Glossario dei termini sui punti di accesso wireless

Obiettivo

In questo articolo vengono elencati i termini utilizzati per l'impostazione, la configurazione e la risoluzione dei problemi dei Cisco Wireless Access Point (WAP).

Dispositivi interessati

- Access point wireless

Elenco di condizioni generali

- VLAN basata su 802.1Q: la specifica IEEE 802.1Q stabilisce un metodo standard per contrassegnare i frame Ethernet con le informazioni sull'appartenenza della VLAN e definisce il funzionamento dei bridge VLAN che consentono la definizione, il funzionamento e l'amministrazione delle topologie VLAN all'interno di un'infrastruttura VLAN con bridging. Lo standard 802.1Q ha lo scopo di risolvere il problema della suddivisione di reti di grandi dimensioni in parti più piccole, in modo che il traffico broadcast e multicast non utilizzi una larghezza di banda maggiore del necessario. Lo standard contribuisce anche a fornire un livello più elevato di sicurezza tra i segmenti delle reti interne.
- Supplicant 802.1X: uno dei tre ruoli dello standard 802.1X IEEE. Lo standard 802.1X è stato sviluppato per garantire la sicurezza nel layer 2 del modello OSI. È composto dai seguenti componenti: Supplicant, Authenticator e Authentication Server. Un supplicant è il client o il software che si connette a una rete in modo che possa accedere alle risorse in tale rete. Deve fornire credenziali o certificati per ottenere un indirizzo IP e far parte di tale rete. Un richiedente non può accedere alle risorse della rete finché non è stato autenticato.
- ACL: un elenco di controllo di accesso (ACL) è un elenco di filtri del traffico di rete e di azioni correlate utilizzate per migliorare la sicurezza. Blocca o consente agli utenti di accedere a risorse specifiche. Un ACL contiene gli host a cui è consentito o negato l'accesso al dispositivo di rete. Gli ACL possono essere definiti in due modi: in base all'indirizzo IPv4 o all'indirizzo IPv6.
- Banda sterzante - Il bilanciamento del carico avanzato, meglio noto come sterzo della banda, è una funzione che rileva dispositivi in grado di trasmettere a banda 5 GHz. La banda a 2,4 GHz è spesso congestionata e subisce interferenze da diversi dispositivi come Bluetooth e persino forni a microonde. Questa funzione consente al punto di accesso di dirigere e dirigere i dispositivi verso una frequenza radio ottimale, migliorando così le prestazioni della rete.
- Utilizzo della larghezza di banda: l'utilizzo della larghezza di banda consente di definire una soglia per il trasferimento medio dei dati completato attraverso un percorso di comunicazione. Alcune delle tecniche utilizzate per migliorare questo processo sono il data shaping, la gestione, la limitazione e l'allocazione della larghezza di banda.
- Bonjour - Bonjour consente di individuare un punto di accesso e i relativi servizi utilizzando il DNS multicast. I servizi vengono pubblicizzati in rete e vengono fornite risposte alle query relative ai tipi di servizi supportati, semplificando la configurazione della rete in ambienti di piccole imprese. Quando Bonjour è abilitato su un dispositivo WAP supportato, qualsiasi client Bonjour può rilevare l'utility basata sul Web e accedervi senza una configurazione precedente. Bonjour lavora sia su reti IPv4 che IPv6.

