Appendix - Glossary of Terms

This appendix contains the following sections:

Cisco Business Wireless - Glossary Of Terms

0-9

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.

A

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.

Allowlist

Allowlist is a list of Client/Mesh Extender MAC addresses that are allowed to join the network.

Anti Clog Threshold

Anti-clogging token is a mechanism to protect entities from Denial of Service (DoS) attack. Anti-clogging token is bound to MAC address of the station (STA). The length of the token cannot be more than 256 bytes.

The threshold is configured in terms of resource percentage. On hitting the threshold for the resource, the primary AP starts to reject authentication commit requests that come with anti-clogging token.

B

Band Steer

Advanced load balancing, better known as band steering, is a feature that detects devices capable of transmitting at 5GHz band. The 2.4GHz 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

Bandwidth is the measurement of the ability of a device to send and receive information.

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.

Basic Service Set (BSS) Coloring

BSS Coloring is a method to differentiate between BSS (APs and their clients) on the same RF channel. Wi-Fi 6 enables each AP radio to assign a value (from 1 to 63), known as the BSS color, to be included in the PHY header of all HE transmissions from devices in its BSS.

With devices of each BSS transmitting a locally-unique color, a device can quickly and easily distinguish transmissions coming from its BSS from those of a neighboring BSS.

Blocklist

A **Blocklist** is a list of Client/Mesh Extender MAC addresses that are denied to join the network.

C

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.

CBD Probe

Cisco Business Dashboard Probe is installed at each site in the network and associated with the Dashboard. The probe performs network discovery and communicates directly with each managed device.

Central web authentication (CWA)

CWA offers the possibility to have a central device that acts as a web portal. Once the user logs into the portal, it is possible to re-authenticate the client so that a new Layer 2 MAC filtering occurs using the Change of Authorization (CoA). This way, the ISE remembers that it was a webauth user and pushes the necessary authorization attributes to the Primary AP for accessing the network.

Channel Isolation

A device with channel management enabled, automatically assigns wireless radio channels to the other A2 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. Automatic channel assignments are supported in non-mesh deployments.

Channel Width

Channel width controls how broad the signal is for transferring data. Think of it like a highway. The wider the road, the more traffic (data) can pass through. On the other hand, the more cars (routers) you have on the road, the more congested the traffic becomes. By increasing the channel width, we can increase the speed and throughput of a wireless broadcast. By default, the 2.4GHz frequency uses a 20 MHz channel width. A 20MHz channel width is wide enough to span one channel.

A 40 MHz channel width bonds two 20 MHz channels together, forming a 40 MHz channel width; therefore, it allows for greater speed and faster transfer rates.

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).

Connection Speed

Connection speed is the speed that data is transferred between your client and the internet.

D

DCA

Dynamic Channel Assignment (DCA) can dynamically determine best bandwidth for each AP connected to the Primary AP. DCA algorithm manages, evaluates the channel assignments on AP on per radio basis. It automatically adjusts the channel to maintain performance of individual radios.

E

EAPol

Extensible Authentication Protocol (EAP) over LAN (EAPoL) is a network port authentication protocol used in IEEE 802.1X (Port Based Network Access Control) developed to give a generic network sign-on to access network resources.

EAPoL, is a simple encapsulation that can run over any LAN. The following are the three main components defined in EAP and EAPoL to accomplish the authentication conversation:

- Supplicant—Port Authentication Entity (PAE) seeking access to network resources
- Authenticator—PAE that controls network access
- Authentication Server—RADIUS/AAA server

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.

F

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.

H

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.

I

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.

ISE

Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches. The purpose is to simplify identity management across diverse devices and applications.

L

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.

Local Probe

Local probe is the same as **Cisco Business Dashboard Probe**. This may be installed on the same host as Cisco Business Dashboard in order to manage devices on the network that is local to the Dashboard.

M

Max Data Rate

Maximum Data rate is the max speed at which data is transferred between two devices, measured in mega bits per second (Mbps or mbps)

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.

MU-MIMO

MU-MIMO (multi-user, multiple input, multiple output) is a wireless technology that was introduced in the 802.11ac Wave 2 (Wi-Fi 5) standard. It allows a single Access Point (AP) to transmit data to multiple devices simultaneously. MU-MIMO dramatically improves performance and efficiency when APs are transmitting to client devices that support Wi-Fi 5 or Wi-Fi 6.

