Draadloze access points Lijst van termen

Doel

Dit artikel bevat de lijst met termen die worden gebruikt bij het instellen, configureren en oplossen van de Cisco draadloze access points (WAP).

Toepasselijke apparaten

- Draadloze access points

Lijst van algemene termen

- 802.1Q-gebaseerd VLAN — De specificatie van IEEE 802.1Q stelt een standaardmethode vast om Ethernet frames met de lidmaatschapsinformatie van VLAN te taggen, en definieert de werking van VLAN-bruggen die de definitie, de werking en het beheer van VLAN-topologieën binnen een SNELLE LAN-infrastructuur mogelijk maken. De 802.1Q standaard is bedoeld om het probleem aan te pakken van hoe u grote netwerken in kleinere delen kunt verdelen zodat uitzending en multicast verkeer niet meer bandbreedte dan nodig gebruiken. De norm helpt ook een hoger beveiligingsniveau te bieden tussen segmenten van interne netwerken.
- Suppliciet 802.1X — Suppliciet is één van de drie rollen in de standaard 802.1X IEEE. De 802.1X werd ontwikkeld om veiligheid in Layer 2 van het OSI-model te bieden. Het bestaat uit de volgende onderdelen: Leverancier, Authenticator en Verificatieserver. Een Leverancier is de client of software die op een netwerk aangesloten is zodat hij toegang heeft tot middelen op dat netwerk. Het moet geloofsbrieven of certificaten verstrekken om een IP-adres te verkrijgen en deel uitmaken van dat specifieke netwerk. Een aanvrager kan geen toegang hebben tot de middelen van het netwerk totdat het is geauthentificeerd.
- ACL (toegangscontrolelijst) is een lijst van netwerkverkeersfilters en bijbehorende acties om beveiliging te verbeteren. Het blokkeert of maakt gebruikers toegang tot specifieke bronnen. Een ACL bevat de hosts die toegang tot het netwerkapparaat is toegestaan of geweigerd. ACL's kunnen op twee manieren worden gedefinieerd: door IPv4-adres of door IPv6-adres.
- Band Steer — Advanced load balances, beter bekend als bandbesturing, is een functie die apparaten detecteert die kunnen uitzenden op een 5 GHz-band. De 2,4 GHz-band wordt vaak overbelast en ervaart interferentie met verschillende apparaten zoals Bluetooth en zelfs microgolfovens. Deze functie stelt uw toegangspunt in staat om apparaten te sturen en te sturen naar een meer optimale radiofrequentie, waardoor de netwerkprestaties worden verbeterd.
- Bandbreedtegebruik — Bandbreedteschatting stelt u in staat een drempel te plaatsen op de gemiddelde succesvolle gegevensoverdracht via een communicatiepad. Een aantal van de technieken die gebruikt worden om dit te verbeteren zijn het vormgeven, beheren, aftoveren en toewijzen van bandbreedte.
- Bonjour — Bonjour maakt het mogelijk een toegangspunt en de diensten ervan te ontdekken met behulp van multicast DNS. Het adverteert zijn diensten aan het netwerk en beantwoordt vragen voor de diensttypes die het ondersteunt, vereenvoudigt netwerkconfiguratie in kleine bedrijfsomgevingen. Wanneer Bonjour op een ondersteund WAP apparaat is geactiveerd, kan elke Bonjour client het web-based voorziening ontdekken en benaderen zonder voorafgaande configuratie. Bonjour werkt in zowel IPv4- als IPv6-netwerken.
- Captive Portal-methode dwingt LAN-gebruikers of -hosts op het netwerk om een speciale

webpagina te zien voordat zij normaliter toegang kunnen krijgen tot het openbare netwerk. Captive Portal verandert een webbrowser in een verificatieapparaat. De webpagina vereist gebruikersinteractie of authenticatie voordat de toegang het netwerk mag gebruiken.