- Captive Portal: il metodo Captive Portal forza gli utenti LAN o gli host della rete a visualizzare una pagina Web speciale prima di poter accedere normalmente alla rete pubblica. Captive Portal trasforma un browser Web in un dispositivo di autenticazione. La pagina Web richiede l'interazione o l'autenticazione dell'utente prima che l'accesso possa utilizzare la rete.
- Isolamento canali: un dispositivo con la gestione dei canali abilitata assegna automaticamente i canali radio wireless agli altri dispositivi WAP nel cluster. L'assegnazione automatica dei canali riduce le interferenze con altri punti di accesso esterni al cluster e massimizza la larghezza di banda Wi-Fi per mantenere l'efficienza della comunicazione sulla rete wireless.
- QoS client: l'associazione QoS (Quality of Service) client è una sezione che fornisce opzioni aggiuntive per la personalizzazione di QoS di un client wireless. Queste opzioni includono la larghezza di banda consentita per l'invio, la ricezione o la garanzia. L'associazione QoS client può essere ulteriormente manipolata utilizzando gli Access Control Lists (ACL).
- Registrazione eventi: gli eventi di sistema sono attività del sistema che possono richiedere attenzione e azioni necessarie per eseguire il sistema senza problemi e prevenire errori. Questi eventi vengono registrati come registri. I registri di sistema consentono all'amministratore di tenere traccia di eventi particolari che si verificano nel dispositivo. I registri eventi sono utili per la risoluzione dei problemi di rete, il debug del flusso di pacchetti e il monitoraggio degli eventi.
- Roaming veloce: il roaming veloce tra punti di accesso wireless consente una connettività wireless veloce, sicura e senza interruzioni per un'esperienza mobile ottimale per applicazioni in tempo reale quali FaceTime, Skype e Cisco Jabber.
- HTTPS — Hyper Text Transfer Protocol Secure (HTTPS) è un protocollo di trasferimento più sicuro di HTTP. Il punto di accesso può essere gestito tramite connessioni HTTP e HTTPS quando i server HTTP/HTTPS sono configurati. Alcuni browser Web utilizzano HTTP mentre altri utilizzano HTTPS. Per utilizzare il servizio HTTPS, un punto di accesso deve disporre di un certificato SSL (Secure Socket Layer) valido.
- IPv4: IPv4 è un sistema di indirizzamento a 32 bit utilizzato per identificare un dispositivo in una rete. È il sistema di indirizzamento utilizzato nella maggior parte delle reti di computer, incluso Internet.
- IPv6 — IPv6 è un sistema di indirizzamento a 128 bit utilizzato per identificare un dispositivo in una rete. È il successore dell'IPv4 e della versione più recente del sistema di indirizzamento utilizzato nelle reti di computer. IPv6 è attualmente in fase di implementazione in tutto il mondo. Un indirizzo IPv6 è rappresentato in otto campi di numeri esadecimali, ognuno contenente 16 bit. Un indirizzo IPv6 è diviso in due parti, ognuna composta da 64 bit. La prima parte è l'indirizzo di rete, la seconda l'indirizzo host.
- LLDP — Link Layer Discovery Protocol (LLDP) è un protocollo di rilevamento definito nello standard IEEE 802.1AB. LLDP consente ai dispositivi di rete di annunciare informazioni su se stessi ad altri dispositivi della rete. LLDP utilizza i servizi LLC (Logical Link Control) per trasmettere e ricevere informazioni da e verso altri agenti LLDP. LLC fornisce un Link Service Access Point (LSAP) per l'accesso a LLDP. Ogni frame LLDP viene trasmesso come una singola richiesta di servizio MAC. Ogni frame LLDP in ingresso viene ricevuto al punto di accesso al servizio MAC (MSAP) dall'entità LLC come indicazione del servizio MAC.
- Bilanciamento del carico: il bilanciamento del carico è una terminologia di rete utilizzata per distribuire il carico di lavoro tra più computer, collegamenti di rete e varie altre risorse al fine di ottenere un corretto utilizzo delle risorse, massimizzare il throughput, il tempo di risposta ed evitare principalmente il sovraccarico.
- ACL MAC — Media Access Control (MAC) basato su Access Control List (ACL) è un elenco di indirizzi MAC di origine. Se un pacchetto proviene da un punto di accesso wireless a una

porta LAN o viceversa, il dispositivo controllerà se l'indirizzo MAC di origine del pacchetto corrisponde a una voce dell'elenco e controllerà le regole ACL in base al contenuto del frame. Utilizza quindi i risultati corrispondenti per autorizzare o negare il pacchetto. Tuttavia, i pacchetti da LAN a porta LAN non verranno controllati.

