Wireless Access Points Frequently Asked Questions

Objective

This article contains the frequently asked questions in setting up, configuring, and troubleshooting the Cisco Wireless Access Points (WAPs) and their answers.

Applicable Devices

- WAP100 Series
- WAP300 Series
- WAP500 Series

Frequently Asked Questions

Table of Contents

1. What is VLAN?
2. What is 802.1Q-based VLAN?
3. What is SSID?
4. What is Multiple SSIDs?
5. What is SSID Broadcast?
6. What is a Scheduler?
7. What is Bandwidth Utilization?
8. What is Spanning Tree?
9. What is RSTP?
10. What is Load Balancing?
11. What is WPA/WPA2?
12. What is ACL?
13. What is MAC-based ACL?
14. What is HTTPS?
15. What is Rogue AP Detection?
16. What is RADIUS Server?
17. What is 802.1X Supplicant?
18. What is QoS?
19. What is WMM?
20. What is TSPEC?
21. What is Client QoS?
22. What is Single Point Setup?
23. What is Remote Management?
24. What is Wireless Isolation?
25. What is Band Steer?
26. What is WDS?
27. What is Fast Roaming?
28. What is LLDP?

29. What is Operating Mode?
30. What is Bonjour?
31. What is Captive Portal?
32. What is Channel Isolation?
33. What is Event Logging?
34. What is IPv4?
35. What is IPv6?
36. What is Packet Capture?
37. What is SNMP?
38. What are the best practices for optimal wireless performance?

1. **What is VLAN?**

   A Virtual Local Area Network (VLAN) is a switched network that is logically sorted by function, area, or application, regardless of the physical locations of the users.

2. **What is 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.

3. **What is SSID?**

   The Service Set Identifier (SSID) is a unique identifier or a network name that wireless clients can connect to or share among all devices in a wireless network.

4. **What are Multiple SSIDs?**

   It is possible to set up several SSIDs or Virtual Access Points (VAPs) on your access point and assign different configuration settings to each of them. All the SSIDs may be active at the same time and client devices can associate to the access point using any of them.

5. **What is SSID Broadcast?**

   SSID Broadcast is the manner where in a wireless network is advertising or making itself visible to any wireless device that searches the area for wireless networks that it can connect to. The broadcast of the SSID is enabled by default but can be disabled to prevent any wireless device from seeing your wireless network.

6. **What is a Scheduler?**

   The wireless scheduler feature helps to schedule a time interval for a VAP or radio to be operational, which helps to save power and increase security.

7. **What is Bandwidth Utilization?**

   Bandwidth utilization allows you to place a threshold on the average successful data transfer through a communication path.

8. **What is Spanning Tree?**

   Spanning Tree Protocol (STP) is a network protocol used to ensure a loop-free topology for

a LAN by removing 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 and can also automatically re-enable redundant paths as back up paths if an active path fails.

9. **What is 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 and is backwards compatible with STP.

10. **What is Load Balancing?**

    Load balancing 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.

11. **What is 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 have improved authentication and encryption features compared to the Wired Equivalent Privacy (WEP) security protocol.

12. **What is ACL?**

    An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security by either blocking or allowing users to access specific resources.

13. **What is MAC-based ACL?**

    A MAC-based ACL is a type of ACL that is based on the source Media Access Control (MAC). 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.

14. **What is HTTPS?**

    Hyper Text Transfer Protocol Secure (HTTPS) is a more secure protocol by which data is transferred between your browser and the website that you are connected to.

15. **What is 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. The Rogue AP Detection feature on your access point allows it to see these rogue APs that are within the range and it displays their information in the web-based utility.

16. **What is 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.

17. **What is 802.1X Supplicant?**

The 802.1X IEEE standard was developed to provide security in Layer 2 of the Open Systems Interconnection (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 and cannot have access to the network's resources until it has been authenticated.

18. **What is 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.

19. **What is WMM?**

Wi-Fi Multimedia (WMM) is a QoS feature that assigns different process priorities to different types of traffic. It 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. If an application does not require WMM, it is given lower priority than video and voice.

20. **What is TSPEC?**

Traffic Specification (TSPEC) is a traffic specification that is sent from a QoS-capable wireless client to a WAP requesting a certain amount of network access for the Traffic Stream (TS) it represents.

21. **What is 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).

22. **What is Single Point Setup?**

Single Point Setup (SPS) is a simple, multi-device management technology that allows you to deploy and manage a group of the exact same access points. 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.

23. **What is Remote Management?**

Remote Management is manipulating the settings of a network device from a remote location using the Wide Area Network (WAN) IP of the device instead of the local IP, allowing network administrators to respond quickly to requests or challenges. This is typically done on devices like computers, switches, routers and many others that have an IP address.

24. **What is Wireless Isolation?**

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.

25. **What is Band Steer?**

Advanced load balancing, better known as band steering, is a feature that detects devices capable of transmitting at 5 GHz band. This feature allows your access point to steer and direct devices to a more optimal radio frequency, thus, improving network performance.

26. **What is WDS?**

Wireless Distribution System (WDS) is a feature which enables the wireless interconnection of access points in a network and 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.

27. **What is 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.

28. **What is 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.

29. **What is Operating Mode?**

The Operating Mode is the ability of the WAP to act on different modes depending on how you want to use it. It can act as a single point-to-point mode access point, point-to-multipoint bridge, or as a repeater.

30. **What is Bonjour?**

Bonjour allows an access point and its services to be discovered by using multicast Domain Name System (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.

31. **What is Captive Portal?**

Captive Portal method forces LAN users or hosts on the network to see a special web page and would require authentication before users can access the public network normally.

32. **What is 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.

33. **What is Event Logging?**

Event Logging is a feature that records activities or events in the system. It allows the administrator to keep track of particular events and is very useful for troubleshooting, system monitoring, and so on.

34. **What is 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.

35. **What is 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.

36. **What is 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 such as Wireshark for troubleshooting or for optimization of network performance.

37. **What is 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.

38. **What are the best practices for optimal wireless performance?**