Wireless Access Points Glossary of Terms

Objective

This article contains the list of terms used in setting up, configuration, and troubleshooting the Cisco Wireless Access Points (WAP).

Applicable Devices

- Wireless Access Points

List of General Terms

- 802.1Q-based VLAN — The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information, and defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure. The 802.1Q standard is intended to address the problem of how to divide large networks into smaller parts so broadcast and multicast traffic does not use more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks.
- 802.1X Supplicant — Supplicant is one of the three roles in the 802.1X IEEE Standard. The 802.1X was developed to provide security in Layer 2 of the OSI Model. It is composed of the following components: Supplicant, Authenticator, and Authentication Server. A Supplicant is the client or software that connects to a network so that it can access resources on that network. It needs to provide credentials or certificates to obtain an IP address and be part of that particular network. A Supplicant cannot have access to the network's resources until it has been authenticated.
- ACL — An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network device. ACLs can be defined in one of two ways: by IPv4 address or by IPv6 address.
- Band Steer — Advanced load balancing, better known as band steering, is a feature that detects devices capable of transmitting at 5 GHz band. The 2.4 GHz band is often congested and experiences interference from different devices such as Bluetooth, and even microwave ovens. This feature allows your access point to steer and direct devices to a more optimal radio frequency, thus, improving network performance.
- Bandwidth Utilization — Bandwidth utilization allows you to place a threshold on the average successful data transfer through a communication path. Some of the techniques used to improve this are bandwidth shaping, management, capping, and allocation.
- Bonjour — Bonjour allows an access point and its services to be discovered by using multicast DNS. It advertises its services to the network and answers queries for the service types that it supports, simplifying network configuration in small business environments. When Bonjour is enabled on a supported WAP device, any Bonjour client can discover and access the web-based utility without prior configuration. Bonjour works in both IPv4 and IPv6 networks.
- Captive Portal — Captive Portal method forces LAN users or hosts on the network to see a special web page before they can access the public network normally. Captive Portal turns a web browser into an authentication device. The web page requires user interaction or authentication before the access is allowed to use the network.

- Channel Isolation — A device with channel management enabled automatically assigns wireless radio channels to the other WAP devices in the cluster. The automatic channel assignment reduces interference with other access points outside of its cluster and maximizes Wi-Fi bandwidth to help maintain the efficiency of communication over the wireless network.
- Client QoS — The Client Quality of Service (QoS) Association is a section that provides additional options for customization of a wireless client's QoS. These options include the bandwidth allowed to send, receive, or guaranteed. Client QoS Association can further be manipulated with the use of Access Control Lists (ACL).
- Event Logging — System events are activities in the system that may require attention and necessary actions to be taken in order to run the system smoothly and prevent failures. These events are recorded as logs. System Logs enable the administrator to keep track of particular events that take place on the device. Event logs are useful for network troubleshooting, debugging packet flow, and monitoring events.
- Fast Roaming — Fast roaming between wireless access points permits a fast, secure, and uninterrupted wireless connectivity to achieve seamless mobile experience for real-time applications such as FaceTime, Skype, and Cisco Jabber.
- HTTPS — Hyper Text Transfer Protocol Secure (HTTPS) is a transfer protocol that is more secure than HTTP. The access point can be managed through both HTTP and HTTPS connections when the HTTP/HTTPS servers are configured. Some web browsers use HTTP while others use HTTPS. An access point must have a valid Secure Socket Layer (SSL) certificate to use HTTPS service.
- IPv4 — IPv4 is a 32-bit addressing system used to identify a device in a network. It is the addressing system used in most computer networks, including the Internet.
- IPv6 — IPv6 is a 128-bit addressing system used to identify a device in a network. It is the successor to IPv4 and the most recent version of the addressing system used in computer networks. IPv6 is currently being rolled out around the world. An IPv6 address is represented in eight fields of hexadecimal numbers, each field containing 16 bits. An IPv6 address is divided into two parts, each part composed of 64 bits. The first part being the Network Address, and the second part the Host Address.
- LLDP — Link Layer Discovery Protocol (LLDP) is a discovery protocol that is defined in the IEEE 802.1AB standard. LLDP allows network devices to advertise information about themselves to other devices on the network. LLDP uses the Logical Link Control (LLC) services to transmit and receive information to and from other LLDP agents. LLC provides a Link Service Access Point (LSAP) for access to LLDP. Each LLDP frame is transmitted as a single MAC service request. Each incoming LLDP frame is received at the MAC Service Access Point (MSAP) by the LLC entity as a MAC service indication.
- Load Balancing — Load balancing is a network terminology which is used to distribute the workload across multiple computers, network links, and various other resources to achieve proper resource utilization, maximize throughput, response time, and mainly avoid the overload.
- MAC ACL — Media Access Control (MAC) based on Access Control List (ACL) is a list of source MAC addresses. If a packet is coming from a wireless access point to a LAN port or vice versa, this device will check if the source MAC address of the packet matches any entry in this list and checks the ACL rules against the content of the frame. It then uses the matched results to permit or deny this packet. However, packets from LAN to LAN port will not be checked.
- Multiple SSIDs — You can configure several Service Set Identifiers (SSIDs) or Virtual Access Points (VAPs) on your access point and assign different configuration settings to each SSID.

