works as the bridge between the WLC and the end device.

Q. What is a Mobility Group?

A. A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC loading information, and can also forward data traffic among them, which enables inter-controller wireless LAN roaming and controller redundancy.

Q. What are the prerequisites for a Mobility Group?

A. Before you add controllers to a mobility group, you must verify that certain requirements are met for all controllers that are to be included in the group. Refer to the Prerequisites section of Configuring Mobility Groups for a list of these requirements.

Q. How do I configure a Mobility Group on the WLC?

A. A Mobility Group is configured manually. The IP and MAC address of the Wireless LAN Controllers (WLCs) that belong to the same Mobility Group are configured on each of the WLCs individually. Mobility Groups can be configured either through the CLI or the GUI.

Q. How do I configure a Mobility Group with WCS?

A. Mobility Groups can also be configured with the Wireless Control System (WCS). This alternative method comes in handy when a large number of WLCs is deployed. Refer to the Configuring Mobility Groups section of Cisco Wireless Control System Configuration Guide, Release 7.0 for more information on how to configure the Mobility Groups with WCS.

Q. Can I configure WLCs in multiple Mobility Groups?

A. No. Wireless LAN Controllers (WLCs) can be configured only in one Mobility Group.

Q. Can the LWAPPs join a WLC that belongs to a Mobility Group that is different from the currently associated Mobility Group?

A. In all Wireless LAN Controller (WLC) versions earlier than 4.2.61.0, when a WLC goes "down," the LAP registered to this WLC can failover only to another WLC of the same Mobility Group, if the LAP is configured for failover. From Cisco WLC version 4.2.61.0 and later, a new feature called Backup Controller Support is introduced for access points to failover to controllers even outside the Mobility Group. Refer to Wireless LAN Controller and Light Weight Access Points Failover Outside the Mobility Group Configuration Example for more information.

Q. How are Mobility Messages exchanged between WLCs?

A. In versions earlier than 5.0 , WLCs sends Mobility Messages with unicast mode, where the copies of Mobility Messages are unicast to all the WLCs in the Mobility Group. But in version 5.0 , Mobility Messages can be sent as Multicast messages wherein only one copy of the Mobility Message is sent to reach all the WLCs in the Mobility Group. Refer to the Messaging among Mobility Groups section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information.

Q. Is there a command to troubleshoot mobility communication between WLCs?

A. Wireless LAN Controllers (WLCs) software release 4.0 and later enables you to test the mobility communication environment with mobility ping tests. These tests can be used in order to validate connectivity between members of a Mobility Group, which includes guest WLCs. Two ping tests are available:

Mobility ping over UDP(mping)—This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.

Mobility ping over EoIP(eping)—This test runs over EoIP. It tests the mobility data traffic over the management interface.

Make sure that the WLCs are configured in the same Mobility Group and ensure that you can ping the WLCs with the mobility pings. Refer to the Running Mobility Ping Tests section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information.

Q. What is a mobility list? How many controllers can be part of the mobility list of a controller?

A. A mobility list is a group of controllers configured on a single controller that specifies members in different mobility groups. Controllers can communicate across mobility groups and clients can roam between access points in different mobility groups if the controllers are included in each other's mobility lists. In the example in this section, controller 1 can communicate with either controller 2 or 3, but controller 2 and controller 3 can communicate only with controller 1 and not with each other. Similarly, clients can roam between controller 1 and controller 2 or between controller 1 and controller 3 but not between controller 2 and controller 3.

Controller software release 5.1 supports up to 72 controllers in the mobility list of a controller and seamless roaming across multiple mobility groups. During seamless roaming, the client maintains its IP address across all mobility groups. However, Cisco Centralized Key Management (CCKM) and Proactive Key Caching (PKC) are supported only for intra-mobility-group roaming. When a client crosses a mobility group boundary during a roam, the client is fully authenticated, but the IP address is maintained, and EtherIP tunneling is initiated for Layer 3 roaming.

Note: Controller software release 5.0 supports up to 48 controllers in a mobility list.
Q. How do I secure or encrypt the Mobility Messages exchanged between the WLCs?

A. In order to secure the Mobility Messages exchanged between the Wireless LAN Controllers (WLCs), enable the Secure mode between the controllers. In order to do this, issue the config mobility secure-mode enable command. In this mode, WLCs use the UDP port 16667 in order to exchange the messages. If there is a firewall, ensure that the UDP port 16667 is opened. In order to ensure this mode is enabled, verify the Mobility Protocol Port from the output of the show mobility summary command. Port 16667 indicates secure-mode (encryption). Port 16666 indicates non secure-mode (no encryption).

CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

CAPWAP is based on LWAPP but adds additional security with Datagram Transport Layer Security (DTLS). CAPWAP establishes tunnels on User Datagram Protocol (UDP) ports. CAPWAP can operate either over IPv4 or IPv6, but uses IPv4 by default.

A key component of CAPWAP is the concept of a split media access control (MAC). The CAPWAP split MAC concept does all of the functions normally performed by individual APs and distributes them between two functional components:

    AP MAC Functions
    WLC MAC Functions

The table shows some of the MAC functions performed by each.

AP MAC Functions
 - Beacons and probe responses
 - Packet acknowledgements and retransmissions
 - Frame queueing and packet prioritization
 - MAC layer data encryption and decryption

WLC MAC Functions
 - Authentication
 - Association and re-association of roaming clients
 - Frame translation to other protocols
 - Termination of 802.11 traffic on a wired interface

DTLS is a protocol which provides security between the AP and the WLC. It allows them to communicate using encryption and prevents eavesdropping or tampering.

DTLS is enabled by default to secure the CAPWAP control channel but is disabled by default for the data channel, as shown in the figure. All CAPWAP management and control traffic exchanged between an AP and WLC is encrypted and secured by default to provide control plane privacy and prevent Man-In-the-Middle (MITM) attacks.

CAPWAP data encryption is optional and is enabled per AP. Data encryption requires a DTLS license to be installed on the WLC prior to being enabled on an AP. When enabled, all WLAN client traffic is encrypted at the AP before being forwarded to the WLC and vice versa.

FlexConnect APs

FlexConnect is a wireless solution for branch office and remote office deployments. It lets you configure and control access points in a branch office from the corporate office through a WAN link, without deploying a controller in each office.

There are two modes of operation for the FlexConnect AP.

 - Connected mode: The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC and can send traffic through the CAPWAP tunnel.The WLC performs all its CAPWAP functions.

 - Standalone mode - The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC. In this mode, a FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.