Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica per la comunicazione digitale (Classe L-31)

REFRESH NETWORK: Evoluzione e Innovazione tra connessioni Wired e Wireless

Laureando
Davide Lotito

Matricola 114627

Relatore
Fausto Marcantoni

Correlatore
Jacopo Fiori

A.A. 2024/2025

Indice

1. Introduzione

In un contesto tecnologico in continua evoluzione come la nostra realtà, la **gestione e l'aggiornamento delle reti aziendali** rappresentano un aspetto cruciale per il **la competitività** di qualsiasi organizzazione. Le reti moderne devono affrontare sfide legate non solo all'**aumento esponenziale del traffico dati** e alla **complessità delle applicazioni**, ma anche ad una crescente esigenza di **sicurezza, scalabilità e adattabilità alle nuove tecnologie**, come il **cloud computing** e la **virtualizzazione**. Questo progetto di tesi si concentra sul **refresh network di una rete aziendale** per un cliente, con l'obiettivo di **migliorare le prestazioni, la sicurezza e la flessibilità** dell'infrastruttura esistente. Il progetto consiste in una **revisione completa dell'architettura di rete attuale**, con un'analisi approfondita delle **esigenze specifiche del cliente**, e culmina nella proposta di una **soluzione tecnologica avanzata e sostenibile**. La tesi seguirà un **approccio metodologico strutturato** che comprende:

- Un'analisi dello stato attuale della rete, con identificazione di **limitazioni, colli di bottiglia e vulnerabilità**;
- Una revisione delle **tecnologie e dei protocolli più recenti** che possono supportare i nuovi requisiti aziendali;
- La progettazione di un'**architettura di rete aggiornata**, comprensiva di un **piano di implementazione graduale** per garantire una **transizione senza interruzioni**.

Il risultato atteso è un'**infrastruttura di rete ottimizzata**, in grado di sostenere le esigenze presenti e future del cliente, migliorando al contempo la **sicurezza, la disponibilità** e le **performance complessive**.

1.1 Che cos'è il network?

Una network (o rete) in ambito informatico è un sistema che consente a dispositivi come: computer, server, smartphone e altri hardware, di comunicare tra loro per condividere dati, risorse e servizi. Si tratta di un'infrastruttura essenziale per il funzionamento delle tecnologie moderne, comprese **internet** e le **reti aziendali** [IBM24]. Dal punto di vista tecnico, una network è costituita da dispositivi (chiamati **"nodi"**) collegati tra loro tramite mezzi fisici, come cavi, o attraverso tecnologie wireless, come il **Wi-Fi** o il **Bluetooth**. Questi dispositivi possono svolgere ruoli diversi: ad esempio, un **client** è un dispositivo che richiede un servizio, mentre un **server** è il nodo che lo fornisce. Il traffico di dati all'interno della rete è regolato da **protocolli di comunicazione**, ovvero insiemi di regole che determinano come i dispositivi trasmettono, ricevono e

interpretano le informazioni. Uno dei protocolli più noti è il **TCP/IP**, che costituisce la base di internet. Le reti informatiche si distinguono per la loro **estensione geografica**. Una **LAN** (Local Area Network) è una rete locale che opera in un'area limitata, come un ufficio o una casa, ed è particolarmente adatta alla **condivisione di risorse** come file o stampanti. Al contrario, una **WAN** (Wide Area Network) collega reti locali su distanze molto ampie, come nel caso di internet. Tra queste due tipologie si collocano le **MAN** (Metropolitan Area Network), che servono aree urbane, e le **PAN** (Personal Area Network), progettate per connessioni personali tra dispositivi vicini, come smartphone e cuffie Bluetooth. [Cre22] Anche la struttura fisica e logica di una rete, nota come **topologia**, gioca un ruolo importante. Tra le topologie più comuni troviamo quella **a stella**, dove tutti i dispositivi sono collegati a un nodo centrale, e quella **a maglia**, che garantisce maggiore ridondanza con connessioni multiple tra nodi. Queste configurazioni influenzano le **prestazioni**, l'**affidabilità** e la **scalabilità** della rete. I dati che viaggiano in una rete sono suddivisi in piccoli blocchi chiamati **pacchetti**, che vengono instradati attraverso i nodi e "riassemblati" all'arrivo. Questo processo è governato dai protocolli di rete, che garantiscono la corretta trasmissione delle informazioni. Ad esempio, il **DNS** traduce i nomi di dominio in indirizzi IP, mentre l'**HTTP** o l'**HTTPS** per i siti sicuri, regola il trasferimento delle pagine web. L'utilizzo delle reti informatiche presenta molti vantaggi. Esse permettono di **condividere risorse** in modo efficiente, semplificando l'accesso a stampanti, file e database da parte di più utenti. Inoltre, consentono una **comunicazione rapida** tramite email, messaggistica istantanea e videochiamate, e favoriscono la **collaborazione** in progetti condivisi. Grazie alla loro **scalabilità**, è possibile aggiungere nuovi dispositivi o utenti senza stravolgere l'infrastruttura esistente. [Tea24]