- Kanaalisolatie — Een toestel met kanaalbeheer dat automatisch draadloze radiokanalen toewijst aan de andere WAP-apparaten in het cluster. De automatische kanaaltoewijzing beperkt interferentie met andere toegangspunten buiten zijn cluster en maximaliseert Wi-Fi-bandbreedte om de efficiëntie van communicatie via het draadloze netwerk te behouden.
- QoS-client — De Client Quality of Service (QoS) Association is een sectie die aanvullende opties biedt voor het aanpassen van QoS van een draadloze klant. Deze opties omvatten de bandbreedte die is toegestaan om te verzenden, ontvangen of gegarandeerd. De client-QoS-vereniging kan verder worden gemanipuleerd met behulp van toegangscontrolelijsten (ACL's).
- Vastlegging van gebeurtenissen — systeemgebeurtenissen zijn activiteiten in het systeem die aandacht en noodzakelijke maatregelen vereisen om het systeem vlot te laten functioneren en storingen te voorkomen. Deze gebeurtenissen worden als logs geregistreerd. Met systeemmeldingen kan de beheerder bepaalde gebeurtenissen die op het apparaat plaatsvinden, bijhouden. Event logs zijn handig voor problemen oplossen bij het netwerk, het foutherstellen van pakketstromen en het bewaken van gebeurtenissen.
- Snel roaming - Snel roaming tussen draadloze access points maakt een snelle, veilige en ononderbroken draadloze connectiviteit mogelijk om een naadloze mobiele ervaring te realiseren voor real-time toepassingen zoals FaceTime, Skype en Cisco Jabber.
- HTTPS - Hyper-Text Transfer Protocol (HTTPS) is een overdrachtprotocol dat veiliger is dan HTTP. Het toegangspunt kan via zowel HTTP- als HTTPS-verbindingen worden beheerd wanneer de HTTP/HTTPS-servers zijn geconfigureerd. Sommige webbrowsers gebruiken HTTP terwijl anderen HTTPS gebruiken. Een access point moet beschikken over een geldig Secure Socket Layer (SSL)-certificaat om HTTPS-service te gebruiken.
- IPv4 — IPv4 is een 32-bits adresseringssysteem dat wordt gebruikt om een apparaat in een netwerk te identificeren. Het is het adresseringssysteem dat in de meeste computernetwerken, waaronder het internet, wordt gebruikt.
- IPv6 — IPv6 is een 128-bits adresseringssysteem dat wordt gebruikt om een apparaat in een netwerk te identificeren. Het is de opvolger van IPv4 en de meest recente versie van het adresseringssysteem dat in computernetwerken wordt gebruikt. IPv6 wordt momenteel wereldwijd uitgerold. Een IPv6-adres wordt weergegeven in acht velden van hexadecimale getallen, elk veld met 16 bits. Een IPv6-adres is verdeeld in twee delen, elk deel bestaat uit 64 bits. Het eerste deel is het Netwerkadres en het tweede deel het host-adres.
- LLDP — Link Layer Discovery Protocol (LLDP) is een zoekprotocol dat is gedefinieerd in de IEEE 802.1AB-standaard. LLDP laat netwerkapparaten toe om informatie over zichzelf aan andere apparaten op het netwerk te adverteren. LLDP gebruikt de diensten Logical Link Control (LLC) om informatie naar en van andere LLDP-agents te verzenden en ontvangen. LLC biedt een Link Service Access Point (LSAP) voor toegang tot LLDP. Elk LLDP-frame wordt verzonden als één MAC-serviceaanvraag. Elk inkomend LLDP-frame wordt bij het MAC Service Access Point (MSAP) door de LLC-entiteit ontvangen als een MAC-servicecontract.
- Taakverdeling — taakverdeling is een netwerkterminologie die wordt gebruikt om de werklast over meerdere computers, netwerkkoppelingen en verschillende andere bronnen te verdelen om een goed gebruik van de middelen te bereiken, de doorvoersnelheid en de responstijd te maximaliseren en vooral de overbelasting te voorkomen.
- MAC ACL (Media Access Control) op basis van toegangscontrolelijst (ACL) is een lijst met bron-MAC-adressen. Als een pakket van een draadloos access point naar een LAN poort komt of omgekeerd, zal dit apparaat controleren of het bron-MAC-adres van het pakket

overeenkomt met een willekeurige ingang in deze lijst en controleert u de ACL-regels tegen de inhoud van het frame. Het gebruikt vervolgens de gecompenseerde resultaten om dit pakje toe te staan of te ontkennen. Er wordt echter niet gecontroleerd of pakketten van LAN naar LAN poort zijn.