All the SSIDs may be active at the same time. Client devices can associate to the access point using any of the SSIDs.

- Operating Mode — The WAP device can act as a single point-to-point mode access point, point-to-multipoint bridge, and as a repeater. In the point-to-point mode, a single WAP device accepts connections from clients and other devices in the network. In a point-to-multipoint bridge mode, a single WAP device behaves as a common link between many access points. WAP device can also act as a repeater, where it can establish a connection between access points which are far apart from each other. Wireless clients can connect to this repeater. A Wireless Distribution System (WDS) role system can be compared similar to the role of the repeater.
- Packet Capture — Packet Capture is a feature of a network device that enables you to capture and store packets that are transmitted and received by the device. The captured packets can be analyzed by a network protocol analyzer to troubleshoot or optimize performance. The captured packet file can be downloaded via HTTP/HTTPS or TFTP server. It can be shared and then further analyzed to understand the packet flow in the network. The Packet Capture page can be used to configure either remote or local packet capture, download a packet capture file, or view the current capture status.
- QoS — Quality of Service (QoS) allows you to prioritize traffic for different applications, users or data flows. It can also be used to guarantee performance to a specified level, thus, affecting the quality of service of the client. QoS is generally affected by the following factors: jitter, latency, and packet loss.
- RADIUS Server — Remote Authentication Dial-In User Service (RADIUS) is an authentication mechanism for devices to connect and use a network service. It is used for centralized authentication, authorization, and accounting purposes. A RADIUS server regulates access to the network by verifying the identity of the users through the login credentials entered. For example, a public Wi-Fi network is installed in a university campus. Only those students who have the password can access these networks. The RADIUS server checks the passwords entered by the users and grants or denies access as appropriate.
- Remote Management — Remote Management is manipulating the settings of a network device from a remote location. This is typically done on devices like computers, switches, routers and many others that have an IP address. It allows network administrators to respond quickly to requests or challenges since they do not have to be on-site physically. Accessing devices in Remote Management is almost like doing it locally, except that the local IP address of the device is used to access the device locally whereas the WAN IP of the device is used when doing it on a remote device.
- Rogue AP Detection — A rogue Access Point (AP) is an access point that has been installed on a network without explicit authorization from a system administrator. Rogue access points pose a security threat because anyone with access to the area can knowingly or unknowingly install a wireless access point that can allow unauthorized parties to access the network. The Rogue AP Detection feature on your access point allows it to see these rogue access points that are within the range and it displays their information in the web-based utility. You can add any authorized access points to the Trusted AP List.
- RSTP — Rapid Spanning Tree Protocol (RSTP) is an enhancement of STP. RSTP provides a faster spanning tree convergence after a topology change. STP can take 30 to 50 seconds to respond to a topology change while RSTP responds within three times the configured hello time. RSTP is backwards compatible with STP.
- Scheduler — The wireless scheduler helps to schedule a time interval for a Virtual Access Point (VAP) or radio to be operational, which helps to save power and increase security. You

can associate up to 16 profiles to different VAPs or radio interfaces, but each interface is allowed only one profile. Each profile can have a certain number of time rules that control the uptime of the associated VAP or WLAN.