1.2 Analisi dell'infrastruttura attuale e requisiti di miglioramento

A seguito di un attento sopralluogo svolto nella sede, sia in ambito wired che wireless, e sulla base delle indicazioni e dei miglioramenti suggeriti nel documento di assessment, è stata elaborata una soluzione progettuale che tiene conto dei seguenti aspetti:

- Il **rinnovo tecnologico dell'infrastruttura LAN e Wireless**;
- Una **visione progettuale che garantisca scalabilità e protezione dell'investimento**;
- Un **maggiore livello di semplicità nella gestione e nel controllo della rete**;
- Un **supporto post-vendita adeguato e garantito**.

Il progetto proposto si sviluppa seguendo la visione di **Cisco per le reti di tipo campus**, con un focus sull'introduzione alla visione **SDN (SD-ACCESS) di Cisco**. Successivamente, l'attenzione si concentra sul **deploy della soluzione**, descrivendo nel dettaglio la sua implementazione. Per quanto riguarda l'infrastruttura wired esaminata, questa è strutturata in modo corretto, adottando una **topologia a stella** con il punto focale situato nel **locale CED**. L'area CED è costituita da un'unica stanza, all'interno della quale sono collocati tre rack di rete. Nel primo rack, è presente l'unico **Core Switch Cisco WS-C3750G-12S**, dotato di 12 porte SFP (fino a 1 Gb/s), dal quale

si diramano le connessioni verso i rack periferici. In questo stesso rack sono sistemati anche i due **firewall del Cluster Check-Point** e i **router per la connettività**. Nel secondo rack si trova il **cablaggio in fibra proveniente dalla periferia**, che viene esteso con bretelle di almeno 5 metri verso il core switch 3750. All'interno di questo rack è inoltre presente il **cablaggio in rame**, che supporta l'area commerciale attraverso uno switch Cisco **Fast Ethernet modello Cisco 3524XL**, il quale ha tutte le porte occupate, limitando la possibilità di attivare ulteriori connessioni cablate. L'ultimo rack, situato di fronte all'ingresso, è destinato ai **server**, la cui connettività è garantita da uno switch Cisco **2960G-48TC**, dotato di interfacce in rame 10/100/1000. Questo apparato, purtroppo, risulta più adatto alla connettività di accesso piuttosto che a quella necessaria per supportare i **server che erogano servizi**. Infine, gli **armadi di accesso** sono organizzati con un cablaggio in fibra OM2, che si collega direttamente al Core, garantendo una connessione affidabile e ad alte prestazioni. Questa panoramica sull'infrastruttura attuale fornisce un quadro dettagliato della situazione esistente e delle opportunità di miglioramento offerte dalla proposta progettuale, con l'obiettivo di **ottimizzare l'efficienza e la scalabilità della rete**, oltre a garantire una **gestione centralizzata e semplificata**.

