Glossar zu Wireless Access Points

Ziel

Dieser Artikel enthält eine Liste der Begriffe, die bei der Einrichtung, Konfiguration und Fehlerbehebung der Cisco Wireless Access Points (WAP) verwendet werden.

Unterstützte Geräte

- Wireless Access Points

Liste der allgemeinen Geschäftsbedingungen

- 802.1Q-basiertes VLAN - Die IEEE 802.1Q-Spezifikation legt eine Standardmethode für das Tagging von Ethernet-Frames mit Informationen zur VLAN-Mitgliedschaft fest und definiert den Betrieb von VLAN-Bridges, die die Definition, den Betrieb und die Verwaltung von VLAN-Topologien innerhalb einer überbrückten LAN-Infrastruktur ermöglichen. Der 802.1Q-Standard ist auf die Aufteilung großer Netzwerke in kleinere Teile ausgelegt, sodass Broadcast- und Multicast-Datenverkehr nicht mehr Bandbreite als nötig beansprucht. Der Standard trägt auch zu einer höheren Sicherheit zwischen Segmenten interner Netzwerke bei.
- 802.1X Supplicant (802.1X-Komponente) - Supplicant (Komponente) ist eine der drei Rollen im 802.1X IEEE-Standard. Der 802.1X-Standard wurde entwickelt, um die Sicherheit in Layer 2 des OSI-Modells zu gewährleisten. Sie besteht aus den folgenden Komponenten: Supplicant, Authenticator und Authentication Server. Ein Supplicant ist der Client oder die Software, der bzw. die eine Verbindung zu einem Netzwerk herstellt, um auf Ressourcen in diesem Netzwerk zugreifen zu können. Sie muss Anmeldeinformationen oder Zertifikate bereitstellen, um eine IP-Adresse zu erhalten und Teil dieses speziellen Netzwerks zu sein. Ein Supplicant kann erst nach Authentifizierung auf die Netzwerkressourcen zugreifen.
- ACL - Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Liste von Netzwerkdatenverkehrsfiltern und zugehörigen Aktionen zur Verbesserung der Sicherheit. Sie blockiert oder ermöglicht Benutzern den Zugriff auf bestimmte Ressourcen. Eine ACL enthält die Hosts, denen der Zugriff auf das Netzwerkgerät gestattet oder verweigert wird. ACLs können auf zwei Arten definiert werden: IPv4-Adresse oder IPv6-Adresse.
- Bandsteuerung - Erweiterter Lastenausgleich, besser bekannt als Bandsteuerung, ist eine Funktion, die Geräte erkennt, die im 5-GHz-Band übertragen werden können. Das 2,4-GHz-Band ist häufig überlastet und wird von verschiedenen Geräten wie Bluetooth und sogar Mikrowellenherden gestört. Diese Funktion ermöglicht Ihrem Access Point die Steuerung und Weiterleitung von Geräten auf eine optimale Funkfrequenz, wodurch die Netzwerkleistung verbessert wird.
- Bandbreitennutzung - Mit Bandbreitennutzung können Sie einen Grenzwert für die durchschnittliche erfolgreiche Datenübertragung über einen Kommunikationspfad festlegen. Zu den Techniken, die zur Verbesserung dieser Situation eingesetzt werden, gehören Bandbreitengestaltung, -verwaltung, -begrenzung und -zuweisung.
- Bonjour - Bonjour ermöglicht die Erkennung eines Access Points und seiner Services mithilfe von Multicast DNS. Er informiert das Netzwerk über seine Services und beantwortet Fragen zu den unterstützten Servicetypen. Dies vereinfacht die Netzwerkkonfiguration in kleinen und mittleren Unternehmen. Wenn Bonjour auf einem unterstützten WAP-Gerät aktiviert ist, kann jeder Bonjour-Client das webbasierte Dienstprogramm ohne vorherige Konfiguration erkennen und darauf zugreifen. Bonjour arbeitet sowohl in IPv4- als auch in IPv6-Netzwerken.