- Più SSID: è possibile configurare più SSID (Service Set Identifier) o VAP (Virtual Access Point) sul punto di accesso e assegnare diverse impostazioni di configurazione a ciascun SSID. Tutti gli SSID possono essere attivi contemporaneamente. I dispositivi client possono essere associati al punto di accesso utilizzando uno qualsiasi degli SSID.
- Modalità operativa: il dispositivo WAP può fungere da singolo punto di accesso in modalità point-to-point, bridge point-to-multipoint e ripetitore. Nella modalità point-to-point, un singolo dispositivo WAP accetta connessioni dai client e da altri dispositivi della rete. In una modalità bridge point-to-multipoint, un singolo dispositivo WAP si comporta come un collegamento comune tra più punti di accesso. Il dispositivo WAP può anche fungere da ripetitore, dove può stabilire una connessione tra punti di accesso che sono lontani l'uno dall'altro. I client wireless possono connettersi a questo ripetitore. Un sistema di ruolo WDS (Wireless Distribution System) può essere paragonato al ruolo del ripetitore.
- Acquisizione pacchetti: l'acquisizione pacchetti è una funzionalità di un dispositivo di rete che consente di acquisire e archiviare i pacchetti trasmessi e ricevuti dal dispositivo. I pacchetti acquisiti possono essere analizzati da un analizzatore di protocolli di rete per risolvere i problemi o ottimizzare le prestazioni. Il file del pacchetto acquisito può essere scaricato tramite HTTP/HTTPS o server TFTP. Può essere condiviso e quindi analizzato ulteriormente per comprendere il flusso di pacchetti nella rete. La pagina Packet Capture può essere utilizzata per configurare l'acquisizione dei pacchetti locale o remota, scaricare un file di acquisizione dei pacchetti o visualizzare lo stato di acquisizione corrente.
- QoS: Quality of Service (QoS) consente di assegnare priorità al traffico per diverse applicazioni, utenti o flussi di dati. e può essere utilizzato anche per garantire prestazioni fino a un determinato livello, con conseguente impatto sulla qualità del servizio del cliente. QoS è generalmente influenzato dai seguenti fattori: jitter, latenza e perdita di pacchetti.
- Server RADIUS - RADIUS (Remote Authentication Dial-In User Service) è un meccanismo di autenticazione che consente ai dispositivi di connettersi e utilizzare un servizio di rete. Viene utilizzato per l'autenticazione, l'autorizzazione e la contabilità centralizzate. Un server RADIUS regola l'accesso alla rete verificando l'identità degli utenti tramite le credenziali di accesso immesse. Ad esempio, una rete Wi-Fi pubblica è installata in un campus universitario. Solo gli studenti che dispongono della password possono accedere a queste reti. Il server RADIUS controlla le password immesse dagli utenti e concede o nega l'accesso in base alle esigenze.
- Gestione remota — Gestione remota sta modificando le impostazioni di un dispositivo di rete da una posizione remota. Questa operazione viene in genere eseguita su dispositivi quali computer, switch, router e molti altri che dispongono di un indirizzo IP. Consente agli amministratori di rete di rispondere rapidamente alle richieste o alle sfide, poiché non devono essere fisicamente in loco. Accedere ai dispositivi in Gestione remota è quasi come farlo localmente, con la differenza che l'indirizzo IP locale del dispositivo viene utilizzato per accedere al dispositivo localmente, mentre l'indirizzo IP WAN del dispositivo viene utilizzato quando lo si esegue su un dispositivo remoto.
- Rilevamento punti di accesso non autorizzati: un punto di accesso non autorizzato è un punto di accesso installato in una rete senza esplicita autorizzazione da parte di un amministratore di sistema. I punti di accesso non autorizzati rappresentano una minaccia per la sicurezza, in quanto chiunque abbia accesso all'area può installare consapevolmente o inconsapevolmente un punto di accesso wireless che consente a utenti non autorizzati di accedere alla rete. La

funzione di rilevamento dei punti di accesso non autorizzati sul punto di accesso consente di visualizzare questi punti di accesso non autorizzati che si trovano entro la portata e di visualizzare le relative informazioni nell'utility basata sul Web. All'elenco punti di accesso attendibili è possibile aggiungere qualsiasi punto di accesso autorizzato.