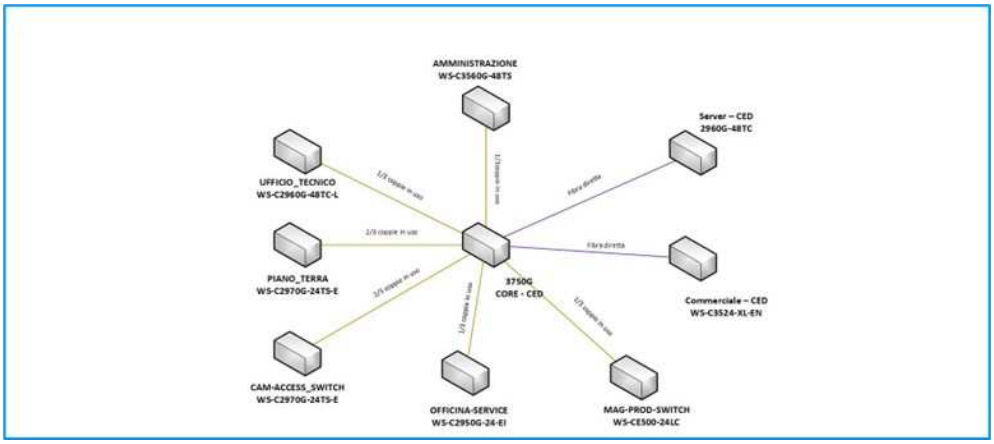

Figura 1.1: Vecchio schema di rete

1.3 Obiettivi e soluzioni tecnologiche

Il progetto consiste nel sostituire i **device oramai obsoleti e fuori supporto** rivedendo non tanto la **topologia fisica**, ma la sua **struttura logica**, introducendo la tecnologia **stackwise** nei due core e la **e ove necessario nei rack periferici con più switch**; in questo modo sarà possibile utilizzare in modalità **active/active** i link sia verso lo stack di CORE utilizzando la tecnologia di **link aggregation (port-channel)** essendo gli switch presenti nei due core, un'unica entità logica. Nel dettaglio sono stati previsti due switch modello **9300X-12Y** dotati di 12 porte, più un'aggiunta di 8 porte grazie al modulo di espansione, con tecnologia SFP/SFP+; nel rack dei server inoltre, sono stati previsti 2 switch **9200L in stack** per interconnettere le porte in rame dei server; questi apparati verranno interconnessi al nuovo core con due cavi **10Gb/s-AOC (Active Optic Cable)** per un totale di **20Gb/s aggregato**, garantendo quindi la banda necessaria, sia ai **server VMware**, sia a qualsiasi dispositivo di rete quali **storage NFS o NAS di rete**. Negli armadi periferici sono stati previsti, anche qui,

switch della famiglia **9200L dotati di tecnologia PoE+ ed uplink** che potranno in futuro scalare fino a **10Gb/s**.

1.4 Descrizione della nuova architettura e benefici attesi

La **nuova architettura di rete** rappresenta un miglioramento sostanziale rispetto alla configurazione precedente, rispondendo non solo alle **esigenze attuali**, ma anche alle **prospettive di crescita futura** dell'organizzazione. Grazie all'introduzione della tecnologia **StackWise**, l'infrastruttura di rete è stata **centralizzata a livello logico**, rendendo più agevoli sia il **monitoraggio** che la **gestione della rete**. Questo approccio elimina i **silos di rete** presenti in precedenza, consolidando il traffico e migliorando la **resilienza del sistema**: in caso di guasto su uno dei dispositivi centrali, la rete può continuare a operare senza interruzioni, assicurando così la **continuità operativa**. L'utilizzo di **Link Aggregation** (tramite il protocollo **Port-Channel**) nei collegamenti tra gli switch di core e i rack periferici ha permesso di incrementare la **capacità di banda** e ottimizzare il **bilanciamento del traffico**. Questa soluzione rende la rete più performante e capace di gestire **carichi di lavoro elevati**, particolarmente vantaggioso in contesti in cui la **velocità di accesso ai dati** e alle **applicazioni** è critica. Inoltre, l'aggregazione dei link permette di ridurre i **tempi di latenza** e garantire un'esperienza più fluida per gli **utenti finali**, migliorando l'efficienza di tutti i servizi che fanno affidamento sulla rete. Gli **switch di accesso di ultima generazione**, predisposti per **PoE+ (Power over Ethernet Plus)**, consentono di alimentare dispositivi collegati direttamente attraverso il cavo di rete, eliminando la necessità di alimentatori separati e semplificando l'installazione di apparecchiature come **telefoni IP, videocamere di sorveglianza** e **access point Wi-Fi**. Questa funzionalità risponde alle esigenze di un **ambiente di lavoro sempre più connesso**, che richiede una rete in grado di supportare un numero crescente di dispositivi e di comunicazione. Inoltre, gli **uplink degli switch di accesso** sono scalabili fino a **10 Gb/s**, permettendo alla rete di accogliere nuovi dispositivi e volumi di traffico aggiuntivi senza perdere in prestazioni. Questo rende l'infrastruttura **altamente scalabile** e pronta per rispondere a esigenze future, senza richiedere aggiornamenti frequenti. Inoltre, l'adozione di **tecnologie ad alte prestazioni** assicura che la rete possa gestire efficacemente sia il **carico di lavoro corrente** sia le possibili espansioni. Le soluzioni implementate offrono un **controllo semplificato e centralizzato**, riducendo la complessità di gestione per il team IT, e garantendo una **maggiore sicurezza** grazie alla possibilità di **segmentare la rete** secondo criteri specifici. Questo migliora la **protezione dei dati** e riduce il rischio di **accessi non autorizzati**, rispondendo anche a **requisiti di compliance** per settori in cui la sicurezza è cruciale. Complessivamente, la nuova architettura non solo risolve le **criticità dell'infrastruttura precedente**, ma rappresenta un **investimento strategico per il futuro**, con un miglior **rapporto costo-beneficio** grazie alla riduzione dei costi di gestione, manutenzione e aggiornamento.