- Meervoudige SSID's — U kunt meerdere Service Set Identifier's (SSID's) of Virtual Access Point (VAP's) op uw access point configureren en verschillende configuratie-instellingen aan elke SSID toewijzen. Alle SSID's kunnen tegelijkertijd actief zijn. Clientapparaten kunnen zich aan het toegangspunt koppelen door gebruik te maken van een van de SSID's.
- Bedieningsmodus — Het WAP-apparaat kan fungeren als één point-to-point mode access point, point-to-multipoint brug en als een repeater. In de point-to-point modus accepteert één WAP-apparaat verbindingen van klanten en andere apparaten in het netwerk. In een point-to-multipoint bridge modus, gedraagt één WAP-apparaat zich als een gemeenschappelijke link tussen veel access points. WAP-apparatuur kan ook fungeren als een repeater, waar een verbinding kan worden gelegd tussen toegangspunten die ver van elkaar verwijderd zijn. Draadloze klanten kunnen aan dit repeater verbinden. Een rolsysteem voor draadloos distributiesysteem (WDS) kan worden vergeleken met de rol van de herhaling.
- Packet Capture — Packet Capture is een functie van een netwerkapparaat waarmee u pakketten kunt opnemen en opslaan die door het apparaat worden verzonden en ontvangen. De opgenomen pakketten kunnen door een netwerkprotocolanalyzer worden geanalyseerd om problemen op te lossen of de prestaties te optimaliseren. Het opgenomen pakketbestand kan worden gedownload via HTTP/HTTPS of TFTP-server. Het kan worden gedeeld en dan verder worden geanalyseerd om de pakketstroom in het netwerk te begrijpen. De pagina Packet Capture kan worden gebruikt om afstandsbediening of lokale pakketvastlegging te configureren, een pakketvastlegging bestand te downloaden of de huidige opnamestatus te bekijken.
- QoS — Quality of Service (QoS) stelt u in staat prioriteit te geven aan verkeer voor verschillende toepassingen, gebruikers of gegevensstromen. Het kan ook worden gebruikt om de prestaties op een bepaald niveau te garanderen, waardoor de kwaliteit van de dienstverlening van de cliënt wordt aangetast. De QoS wordt in het algemeen beïnvloed door de volgende factoren: jitter, latentie en pakketverlies.
- RADIUS Server - Remote Authentication Dial-In User Service (RADIUS) is een verificatiemechanisme voor apparaten om een netwerkservice te verbinden en te gebruiken. Het wordt gebruikt voor gecentraliseerde authenticatie, autorisatie en boekhoudkundige doeleinden. Een RADIUS-server reguleert de toegang tot het netwerk door de identiteit van de gebruikers te controleren met behulp van de ingevoerde inlogaanmeldingsgegevens. Een openbaar Wi-Fi-netwerk is bijvoorbeeld geïnstalleerd op een universiteitscampus. Alleen studenten die het wachtwoord hebben, hebben toegang tot deze netwerken. De RADIUS-server controleert de wachtwoorden die de gebruikers hebben ingevoerd en verleent of ontkent de toegang indien nodig.
- Afstandsbeheer — Afstandsbeheer manipuleert de instellingen van een netwerkapparaat vanaf een afgelegen locatie. Dit gebeurt doorgaans op apparaten zoals computers, switches, routers en vele andere die een IP-adres hebben. Hiermee kunnen netwerkbeheerders snel reageren op verzoeken of uitdagingen omdat zij niet fysiek ter plaatse hoeven te zijn. Apparaten in afstandsbeheer gebruiken is bijna zoals het lokaal doen, behalve dat het lokale IP-adres van het apparaat wordt gebruikt om het apparaat lokaal te benaderen, terwijl het WAN IP van het apparaat wordt gebruikt wanneer het op een extern apparaat wordt uitgevoerd.
- AP Detectie van schurken - Een frauduleus access point (AP) is een access point dat op een

netwerk is geïnstalleerd zonder uitdrukkelijke toestemming van een systeembeheerder. Moeilijke toegangspunten vormen een veiligheidsbedreiging omdat iedereen met toegang tot het gebied bewust of onbewust een draadloos access point kan installeren dat onbevoegde partijen toegang tot het netwerk kan verlenen. Met de detectie van AP van de Rogue op uw toegangspunt staat het toe om deze punten van schurkentoegang te zien die binnen het bereik zijn en het toont hun informatie in het web-based voorziening. U kunt alle geautoriseerde access points aan de lijst met vertrouwde functies toevoegen.