- Captive Portal - Die Captive Portal-Methode zwingt LAN-Benutzer oder -Hosts im Netzwerk, eine spezielle Webseite anzuzeigen, bevor sie normal auf das öffentliche Netzwerk zugreifen können. Captive Portal verwandelt einen Webbrowser in ein Authentifizierungsgerät. Die Webseite erfordert eine Benutzerinteraktion oder -authentifizierung, bevor der Zugriff auf das Netzwerk zugelassen wird.
- Kanalisolierung - Ein Gerät mit aktivierter Kanalverwaltung weist den anderen WAP-Geräten im Cluster automatisch Wireless-Funkkanäle zu. Die automatische Kanalzuweisung reduziert Interferenzen mit anderen Access Points außerhalb des Clusters und maximiert die Wi-Fi-Bandbreite, um die Effizienz der Kommunikation über das Wireless-Netzwerk aufrechtzuerhalten.
- Client QoS - Die Client Quality of Service (QoS) Association ist ein Abschnitt, der zusätzliche Optionen für die Anpassung der QoS eines Wireless-Clients bietet. Diese Optionen beinhalten die Bandbreite, die gesendet, empfangen oder garantiert werden darf. Die Client-QoS-Zuordnung kann mithilfe von Zugriffskontrolllisten (Access Control Lists, ACL) weiter bearbeitet werden.
- Ereignisprotokollierung - Systemereignisse sind Aktivitäten im System, die Aufmerksamkeit erfordern und erforderliche Maßnahmen erfordern, um das System reibungslos auszuführen und Ausfälle zu verhindern. Diese Ereignisse werden als Protokolle aufgezeichnet. Mithilfe von Systemprotokollen kann der Administrator bestimmte Ereignisse auf dem Gerät verfolgen. Ereignisprotokolle sind nützlich für die Fehlerbehebung im Netzwerk, das Debuggen des Paketflusses und die Überwachung von Ereignissen.
- Schnelles Roaming - Schnelles Roaming zwischen Wireless Access Points ermöglicht schnelle, sichere und unterbrechungsfreie Wireless-Verbindungen, um eine nahtlose mobile Umgebung für Echtzeitanwendungen wie FaceTime, Skype und Cisco Jabber zu ermöglichen.
- HTTPS - Hyper Text Transfer Protocol Secure (HTTPS) ist ein Übertragungsprotokoll, das sicherer ist als HTTP. Der Access Point kann sowohl über HTTP- als auch über HTTPS-Verbindungen verwaltet werden, wenn die HTTP-/HTTPS-Server konfiguriert sind. Einige Webbrowser verwenden HTTP, während andere HTTPS verwenden. Ein Access Point muss über ein gültiges SSL-Zertifikat (Secure Socket Layer) verfügen, um den HTTPS-Service nutzen zu können.
- IPv4 - IPv4 ist ein 32-Bit-Adressierungssystem, das zur Identifizierung eines Geräts in einem Netzwerk verwendet wird. Es ist das Adressierungssystem, das in den meisten Computernetzwerken, einschließlich des Internets, verwendet wird.
- IPv6 - IPv6 ist ein 128-Bit-Adressierungssystem, das zur Identifizierung eines Geräts in einem Netzwerk verwendet wird. Es ist die Nachfolgerin von IPv4 und die neueste Version des Adressierungssystems, das in Computernetzwerken verwendet wird. IPv6 wird derzeit weltweit eingeführt. Eine IPv6-Adresse wird in acht Feldern mit hexadezimalen Zahlen dargestellt, wobei jedes Feld 16 Bit enthält. Eine IPv6-Adresse ist in zwei Teile unterteilt, die jeweils 64 Bit enthalten. Der erste Teil ist die Netzwerkadresse und der zweite Teil die Host-Adresse.
- LLDP - Link Layer Discovery Protocol (LLDP) ist ein Erkennungsprotokoll, das im IEEE 802.1AB-Standard definiert ist. Mithilfe von LLDP können Netzwerkgeräte anderen Geräten im Netzwerk Informationen über sich selbst übermitteln. LLDP verwendet die Logical Link Control (LLC)-Dienste, um Informationen an andere LLDP-Agenten und von diesen zu senden und zu empfangen. LLC stellt einen Link Service Access Point (LSAP) für den Zugriff auf LLDP bereit. Jeder LLDP-Frame wird als eine einzige MAC-Serviceanfrage übertragen. Jeder eingehende LLDP-Frame wird von der LLC-Einheit als MAC-Dienstanzeige am MAC Service Access Point (MSAP) empfangen.