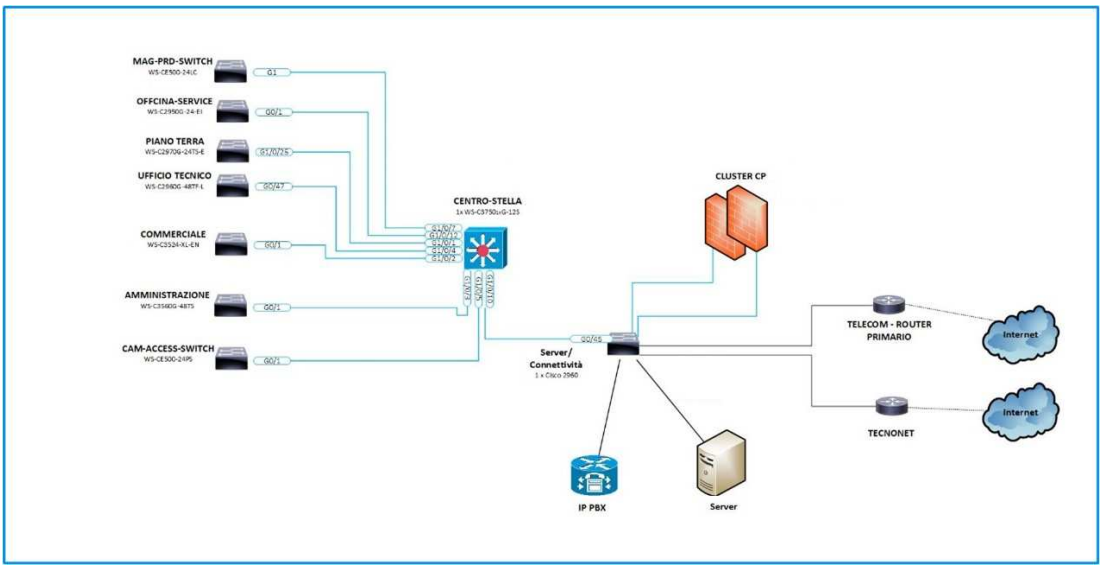

Figura 1.2: Ipotesi nuovo schema di rete

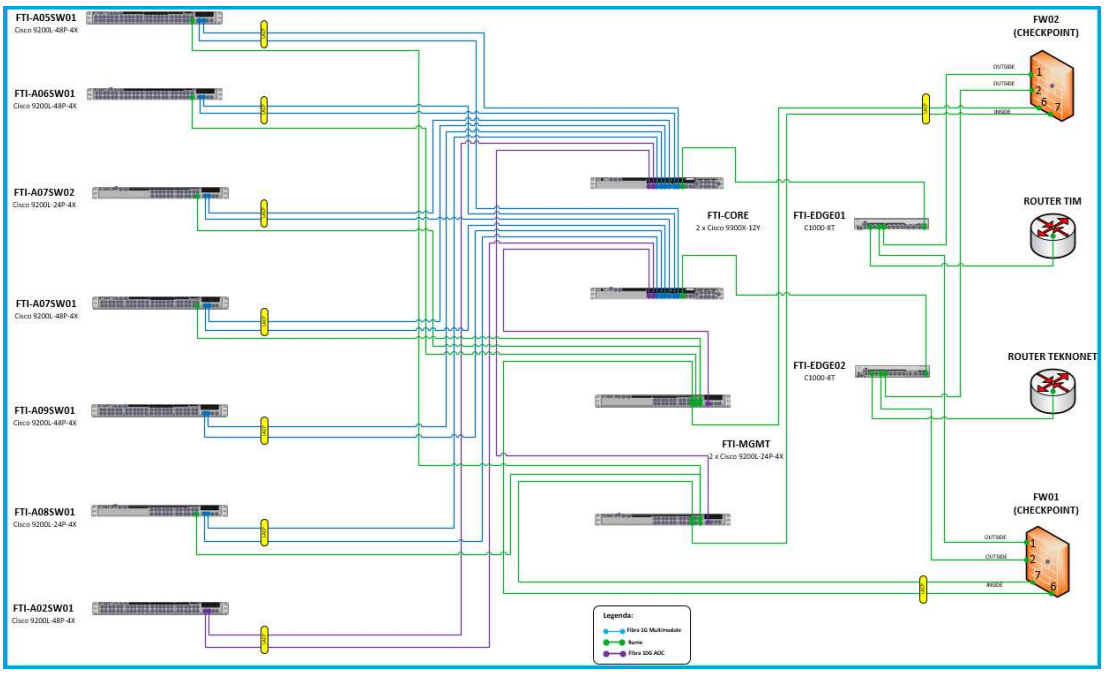

Figura 1.3: Nuovo schema di rete

2. Progettazione dell'architettura di rete: componenti, aggiornamenti e ottimizzazione della struttura wireless

2.1 2.4GHz, 5GHz, 6GHz

Le frequenze di **2.4GHz**, **5GHz** e **6GHz** sono bande radio utilizzate nelle comunicazioni wireless, in particolare per il Wi-Fi. Ogni banda ha caratteristiche che la rendono adatta a specifici scenari di utilizzo, con vantaggi e svantaggi distinti. La banda a **2.4GHz** è la più antica e ampiamente supportata dai dispositivi Wi-Fi. Ha una **portata relativamente lunga** grazie alla sua capacità di attraversare meglio gli ostacoli come muri e altri oggetti. Tuttavia, questa capacità di penetrazione ha anche dei limiti in termini di **velocità**: la banda **2.4GHz** offre prestazioni inferiori rispetto alle altre bande, con velocità che raramente superano i **600 Mbps** nelle configurazioni più avanzate. Inoltre, è una banda molto **congestionata**, poiché oltre al Wi-Fi, la frequenza di **2.4GHz** è condivisa con altri dispositivi elettronici come **forni a microonde**, **telefoni cordless** e alcuni dispositivi **Bluetooth**, causando interferenze che possono compromettere la qualità della connessione. La banda a **5GHz** è stata introdotta per risolvere i problemi di **congestione** della banda a **2.4GHz**. È meno soggetta a interferenze, poiché viene utilizzata da meno dispositivi, e offre **velocità superiori**. Grazie a una **larghezza di banda più ampia**, la banda a **5GHz** supporta velocità teoriche fino a **1.3 Gbps** o più con le tecnologie Wi-Fi più recenti. Tuttavia, la maggiore velocità comporta anche una **portata ridotta**: la banda a **5GHz** ha una minore capacità di attraversare ostacoli, quindi è più adatta a spazi aperti o ambienti in cui non ci sono molte barriere fisiche. Nonostante la ridotta portata, la banda a **5GHz** è preferita per applicazioni che richiedono elevate prestazioni, come lo **streaming video in alta definizione** o il **gaming online**, dove la **velocità** e la **qualità della connessione** sono fondamentali. La banda a **6GHz** è l'ultima arrivata nel mondo delle comunicazioni Wi-Fi e fa parte dello standard **Wi-Fi 6E**. Offre una **velocità ancora maggiore** rispetto alle bande a **2.4GHz** e **5GHz**, con una **larghezza di banda più ampia** e meno **congestione**. Questo la rende ideale per ambienti ad alta densità di dispositivi e per applicazioni che richiedono alte prestazioni, come il **video streaming 8K** o la **realtà virtuale**. Tuttavia, la banda a **6GHz** presenta delle limitazioni simili a quelle della banda a **5GHz** in termini di **portata**, poiché non è altrettanto capace di attraversare ostacoli. Inoltre, i dispositivi compatibili con la banda a **6GHz** sono ancora relativamente pochi, in quanto è una tecnologia recente che richiede **supporto**