- RSTP — Rapid Spanning Tree Protocol (RSTP) è un miglioramento di STP. RSTP garantisce una convergenza Spanning Tree più rapida dopo una modifica della topologia. Il processo STP può impiegare da 30 a 50 secondi per rispondere a una modifica della topologia, mentre il processo RSTP risponde entro tre volte il tempo di benvenuto configurato. RSTP è compatibile con STP.
- Utilità di pianificazione: l'utilità di pianificazione wireless consente di pianificare un intervallo di tempo per il funzionamento di un punto di accesso virtuale (VAP, Virtual Access Point) o di una radio, in modo da risparmiare energia e aumentare la sicurezza. È possibile associare fino a 16 profili a VAP o interfacce radio diverse, ma a ogni interfaccia è consentito un solo profilo. Ogni profilo può avere un determinato numero di regole di tempo che controllano il tempo di attività della VAP o della WLAN associata.
- Single Point Setup: Single Point Setup è una semplice tecnologia di gestione per più dispositivi che consente di installare e gestire un gruppo di punti di accesso che supportano questa funzione. Offre la praticità di configurare un gruppo di punti di accesso da un singolo punto anziché configurarli singolarmente. Consente inoltre di gestire i punti di accesso in locale o in remoto.
- SNMP — Simple Network Management Protocol (SNMP) è uno standard di rete per l'archiviazione e la condivisione di informazioni sui dispositivi di rete. L'SNMP semplifica la gestione, la risoluzione dei problemi e la manutenzione della rete.
- Spanning Tree: lo Spanning Tree Protocol (STP) è un protocollo di rete utilizzato su una LAN. Lo scopo di STP è garantire una topologia senza loop per una LAN. L'algoritmo STP rimuove i loop attraverso un algoritmo che garantisce la presenza di un solo percorso attivo tra due dispositivi di rete. Il protocollo STP assicura che il traffico utilizzi il percorso più breve possibile all'interno della rete. STP può inoltre riattivare automaticamente i percorsi ridondanti come percorsi di backup in caso di errore di un percorso attivo.
- SSID: SSID (Service Set Identifier) è un identificatore univoco che i client wireless possono connettere o condividere tra tutti i dispositivi di una rete wireless. Fa distinzione tra maiuscole e minuscole e non deve superare i 32 caratteri alfanumerici. Questo nome è anche denominato Nome rete wireless.
- Trasmissione SSID: quando un dispositivo wireless cerca nell'area le reti wireless a cui può connettersi, rileva le reti wireless nel proprio raggio di copertura tramite i relativi nomi di rete o SSID. La trasmissione del SSID è attivata per impostazione predefinita. Tuttavia, è possibile scegliere di disabilitarla.
- TSPEC — Traffic Specification (TSPEC) è una specifica di traffico inviata da un client wireless QoS a un dispositivo WAP che richiede una determinata quantità di accesso alla rete per il flusso di traffico (TS) che rappresenta.
- VLAN: una VLAN (Virtual Local Area Network) è una rete commutata segmentata logicamente in base alla funzione, all'area o all'applicazione, indipendentemente dalla posizione fisica degli utenti. Le VLAN sono un gruppo di host o porte che possono essere collocate in qualsiasi punto della rete ma che comunicano come se si trovassero sullo stesso segmento fisico. Le VLAN semplificano la gestione della rete consentendo di spostare un dispositivo su una nuova VLAN senza modificare le connessioni fisiche.
- WDS — Wireless Distribution System (WDS) è una funzionalità che consente l'interconnessione wireless dei punti di accesso in una rete. Consente all'utente di espandere

la rete con più punti di accesso wireless. WDS inoltre mantiene gli indirizzi MAC dei frame client attraverso i collegamenti tra i punti di accesso. Questa funzionalità è fondamentale perché offre un'esperienza ottimale per i client in roaming e consente la gestione di più reti wireless.
- WMM — Wi-Fi Multimedia (WMM) è una funzione che assegna diverse priorità di processo a diversi tipi di traffico. WMM è anche una funzione QoS che migliora le prestazioni della rete wireless impostando la priorità del pacchetto dati wireless in base a quattro categorie: voce, video, massimo sforzo e background. Per impostazione predefinita, WMM è attivato. Se un'applicazione non richiede WMM, viene assegnata una priorità inferiore rispetto a quella di video e voce.
- Isolamento wireless: impedisce la comunicazione e i trasferimenti di file tra computer connessi a SSID diversi. Il traffico su un SSID non verrà inoltrato ad altri SSID.
- WPA/WPA2 — Wi-Fi Protected Access (WPA e WPA2) sono protocolli di sicurezza utilizzati per le reti wireless per proteggere la privacy mediante la crittografia dei dati trasmessi sulla rete wireless. WPA e WPA2 sono entrambi compatibili con IEEE 802.11e e 802.11i. WPA e WPA2 offrono funzionalità di autenticazione e crittografia migliorate rispetto al protocollo di sicurezza WEP (Wired Equivalent Privacy).