- Lastenausgleich - Lastenausgleich ist eine Netzwerkterminologie, mit der der Workload auf mehrere Computer, Netzwerkverbindungen und verschiedene andere Ressourcen verteilt wird, um eine angemessene Ressourcennutzung zu erzielen, den Durchsatz zu maximieren, die Reaktionszeit zu verkürzen und hauptsächlich die Überlastung zu vermeiden.
- MAC ACL - Die auf der Zugriffskontrollliste (ACL) basierende Media Access Control (MAC) ist eine Liste der Quell-MAC-Adressen. Wenn ein Paket von einem Wireless Access Point zu einem LAN-Port oder umgekehrt kommt, prüft dieses Gerät, ob die Quell-MAC-Adresse des Pakets mit einem Eintrag in dieser Liste übereinstimmt, und überprüft die ACL-Regeln auf den Inhalt des Frames. Anschließend werden die übereinstimmenden Ergebnisse verwendet, um dieses Paket zuzulassen oder zu verweigern. Pakete vom LAN zum LAN-Port werden jedoch nicht überprüft.
- Mehrere SSIDs: Sie können mehrere Service Set Identifiers (SSIDs) oder Virtual Access Points (VAPs) für Ihren Access Point konfigurieren und jeder SSID unterschiedliche Konfigurationseinstellungen zuweisen. Alle SSIDs können gleichzeitig aktiv sein. Client-Geräte können über die SSIDs mit dem Access Point verbunden werden.
- Betriebsmodus - Das WAP-Gerät kann als Access Point im Point-to-Point-Modus, Point-to-Multipoint Bridge und Repeater fungieren. Im Point-to-Point-Modus akzeptiert ein einzelnes WAP-Gerät Verbindungen von Clients und anderen Geräten im Netzwerk. In einem Punkt-zu-Mehrpunkt-Bridge-Modus fungiert ein einzelnes WAP-Gerät als gemeinsame Verbindung zwischen vielen Access Points. WAP-Geräte können auch als Repeater fungieren, bei dem eine Verbindung zwischen Access Points hergestellt werden kann, die sich weit voneinander entfernt befinden. Wireless-Clients können eine Verbindung zu diesem Repeater herstellen. Ein WDS-Rollensystem (Wireless Distribution System) kann mit der Rolle des Repeaters verglichen werden.
- Paketerfassung - Die Paketerfassung ist ein Feature eines Netzwerkgeräts, mit dem Sie Pakete erfassen und speichern können, die vom Gerät übertragen und empfangen werden. Die erfassten Pakete können von einem Netzwerkprotokoll-Analyzer analysiert werden, um Leistungsfehler zu beheben oder zu optimieren. Die erfasste Paketdatei kann über HTTP/HTTPS oder TFTP-Server heruntergeladen werden. Sie kann gemeinsam genutzt und anschließend weiter analysiert werden, um den Paketfluss im Netzwerk zu ermitteln. Auf der Seite Paketerfassung können Sie entweder die Paketerfassung per Remote- oder lokal konfigurieren, eine Paketerfassungsdatei herunterladen oder den aktuellen Erfassungsstatus anzeigen.
- QoS - Quality of Service (QoS) ermöglicht die Priorisierung des Datenverkehrs für verschiedene Anwendungen, Benutzer oder Datenflüsse. Sie kann auch verwendet werden, um die Leistung auf ein bestimmtes Niveau zu garantieren, was sich auf die Quality of Service des Clients auswirkt. QoS wird im Allgemeinen durch folgende Faktoren beeinflusst: Jitter, Latenz und Paketverlust.
- RADIUS Server - RADIUS (Remote Authentication Dial-In User Service) ist ein Authentifizierungsmechanismus für Geräte, die eine Verbindung herstellen und einen Netzwerkdienst verwenden. Sie wird für zentralisierte Authentifizierungs-, Autorisierungs- und Abrechnungszwecke verwendet. Ein RADIUS-Server regelt den Zugriff auf das Netzwerk, indem er die Identität der Benutzer mithilfe der eingegebenen Anmeldeinformationen überprüft. So wird beispielsweise ein öffentliches Wi-Fi-Netzwerk auf einem Universitätsgelände installiert. Nur Schüler mit Passwort können auf diese Netzwerke zugreifen. Der RADIUS-Server überprüft die von den Benutzern eingegebenen Kennwörter und gewährt bzw. verweigert den Zugriff.
- Remote-Management - Die Remote-Verwaltung bearbeitet die Einstellungen eines