hardware specifico.

Caratteristica	**2.4GHz**	**5GHz**	**6GHz**
Velocità	Bassa	Alta	Molto alta
Portata	Lunga	Media	Media
Interferenze	Alta	Media	Bassa
Compatibilità	Universale	Moderna	Nuova generazione

2.2 Tecnologie Wi-Fi

Negli ultimi decenni, le reti di comunicazione wireless sono diventate un elemento fondamentale per la nostra vita quotidiana. L'accesso a **Internet**, la **comunicazione mobile**, la **trasmissione di dati ad alta velocità** e l'**interconnessione di dispositivi smart** sono solo alcune delle applicazioni che dipendono dalle tecnologie wireless. Tra queste, il **Wi-Fi** è la tecnologia che ha rivoluzionato il modo in cui ci connettiamo, consentendo l'accesso a Internet senza l'uso di cavi. Gli standard **Wi-Fi**, definiti dall'**IEEE**, sono evoluti nel tempo per rispondere alle crescenti esigenze di **velocità**, **capacità** e **efficienza** nelle reti moderne. Essa ha subito numerose evoluzioni nel tempo, con ogni nuova versione che porta miglioramenti in termini di **velocità**, **capacità di gestione delle interferenze** e di **connettività**. Gli **standard principali** sono:

- **802.11b** (1999): Uno dei primi standard Wi-Fi, operante sulla banda a **2.4 GHz** con una velocità massima di **11 Mbps**. È stato ampiamente usato, ma oggi è **obsoleto** a causa delle sue limitate prestazioni e della suscettibilità alle **interferenze**;
- **802.11g** (2003): Ha aumentato la velocità fino a **54 Mbps**, ma continua a utilizzare la banda a **2.4 GHz**, con le stesse problematiche di **interferenza**;
- **802.11n** (2009): Introdotto per migliorare le prestazioni con l'uso simultaneo delle bande a **2.4 GHz** e **5 GHz**. Ha una velocità di trasferimento dati fino a **600 Mbps** grazie alla tecnologia **MIMO** (Multiple Input Multiple Output);
- **802.11ac** (**Wi-Fi 5**) (2013): Utilizza principalmente la banda a **5 GHz** e offre velocità fino a **1.3 Gbps**, supportando tecniche avanzate come il **beamforming** e la **larghezza dei canali** per una maggiore capacità;
- 802.11ax (Wi-Fi 6) (2019): Con velocità fino a 9.6 Gbps, Wi-Fi 6 è progettato per ambienti ad alta densità, con funzionalità come OFDMA (Orthogonal Frequency Division Multiple Access) per migliorare l'efficienza della rete.
- **Wi-Fi 6E** (2020): Un'estensione di **Wi-Fi 6**, che sfrutta la nuova banda a **6 GHz** per ridurre le **interferenze** e aumentare la **velocità di trasferimento**. Questo standard è ideale per scenari che richiedono una **larghezza di banda maggiore**, come la **realtà virtuale** o lo **streaming 8K**.
- **Wi-Fi 7** (**802.11be**) (previsto per il 2024): Questo futuro standard promette **velocità fino a 30 Gbps**, miglioramenti nella gestione delle **interferenze** e una **latenza ridotta**, offrendo **performance ottimali** in ambienti molto congestionati. [Cis24b] [Net24a]