- RSTP - Rapid Spanning Tree Protocol (RSTP) is een versterking van STP. RSTP biedt een snellere overspant van boomconvergentie na een topologie verandering. STP kan 30 tot 50 seconden duren om op een topologie te reageren terwijl RSTP binnen drie keer de geconfigureerde hallo-tijd reageert. RSTP is achterwaarts compatibel met STP.
- Scheduler - De draadloze planner helpt u een tijdinterval te plannen voor een Virtual Access Point (VAP) of radio om operationeel te zijn, waardoor u minder stroom kunt besparen en de beveiliging kan toenemen. U kunt maximaal 16 profielen koppelen aan verschillende VAP's of radio interfaces, maar elke interface is slechts één profiel toegestaan. Elk profiel kan een bepaald aantal tijdregels hebben die de uptime van de gekoppelde VAP of WLAN controleren.
- Single Point Setup — Single Point Setup is een eenvoudige beheertechnologie voor meerdere apparaten waarmee u een groep access points kunt implementeren en beheren die deze functie ondersteunen. Het is handig om een groep toegangspunten uit één punt te configureren in plaats van ze afzonderlijk te configureren. Hiermee kunt u de toegangspunten ook lokaal of extern beheren.
- SNMP — Simple Network Management Protocol (SNMP) is een netwerkstandaard voor het opslaan en delen van informatie over netwerkapparaten. SNMP vergemakkelijkt netwerkbeheer, probleemoplossing en onderhoud.
- Spanning Tree Protocol (STP) is een netwerkprotocol dat op een LAN wordt gebruikt. Het doel van STP is om een lus-vrije topologie voor een LAN te verzekeren. STP verwijdert lusjes door een algoritme dat waarborgt dat er slechts één actief pad tussen twee netwerkapparaten is. STP garandeert dat het verkeer de kortste route die mogelijk is binnen het netwerk. STP kan ook automatisch redundante paden als back-uppaden opnieuw inschakelen indien een actief pad mislukt.
- SSID — The Service Set Identifier (SSID) is een uniek identificatiemiddel dat draadloze klanten met alle apparaten in een draadloos netwerk kunnen verbinden of delen. Het is hoofdlettergevoelig en mag niet meer dan 32 alfanumerieke tekens bevatten. Dit wordt ook wel draadloze netwerknaam genoemd.
- SSID Broadcast — Wanneer een draadloos apparaat het gebied doorzoekt naar draadloze netwerken waarmee het kan verbinden, zal het de draadloze netwerken binnen zijn bereik detecteren via hun netwerknamen of SSID’s. De uitzending van SSID wordt standaard ingeschakeld. U kunt er echter ook voor kiezen om dit uit te schakelen.
- TSPEC — Traffic Specification (TSPEC) is een verkeersspecificatie die van een draadloos QoS-enabled-client naar een WAP-apparaat wordt verzonden waarin een bepaalde hoeveelheid netwerktoegang voor de Traffic Stream (TS) wordt gevraagd die door deze client wordt vertegenwoordigd.
- VLAN — Een Virtual Local Area Network (VLAN) is een geschakeld netwerk dat logisch gesegmenteerd wordt door functie, gebied of toepassing, zonder rekening te houden met de fysieke locaties van de gebruikers. VLAN’s zijn een groep hosts of poorten die overal in een netwerk te vinden is, maar die kunnen communiceren alsof ze op hetzelfde fysieke segment vallen. VLAN’s helpen het netwerkbeheer te vereenvoudigen door u een apparaat naar een nieuw VLAN te laten verplaatsen zonder de fysieke verbindingen te wijzigen.

- WDS — Wireless Distribution System (WDS) is een functie die draadloze interconnectie van toegangspunten in een netwerk mogelijk maakt. Het stelt de gebruiker in staat het netwerk draadloos uit te breiden met meerdere toegangspunten. WDS behoudt ook de MAC-adressen van client-frames tussen koppelingen tussen toegangspunten. Dit vermogen is van cruciaal belang omdat het een naadloze ervaring biedt voor roamende klanten en het beheer van meerdere draadloze netwerken mogelijk maakt.
- WMM — Wi-Fi Multimedia (WMM) is een functie die verschillende procesprioriteiten toegewijst aan verschillende soorten verkeer. WMM is ook een QoS optie die de prestaties van het draadloze netwerk verbetert door de prioriteit van het draadloze gegevenspakket in te stellen op basis van vier categorieën: spraak, video, moeite en achtergrond. Standaard is WMM ingeschakeld. Als een toepassing geen WMM vereist, krijgt deze lagere prioriteit dan video en stem.
- Draadloze isolatie — belet communicatie en bestandsoverdracht tussen computers die zijn aangesloten op verschillende SSID's. Het verkeer op één SSID zal niet naar andere SSID's worden doorgestuurd.
- WAP/WAP2 — Wi-Fi Beschermde Toegang (WAP en WAP2) zijn veiligheidsprotocollen die gebruikt worden voor draadloze netwerken om privacy te beschermen door de verzonden gegevens via het draadloze netwerk te versleutelen. WAP en WAP2 zijn beide voorwaarts compatibel met IEEE 802.11e en 802.11i. WAP en WAP2 hebben verbeterde verificatie- en encryptie-functies in vergelijking met het Wired Equivalent Privacy (WLAN) security protocol.