Netzwerkgeräts von einem Remote-Standort aus. Dies geschieht in der Regel auf Geräten wie Computern, Switches, Routern und vielen anderen Geräten, die über eine IP-Adresse verfügen. So können Netzwerkadministratoren schnell auf Anfragen oder Herausforderungen reagieren, da sie nicht physisch vor Ort sein müssen. Der Zugriff auf Geräte in der Remote-Verwaltung ist fast wie eine lokale Ausführung, mit der Ausnahme, dass die lokale IP-Adresse des Geräts für den lokalen Zugriff auf das Gerät verwendet wird, während die WAN-IP-Adresse des Geräts für den Zugriff auf ein Remote-Gerät verwendet wird.

- Erkennung nicht autorisierter APs - Ein nicht autorisierter Access Point (AP) ist ein Access Point, der in einem Netzwerk ohne ausdrückliche Autorisierung eines Systemadministrators installiert wurde. Nicht autorisierte Access Points stellen eine Sicherheitsbedrohung dar, da jeder, der Zugriff auf den Bereich hat, einen Wireless Access Point wissentlich oder unwissentlich installieren kann, der unbefugten Zugriff auf das Netzwerk ermöglicht. Mit der Funktion zur Erkennung nicht autorisierter APs auf Ihrem Access Point können diese nicht autorisierten Access Points innerhalb des Bereichs angezeigt werden, und ihre Informationen werden im webbasierten Dienstprogramm angezeigt. Sie können der Liste der vertrauenswürdigen Access Points alle autorisierten Access Points hinzufügen.
- RSTP - Rapid Spanning Tree Protocol (RSTP) ist eine Erweiterung von STP. RSTP bietet eine schnellere Spanning Tree-Konvergenz nach einer Topologieänderung. STP kann 30 bis 50 Sekunden dauern, bis auf eine Topologieänderung reagiert wird, während das RSTP innerhalb der dreifachen Hello-Zeit antwortet. RSTP ist abwärtskompatibel mit STP.
- Scheduler - Der Wireless Scheduler dient der Planung eines Zeitintervalls für den Betrieb eines Virtual Access Point (VAP) oder einer Funkeinheit, wodurch Energie gespart und die Sicherheit erhöht wird. Sie können bis zu 16 Profile verschiedenen VAPs oder Funkschnittstellen zuordnen, aber jede Schnittstelle ist nur für ein Profil zulässig. Jedes Profil kann eine bestimmte Anzahl von Zeitregeln enthalten, die die Betriebszeit des verknüpften VAP oder WLAN steuern.
- Single-Point-Einrichtung - Single-Point-Einrichtung ist eine einfache Verwaltungstechnologie mit mehreren Geräten, mit der Sie eine Gruppe von Access Points bereitstellen und verwalten können, die diese Funktion unterstützen. Es bietet die Möglichkeit, eine Gruppe von Access Points von einem einzigen Punkt aus zu konfigurieren, anstatt sie einzeln zu konfigurieren. Außerdem können Sie die Access Points lokal oder remote verwalten.
- SNMP - Simple Network Management Protocol (SNMP) ist ein Netzwerkstandard zum Speichern und Freigeben von Informationen über Netzwerkgeräte. SNMP vereinfacht Netzwerkverwaltung, Fehlerbehebung und Wartung.
- Spanning Tree - Spanning Tree Protocol (STP) ist ein Netzwerkprotokoll, das in einem LAN verwendet wird. STP soll eine schleifenfreie Topologie für ein LAN sicherstellen. STP entfernt Schleifen mithilfe eines Algorithmus, der sicherstellt, dass nur ein aktiver Pfad zwischen zwei Netzwerkgeräten vorhanden ist. STP stellt sicher, dass der Datenverkehr den kürzestmöglichen Pfad innerhalb des Netzwerks annimmt. STP kann auch redundante Pfade automatisch als Backup-Pfade wieder aktivieren, wenn ein aktiver Pfad ausfällt.
- SSID - Der Service Set Identifier (SSID) ist eine eindeutige Kennung, mit der Wireless-Clients eine Verbindung zu allen Geräten in einem Wireless-Netzwerk herstellen oder diese gemeinsam nutzen können. Es wird zwischen Groß- und Kleinschreibung unterschieden und darf 32 alphanumerische Zeichen nicht überschreiten. Dies wird auch als Wireless-Netzwerkname bezeichnet.
- SSID-Broadcast - Wenn ein Wireless-Gerät den Bereich nach Wireless-Netzwerken durchsucht, mit denen eine Verbindung hergestellt werden kann, erkennt es die Wireless-Netzwerke in seiner Reichweite über deren Netzwerknamen oder SSIDs. Die Übertragung der