La **nuova architettura di rete** è stata progettata per **modernizzare l'infrastruttura esistente**, con l'obiettivo di migliorarne le **prestazioni**, l'**affidabilità** e la **gestione**, rispondendo alle esigenze di **scalabilità** e **semplificazione**. L'aggiornamento si concentra sulla modifica della **struttura logica della rete**, pur mantenendo invariata la **topologia fisica**, per non compromettere la **continuità operativa** e ridurre al minimo l'**impatto sui sistemi esistenti**.

2.3 Core della Rete: Switch Cisco 9300X

Il **cuore della rete** è stato aggiornato con l'installazione di due switch **Cisco 9300X-12Y**, dispositivi di fascia alta ideali per ambienti che richiedono alte prestazioni e una gestione efficiente delle connessioni. Gli switch **Cisco 9300X-12Y** sono dotati di 12 porte 1/10/25 Gb/s, supportando diverse velocità di trasmissione a seconda delle necessità del traffico dati. Questi switch sono progettati per garantire **alte prestazioni** e **resilienza**, grazie alla loro capacità di gestire ampie quantità di traffico senza compromettere la **qualità del servizio**. Oltre a migliorare la **velocità** e la **capacità della rete**, i **Cisco 9300X-12Y** sono fondamentali per la **gestione centralizzata** e la **configurazione semplificata della rete**. La **gestione centralizzata** è essenziale per facilitare la **manutenzione** e l'**aggiornamento della rete**, riducendo la **complessità operativa**. Inoltre, una peculiarità di questi switch è la **modularità**, il che significa che offrono una maggiore **flessibilità** e **scalabilità**. La modularità consente di aggiungere o sostituire moduli specifici, come **porte aggiuntive** o **moduli di alimentazione**, per adattarsi facilmente alle **esigenze future** senza dover sostituire l'intero dispositivo. Questo approccio rende possibile l'**espansione della rete** in modo semplice e **cost-effective**, offrendo la possibilità di supportare nuove funzionalità o aumentare la **capacità della rete** in base alla crescita e all'evoluzione delle **necessità aziendali**. I due switch **Cisco 9300X-12Y** sono stati collegati in **stack** (la tecnologia StackWise, come AOC, sarà spiegata nel paragrafo 2.4), creando una **soluzione unica** e **scalabile** che permette di gestire entrambi gli switch come un **singolo dispositivo**.

2.4 Switch dedicati ai Server: Switch Cisco 9200L

Nel rack destinato ai server, sono stati installati due switch **Cisco 9200L**, configurati anch'essi in modalità **StaclWise** per semplificare la **gestione**. Questi switch sono progettati per supportare le connessioni verso i **server aziendali** e i dispositivi di **storage** (come **NFS** o **NAS**), che richiedono una **larghezza di banda significativa**. Il **Cisco 9200L** è dotato di porte con velocità fino a **10 Gb/s**, sufficiente a garantire una connessione **rapida e stabile** tra i server e gli altri dispositivi della rete. I due switch sono collegati al **core** tramite cavi **10 Gb/s** cavi ottici attivi, che forniscono una **banda aggregata di 20 Gb/s**. Questa configurazione assicura una **trasmissione dati ad alta velocità** e **affidabile**, essenziale per il corretto funzionamento di applicazioni aziendali critiche, come quelle basate su **virtualizzazione** come per esempio **VMWare**, e per l'**accesso rapido** ai sistemi di **storage centralizzati**.

2.5 Rack Periferici e Supporto PoE+

Per i rack periferici, sono stati scelti switch **Cisco 9200L** dotati di supporto per **Power over Ethernet (PoE+)**. Questa tecnologia consente di alimentare i dispositivi di rete

direttamente attraverso il cavo **Ethernet**, eliminando la necessità di cavi separati per l'alimentazione. Ciò semplifica l'**installazione**, riducendo i **costi** e il **disordine dei cablaggi**, oltre a migliorare l'**efficienza energetica**. I dispositivi alimentati da **PoE+** includono **telefoni VoIP**, **videocamere di sorveglianza**, e **access point wireless**, che sono essenziali per le **comunicazioni aziendali**, la **sicurezza** e la **connettività**. Inoltre, gli switch **Cisco 9200L** sono dotati di moduli **SFP** (**Small Form-factor Pluggable**), che offrono maggiore **flessibilità** per la connessione a lunghe distanze tramite **fibre ottiche**. I moduli **SFP** permettono di adattare facilmente le porte dello switch a diverse esigenze di **connettività**, che siano per **reti in rame** o in **fibra**, a seconda dei requisiti specifici della rete, senza compromettere le **prestazioni**. Nel nostro caso, sono stati installati due moduli **SFP da 1Gb** per realizzare un **port-channel** verso il **core della rete**, garantendo una **connessione ridondante** e ad **alta disponibilità**, fondamentale per migliorare la **capacità di banda** e la **resilienza della rete** tra i dispositivi periferici e il core.