Lijst van termen in mesh-netwerken

- Access point (AP): Een apparaat in een netwerk dat wordt gebruikt om gebruikers draadloos verbinding te maken met het netwerk. Afhankelijk van de functie kunnen specifieke etiketten worden toegevoegd: Master, Remote, Root, Subordinaat, enz.
- Draadloos mesh-netwerk: Een type topologie waar de draadloze toegangspunten met elkaar verbinden om informatie door te geven. Deze netwerken werken dynamisch om de behoeften aan te passen en connectiviteit voor alle gebruikers te behouden.
- Hoofd AP: Het Master AP verstrekt beheer en controle van het draadloze netwerk en de topologie. Het is de brug naar de rest van het externe netwerk, (gewoonlijk het Internet) die een Internet Service Provider (ISP) gebruikt. De Master AP linkt rechtstreeks naar de vorige router die op zijn beurt het verkeer naar de WAN ISP-interface routeert. De Master AP is de orchestrator van alle knooppunten die draadloze diensten binnen het netwerk van de mazen leveren. Het beheert informatie van de knooppunten op het netwerk, elke kwaliteit van de clientverbinding en buurinformatie om de beste beslissing te nemen over de beste route voor een geoptimaliseerde draadloze dienstverlening aan de mobiele klant.
- Primaire Master: De huidige AP is belast met het beheer van de WLAN.
- Voorkeurster: Een instelling waarin een specifieke Master-capabel AP als geprefereerd wordt vermeld. Als de Master AP faalt, zal de Preferent Master AP overnemen. Zodra het Preferent AP weer omhoog is, schakelt het niet automatisch terug. U hebt geen voorkeursmeester aangewezen.
- Master Capable AP: Een AP die een fysieke verbinding terug naar het netwerk heeft. Deze AP moet worden aangesloten op Ethernet en kan de Master AP worden als de Master AP faalt.
- mesh-extender: Een externe ondergeschikte AP in het netwerk dat niet op het bekabelde netwerk is aangesloten.
- Subordinaat AP: Een algemene term die kan worden toegepast op elke vermaasde AP die niet als Master is ingesteld.

- **Ouderlijke AP:** Een ouder AP is AP dat de beste route terug naar de Meester AP verstrekt.
- **Kind:** Een kind-AP is een vermaasde extender die de ouder-AP als zijn beste route terug naar de Meester AP selecteert.
- **Upstream AP:** Een upstream AP is een algemene term die verwijst naar de richting gegevens stromen door AP's wanneer je van de client naar de server gaat.
- **Downstream AP:** Een stroomafwaarts AP draagt gegevens van het internet naar de cliënt.
- **Gelijktijdige toegang:** mesh-extenders die binnen het bereik van de backhaul-kanalen vallen.
- **Knooppunten:** In dit artikel worden AP's knooppunten genoemd. In het algemeen beschrijven knooppunten elk apparaat dat een verbinding of interactie binnen een netwerk maakt, of de mogelijkheid heeft om informatie te verzenden, ontvangen en op te slaan, met het internet te communiceren en een IP adres heeft. In een netwerk met maaswijdtes zorgen geoptimaliseerde radiofarameters over alle knooppunten voor een maximale draadloze dekking terwijl radioverbinding tussen knooppunten wordt beperkt om superieure gegevenssnelheden en -doorvoersnelheid te bieden.
- **Backhaul:** In een draadloos netwerk moet informatie in het Local Area Network (LAN) aan een bekabeld access point worden geleverd om het internet te bereiken. Backhaul is het proces om die informatie terug te krijgen naar het bekabelde toegangspunt.