SSID ist standardmäßig aktiviert. Sie können es jedoch auch deaktivieren.

- TSPEC - Traffic Specification (TSPEC) ist eine Datenverkehrsspezifikation, die von einem QoS-fähigen Wireless-Client an ein WAP-Gerät gesendet wird, das eine bestimmte Menge an Netzwerkzugriff für den von ihm repräsentierten Traffic Stream (TS) anfordert.
- VLAN - Ein Virtual Local Area Network (VLAN) ist ein Switch-Netzwerk, das logisch nach Funktion, Bereich oder Anwendung segmentiert ist, unabhängig von den physischen Standorten der Benutzer. VLANs sind eine Gruppe von Hosts oder Ports, die sich an einem beliebigen Ort in einem Netzwerk befinden, aber so kommunizieren können, als ob sie sich im selben physischen Segment befinden. VLANs vereinfachen die Netzwerkverwaltung, indem Sie das Gerät in ein neues VLAN verschieben können, ohne physische Verbindungen zu ändern.
- WDS - Wireless Distribution System (WDS) ist eine Funktion, die die Wireless-Verbindung von Access Points in einem Netzwerk ermöglicht. Es ermöglicht dem Benutzer, das Netzwerk mit mehreren Access Points drahtlos zu erweitern. WDS behält darüber hinaus die MAC-Adressen von Client-Frames über Verbindungen zwischen Access Points hinweg bei. Diese Funktion ist von entscheidender Bedeutung, da sie eine nahtlose Umgebung für Roaming-Clients bietet und die Verwaltung mehrerer Wireless-Netzwerke ermöglicht.
- WMM - Wi-Fi Multimedia (WMM) ist eine Funktion, die verschiedenen Arten von Datenverkehr unterschiedliche Prozessprioritäten zuweist. WMM ist außerdem eine QoS-Funktion, die die Leistung des Wireless-Netzwerks verbessert, indem die Priorität des Wireless-Datenpakets auf vier Kategorien festgelegt wird: Sprache, Video, Best Effort und Hintergrund. Standardmäßig ist WMM aktiviert. Wenn eine Anwendung kein WMM erfordert, erhält sie eine niedrigere Priorität als Video und Sprache.
- Wireless-Isolierung - Verhindert die Kommunikation und Dateiübertragung zwischen Computern, die mit verschiedenen SSIDs verbunden sind. Der Datenverkehr einer SSID wird nicht an andere SSIDs weitergeleitet.
- WPA/WPA2 - Wi-Fi Protected Access (WPA und WPA2) sind Sicherheitsprotokolle, die für Wireless-Netzwerke verwendet werden, um die Privatsphäre zu schützen, indem die übertragenen Daten über das Wireless-Netzwerk verschlüsselt werden. WPA und WPA2 sind beide aufwärtskompatibel mit IEEE 802.11e und 802.11i. WPA und WPA2 verfügen im Vergleich zum Sicherheitsprotokoll Wired Equivalent Privacy (WEP) über verbesserte Authentifizierungs- und Verschlüsselungsfunktionen.