2.6 Confronto tra AOC e cavi Stack: tecnologie di connessione a confronto

Nel corso dei capitoli precedenti, sono stati brevemente citati due tipi di soluzioni di connessione utilizzate nelle moderne architetture di rete: i cavi ottici attivi (**AOC**) e i cavi stack. In questa sezione, si procederà con un confronto tra i cavi ottici attivi e i cavi **twinax**, analizzandone le **principali caratteristiche**, **applicazioni** e **differenze**. Successivamente, verranno anche spiegate le **caratteristiche dei cavi stack** e il loro **ruolo nelle configurazioni di rete**.

2.6.1 Cavi Ottici (AOC)

Gli **AOC** sono cavi che combinano la tecnologia di trasmissione ottica con componenti elettronici attivi, permettendo la trasmissione di dati ad alta velocità su distanze relativamente lunghe. La principale caratteristica degli **AOC** è che integrano all'interno del cavo stesso sia i **transceiver ottici** che la **fibra ottica**, semplificando notevolmente l'installazione, poiché non è necessario utilizzare moduli separati. Questi cavi, che supportano velocità fino a **100 Gb/s**, sono ideali per ambienti che richiedono alte prestazioni e larghezza di banda elevata. La tecnologia ottica permette inoltre di superare le limitazioni dei tradizionali cavi in **rame**, come la perdita di segnale su lunghe distanze, e consente di ottenere prestazioni superiori in termini di **latenza** e **capacità di trasmissione**, con una distanza di connessione che può arrivare anche a **100 metri o più**, a seconda del modello e dell'applicazione. Gli **AOC** sono cavi **plug-and-play**, che non richiedono particolari configurazioni o l'uso di moduli separati. Si inseriscono direttamente nelle porte dei dispositivi e sono pronti all'uso, rendendo l'installazione particolarmente semplice. Essendo soluzioni di fascia alta che integrano la tecnologia della **fibra ottica** e componenti elettronici attivi, gli **AOC** tendono ad avere un **costo superiore** rispetto ad altre opzioni.

Figura 2.1: Cavi ottici attivi

2.6.2 Cavi Twinax

I cavi **twinax** sono una soluzione di connessione progettata per distanze più brevi rispetto agli **AOC**. Si tratta di cavi in **rame schermati**, dotati di connettori diretti che possono raggiungere velocità di trasmissione elevate, spesso utilizzati per collegamenti a breve raggio, generalmente inferiori ai **7 metri**. Questi cavi sono comunemente usati in applicazioni di **data center** per connessioni interne tra dispositivi come **switch**, **server** e **storage**. Grazie alla loro costruzione in **rame**, i cavi twinax offrono un buon equilibrio tra **prestazioni** e **costi**. Inoltre, garantiscono una **bassa latenza** e sono **plug-and-play**, rendendo l'installazione relativamente semplice. Rispetto agli **AOC**, i cavi twinax soffrono di limitazioni sulla **lunghezza massima del collegamento** e sulla **flessibilità di utilizzo** in ambienti che richiedono connessioni più lunghe. Per questo motivo, sono più indicati per **infrastrutture di rete locali** o per collegamenti tra **rack adiacenti**.

Figura 2.2: Cavi Twinax

2.6.3 Cavi Stack

I cavi **stack**, invece, sono progettati per interconnettere **switch** in una configurazione **stackable**, ossia per collegare più dispositivi di rete in modo che funzionino come un'unica entità logica. Questa configurazione è molto comune nei sistemi di **networking** dove è necessaria una **gestione centralizzata dei dispositivi**, riducendo la complessità operativa. I cavi stack sono tipicamente utilizzati per collegare **switch** all'interno di uno stesso **rack** o tra **rack adiacenti**. Sono progettati per garantire una **bassa latenza** e **alta velocità di trasmissione** su distanze brevi, generalmente non superiori ai **10-15 metri**. Questi cavi sono particolarmente utili per garantire la **ridondanza** e la **continuità del servizio**: in caso di guasto di uno degli **switch**, gli altri nel gruppo di stack continuano a operare, assicurando che la rete non subisca interruzioni. Per quanto riguarda l'installazione, i cavi stack richiedono una **gestione** e una **configurazione specifica** degli switch per abilitare correttamente il funzionamento della configurazione stackable. Una volta configurati, però, consentono una facile amministrazione grazie alla **gestione centralizzata**. Dal punto di vista del costo, i cavi stack rappresentano una soluzione **economica** per soddisfare le esigenze di stacking degli switch e offrono un buon **rapporto costo-prestazioni** per connessioni locali a breve distanza.[Cab23]