N

Network Plug n Play

Network Plug and Play is a service that works in conjunction with Network Plug and Play enabled devices to allow firmware and configuration to be managed centrally, and to allow zero-touch deployment of new network devices. Devices may be deployed directly using the Network Plug and Play protocol, or indirectly if discovered by a probe that is associated with the Dashboard.

O

OFDMA

OFDMA (orthogonal frequency-division multiple access), a technology in Wi-Fi 6, improves wireless network performance by establishing independently modulating subcarriers within frequencies. This approach allows simultaneous transmissions to and from multiple clients.

Operating Mode

The A2 Access points, CBW140, CBW240, CBW145 are Primary Capable and they can serve as Primary AP. CBW141, CBW142, CBW143 are Mesh Extenders. The Primary Capable AP can serve as Mesh Extenders wirelessly, in addition to connecting the clients. The A2 Access Points acting as Mesh Extenders helps in extending the network coverage.

P

PMF

This is specific to 802.11w protocol. The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

PMKID

Pairwise Primary Key Identifier (PMKID) is the unique key identifier used by the Access Point to keep track of the PMK being used for the client.

PoE-PD

Power Over Ethernet Powered Device. An Ethernet port that can receive power to provide network connectivity.

PoE-PSE

Power Over Ethernet Power Sourcing Equipment. An Etherent port that can supply power and provide network connectivity.

Q

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.

R

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.

Radio Domains

Based on the regulatory domain of the AP, the carrier set values will be set for both 2.4GHz and 5GHz. For example, the radio domains for US regulatory domain is –A for 2.4GHz and –B for 5GHz.

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

S

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.

Signal Quality

Signal quality is a value ranging from 0 to 100, which considers, the noise generated by interference sources, along with signal strength.

Signal Strength

The signal strength is the wireless signal power level received by the wireless client. Strong signal strength results in more reliable connections and higher speeds. Signal strength is represented in -dBm format (0 to -100). This is the power ratio in decibels (dB) of

the measured power referenced to one milliwatt. The closer the value is to 0, the stronger the signal. For example, -41dBm is better signal strength than -61dBm.

Spatial Streams

Wi-Fi Spatial streaming or multiplexing is a transmission technique used in multiple-input-multiple-output (MIMO) wireless communication to transmit/receive independent and separately coded data signals (which are called as streams), from each of the multiple transmit antennas.

In other words, wireless signals that are transmitted or received by the various antennae are multiplexed by using different spaces within the same spectral channel. These spaces is known as spatial streams.

Spectrum Intelligence

Spectrum intelligence scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands, and provides basic functions to detect interferences of three types, namely microwave, continuous wave (like video bridge and baby monitor), Wi-Fi and frequency hopping (Bluetooth and frequency-hopping spread spectrum (FHSS) cordless phone).

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.

T

Target Waketime

A new power-saving mode called Target Wake Time (TWT) allows the client to stay asleep and to wake up only at pre-scheduled (target) times to exchange data with the Access Point. This offers significant energy savings for battery-operated devices, up to three to four times the savings achieved by 802.11n and 802.11ac.

V

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

W

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.

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. This uses AES type of encryption. The encryption keys that are used for each client on the network are unique and specific to that client. 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.

WPA2 Enterprise

This mode of security will use EAP-FAST for authenticating the Wireless clients and AES for encryption. Cisco Secure ACS server will be used as the external RADIUS server for authenticating the wireless clients.

In Enterprise mode of operation there is a mutual authentication between a client and an authentication server (Internal or External). In addition,it removes the administrative burden and security issues surrounding static encryption keys.

WPA3

Wi-Fi Protected Access 3 (WPA3) is the third iteration of a security standard or protocol developed by the Wi-Fi Alliance. WPA3 was designed to replace the WPA2 security standard, adding several security enhancements and tackling security vulnerabilities of the WPA2 to better secure personal and enterprise wireless networks. WPA3 uses a more powerful and robust encryption by AES with the GCMP (Galois/Counter Mode Protocol) and uses more reliable handshake mechanism called Simultaneous Authentication of Equals (SAE).

WPA3