Elenco di termini nelle reti Mesh

- **Access Point (AP)**: Periferica di una rete utilizzata per consentire agli utenti di connettersi alla rete in modalità wireless. A seconda della funzione, è possibile aggiungere etichette specifiche: Principale, remoto, principale, subordinato e così via
- **Rete Mesh Wireless:** Tipo di topologia in cui i punti di accesso wireless si connettono tra loro per l'inoltro delle informazioni. Queste reti funzionano in modo dinamico per adattare le esigenze e mantenere la connettività per tutti gli utenti.
- **AP primario:** Il punto di accesso principale consente la gestione e il controllo della rete wireless e della topologia. Rappresenta il collegamento con il resto della rete esterna, in genere Internet, che utilizza un provider di servizi Internet (ISP). L'access point principale si collega direttamente al router locale che a sua volta instrada il traffico all'interfaccia ISP WAN. L'access point principale è l'orchestrator di tutti i nodi che forniscono servizi wireless all'interno della rete mesh. Gestisce le informazioni dai nodi della rete, la qualità della connessione di ogni client e le informazioni sui router adiacenti per prendere la decisione migliore sul percorso migliore per servizi wireless ottimizzati verso il client mobile.
- **Primario:** L'access point corrente ha il compito di gestire la WLAN.
- **Primario preferito:** Impostazione in cui uno specifico punto di accesso con capacità primaria è elencato come preferito. Se si verifica un errore nell'access point primario, subentra l'access point primario preferito. Una volta eseguito il backup, l'access point preferito non torna automaticamente al sistema precedente. Non è stato specificato un database primario preferito.
- **Punto di accesso principale:** Un access point che dispone di una connessione fisica cablata alla rete. Questo access point deve essere connesso a Ethernet e può diventare il principale se si verifica un errore nel primo.
- **Mesh Extender:** Punto di accesso remoto subordinato nella rete non connesso alla rete cablata.
- **Punto di accesso subordinato:** Termine generale che può essere applicato a qualsiasi punto di accesso mesh non configurato come primario.
- **AP padre:** Un access point padre è un access point che fornisce il percorso migliore per tornare all'access point primario.

- **Punto di accesso figlio:** Un access point figlio è un'estensione di mesh che seleziona l'access point padre come percorso migliore per tornare all'access point primario.
- **Punto di accesso upstream:** Un punto di accesso upstream è un termine generale che si riferisce al flusso di dati di direzione attraverso i punti di accesso quando si passa dal client al server.
- **Punto di accesso downstream:** Un access point a valle trasferisce i dati da Internet al client.
- **Punti di accesso co-posizionati:** Estensori di rete nel raggio di trasmissione del canale backhaul.
- **Nodi:** In questo articolo, i punti di accesso vengono definiti nodi. In generale, i nodi descrivono qualsiasi dispositivo che stabilisce una connessione o un'interazione all'interno di una rete o che è in grado di inviare, ricevere e archiviare informazioni, comunicare con Internet e dispone di un indirizzo IP. In una rete mesh, parametri radio ottimizzati su tutti i nodi garantiscono la massima copertura wireless riducendo al contempo le interferenze radio tra i nodi per fornire velocità di dati e throughput superiori.
- **Backhaul:** In una rete mesh wireless, le informazioni nella LAN (Local Area Network) devono raggiungere un punto di accesso cablato per poter raggiungere Internet. Il backhaul è il processo che consente di riportare le informazioni al punto di accesso cablato.