- Single Point Setup — Single Point Setup is a simple, multi-device management technology that allows you to deploy and manage a group of access points that support the feature. It offers the convenience of configuring a group of access points from a single point instead of configuring them individually. It also allows you to manage the access points locally or remotely.
- SNMP — Simple Network Management Protocol (SNMP) is a network standard for storing and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance.
- Spanning Tree — Spanning Tree Protocol (STP) is a network protocol used on a LAN. The purpose of STP is to ensure a loop-free topology for a LAN. STP removes loops through an algorithm that guarantees that there is only one active path between two network devices. STP ensures that traffic takes the shortest path possible within the network. STP can also automatically re-enable redundant paths as back up paths if an active path fails.
- SSID — The Service Set Identifier (SSID) is a unique identifier that wireless clients can connect to or share among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters. This is also called Wireless Network Name.
- SSID Broadcast — When a wireless device searches the area for wireless networks that it can connect to, it will detect the wireless networks within its range through their network names or SSIDs. The broadcast of the SSID is enabled by default. However, you may also choose to disable it.
- TSPEC — Traffic Specification (TSPEC) is a traffic specification that is sent from a QoS-capable wireless client to a WAP device requesting a certain amount of network access for the Traffic Stream (TS) it represents.
- VLAN — A Virtual Local Area Network (VLAN) is a switched network that is logically segmented by function, area, or application, without regard to the physical locations of the users. VLANs are a group of hosts or ports that can be located anywhere in a network but communicate as if they are on the same physical segment. VLANs help to simplify network management by letting you move a device to a new VLAN without changing any physical connections.
- WDS — Wireless Distribution System (WDS) is a feature which enables the wireless interconnection of access points in a network. It enables the user to expand the network with multiple access points wirelessly. WDS also preserves the MAC addresses of client frames across links between access points. This capability is critical because it provides a seamless experience for roaming clients and allows management of multiple wireless networks.
- WMM — Wi-Fi Multimedia (WMM) is a feature that assigns different process priorities to different types of traffic. WMM is also a QoS feature that enhances the performance of the wireless network through setting the priority of the wireless data packet based on four categories: voice, video, best effort, and background. By default, WMM is enabled. If an application does not require WMM, it is given lower priority than video and voice.
- Wireless Isolation — Prevents communication and file transfers between computers that are connected to different SSIDs. Traffic on one SSID will not be forwarded to any other SSIDs.
- WPA/WPA2 — Wi-Fi Protected Access (WPA and WPA2) are security protocols used for wireless networks to protect privacy by encrypting the transmitted data over the wireless network. WPA and WPA2 are both forward compatible with IEEE 802.11e and 802.11i. WPA and WPA2 have improved authentication and encryption features compared to the Wired

Equivalent Privacy (WEP) security protocol.

List of Terms in Mesh Networks

- **Access Point (AP)**: A device in a network that is used to allow users to connect to the Network wirelessly. Specific labels may be added to this depending on its function: Primary, Remote, Root, Subordinate, etc.
- **Wireless Mesh Network:** A type of topology where the wireless access points connect to each other to relay information. These networks work dynamically to adjust the needs and maintain connectivity for all users.
- **Primary AP:** The Primary AP provides management and control of the wireless network and topology. It is the bridge to the rest of the external network, (usually the Internet) using an Internet Service Provider (ISP). The Primary AP directly links to the premise router which in turn routes traffic to the WAN ISP interface. The Primary AP is the orchestrator of all the nodes providing wireless services within the mesh network. It manages information from the nodes on the network, each client connection quality and neighbor information in order to make the best decision on the best route for optimized wireless services out to the mobile client.
- **Primary Primary:** The current AP tasked with management of the WLAN.
- **Preferred Primary:** A setting in which a specific Primary-capable AP is listed as preferred. If the Primary AP fails, the Preferred Primary AP will take over. Once the Preferred AP is back up, it does not automatically switch back over. You do not have designate a Preferred Primary.
- **Primary Capable AP:** An AP that has a physical wired connection back to the network. This AP needs to be connected to Ethernet and can become the Primary AP if the Primary AP fails.
- **Mesh Extender:** A remote subordinate AP in the network that is not connected to the wired network.
- **Subordinate AP:** A general term that can be applied to any mesh AP that is not configured as a Primary.
- **Parent AP:** A parent AP is an AP that provides the best route back to the Primary AP.
- **Child AP:** A child AP is a mesh extender that selects the parent AP as its best route back to the Primary AP.
- **Upstream AP:** An upstream AP is a general term referring to the direction data flows through APs when going from the client to the server.
- **Downstream AP:** A downstream AP carries data from the Internet down to the client.
- **Co-located APs:** Mesh Extenders that are within broadcast range of the backhaul channel.
- **Nodes:** In this article, APs are referred to as nodes. In general, nodes describe any device that makes a connection or interaction within a network, or has the ability to send, receive, and store information, communicate with the internet, and has an IP address. In a mesh network, optimized radio parameters across all nodes assures maximum wireless coverage while reducing radio interference among nodes to provide superior data speeds and throughput.
- **Backhaul:** In a wireless mesh network, information in the Local Area Network (LAN) needs to get to a wired access point in order to reach the Internet. Backhaul is the process of getting that information back to the wired access point.