Liste der Begriffe in Mesh-Netzwerken

- **Access Point (AP)**: Ein Gerät in einem Netzwerk, mit dem Benutzer eine drahtlose Verbindung zum Netzwerk herstellen können. Bestimmte Etiketten können je nach Funktion hinzugefügt werden: Primär, Remote, Root, Untergeordnet usw.
- **Wireless Mesh-Netzwerk:** Eine Topologie, bei der die Wireless Access Points miteinander verbunden sind, um Informationen weiterzuleiten. Diese Netzwerke arbeiten dynamisch, um die Anforderungen anzupassen und die Konnektivität für alle Benutzer aufrechtzuerhalten.
- **Primärer Access Point:** Der primäre Access Point ermöglicht die Verwaltung und Steuerung des Wireless-Netzwerks und der Wireless-Topologie. Es handelt sich dabei um die Bridge zum übrigen externen Netzwerk (normalerweise zum Internet), das einen Internetdienstanbieter (Internet Service Provider, ISP) verwendet. Der primäre Access Point stellt eine direkte Verbindung zum Router vor Ort her, der wiederum Datenverkehr an die WAN-ISP-Schnittstelle weiterleitet. Der primäre Access Point ist der Orchestrator aller Knoten, die Wireless-Services innerhalb des Mesh-Netzwerks bereitstellen. Es verwaltet Informationen von den Knoten im Netzwerk, von jeder Client-Verbindungsqualität und von

Nachbarinformationen, um die beste Entscheidung für die optimale Route für optimierte Wireless-Services zum mobilen Client zu treffen.

- **Primär:** Der aktuelle WAP dient der Verwaltung des WLAN.
- **Primär bevorzugt:** Eine Einstellung, bei der ein bestimmter primärfähiger Access Point als bevorzugt aufgeführt wird. Wenn der primäre Access Point ausfällt, übernimmt der Preferred Primary AP (Bevorzugter primärer Access Point). Wenn der bevorzugte Access Point gesichert ist, wird er nicht automatisch wieder umgeschaltet. Sie haben keine bevorzugte primäre Priorität festgelegt.
- **Primäre AP-Kapazität:** Ein WAP mit einer physischen kabelgebundenen Verbindung zum Netzwerk. Dieser AP muss mit Ethernet verbunden sein und kann der primäre Access Point werden, wenn der primäre Access Point ausfällt.
- **Mesh-Extender:** Ein untergeordneter Remote-Access-Point im Netzwerk, der nicht mit dem kabelgebundenen Netzwerk verbunden ist.
- **Zugangspunkt:** Ein allgemeiner Begriff, der auf jeden Mesh-Access Point angewendet werden kann, der nicht als primärer Access Point konfiguriert ist.
- **Übergeordneter Access Point:** Ein übergeordneter Access Point ist ein Access Point, der die beste Route zurück zum primären Access Point bereitstellt.
- **Untergeordneter Access Point:** Ein untergeordneter Access Point ist ein Mesh-Extender, der den übergeordneten Access Point als beste Route zurück zum primären Access Point auswählt.
- **Upstream-AP:** Ein Upstream-Zugangspunkt ist ein allgemeiner Begriff, der sich auf die Richtung bezieht, die Daten durch APs fließen, wenn sie vom Client zum Server gelangen.
- **Downstream-AP:** Ein Downstream-Access-Point überträgt Daten vom Internet bis zum Client.
- **Zugeordnete Zugangspunkte:** Mesh-Extender, die sich im Broadcast-Bereich des Backhaul-Kanals befinden.
- **Knoten:** In diesem Artikel werden APs als Knoten bezeichnet. Im Allgemeinen beschreiben Knoten jedes Gerät, das eine Verbindung oder Interaktion innerhalb eines Netzwerks herstellt oder Informationen sendet, empfängt und speichert, mit dem Internet kommuniziert und über eine IP-Adresse verfügt. In einem Mesh-Netzwerk sorgen optimierte Funkparameter für alle Knoten für eine maximale Wireless-Abdeckung und reduzieren gleichzeitig die Funkinterferenzen zwischen Knoten, um höhere Datengeschwindigkeiten und einen höheren Durchsatz zu ermöglichen.
- **Backhaul:** In einem Wireless Mesh-Netzwerk müssen die Informationen im Local Area Network (LAN) zu einem kabelgebundenen Access Point gelangen, um das Internet zu erreichen. Backhaul ist der Prozess, bei dem diese Informationen zum kabelgebundenen Access Point zurückgegeben werden.