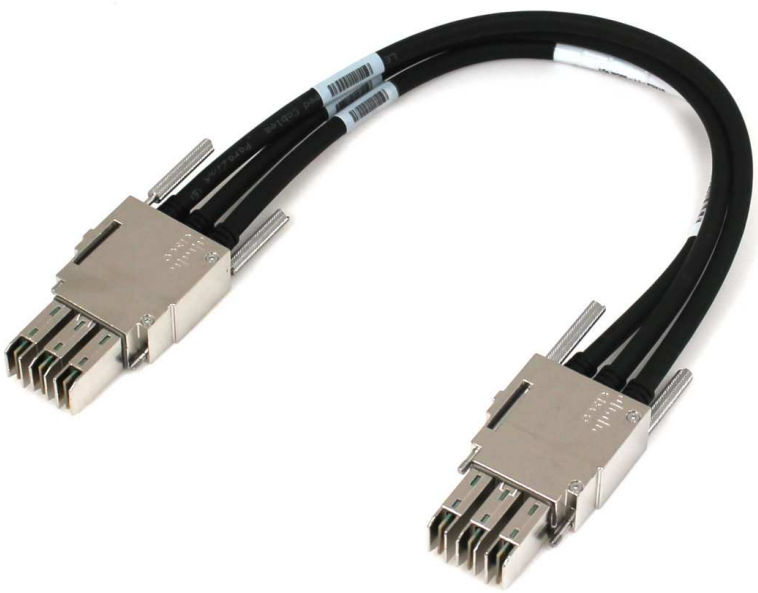

Figura 2.3: Cavi Stack

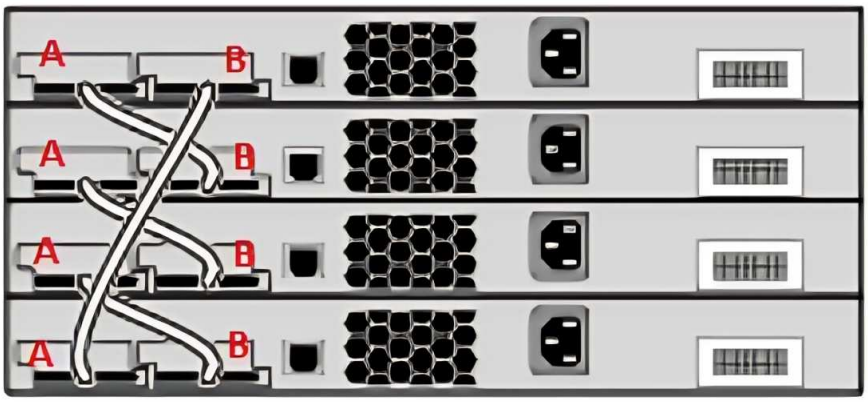

Figura 2.4: Come collegare i cavi stack

2.7 Access point: 9115AX

L'infrastruttura wireless attualmente in uso è composta da sei **Access Point (AP)**, di cui uno del modello **Cisco AIR-AP1121G-E-K9**, dotato di tecnologia **WiFi 1** che è fuori supporto dal **18 giugno 2014**, e cinque dispositivi **TP-Link AC1200**, di cui due modelli standard e tre modelli con supporto alla tecnologia **Mesh**. È previsto un **piano di sostituzione** degli Access Point esistenti, con l'integrazione di nuovi dispositivi **Cisco 9115AX**, che supportano la tecnologia **Wi-Fi 6**. Questi dispositivi sono in grado di gestire connessioni verso client **Wi-Fi 6 (AX)** con una velocità fino a **5,38 Gb/s**, sfruttando canali radio a **160 MHz**. Ogni Access Point, dotato della licenza adeguata, è in grado di supportare fino a **200 client per radio**, garantendo prestazioni elevate e una copertura ottimale in ambienti ad alta densità. È importante considerare che la presenza di diverse generazioni di Access Point all'interno della stessa infrastruttura complica la gestione delle configurazioni, in particolare per quanto riguarda i **profili di radiofrequenza**. Inoltre, la non uniformità nelle funzionalità tra i dispositivi, come nel caso della transizione tra diverse tecnologie Wi-Fi (ad esempio, Wi-Fi 5 e Wi-Fi 1), può generare **disconnessioni** nei dispositivi client quando questi passano da una modulazione all'altra.

2.8 Wireless Lan Controller: 9800-CL

Il **Cisco Wireless LAN Controller 9800-CL** è una soluzione altamente **scalabile** e **versatile** progettata per gestire in modo **centralizzato** e **sicuro** le reti wireless aziendali. Disponibile in tre varianti – **Small**, **Medium** e **Large** – il modello 9800-CL è in grado di supportare throughput fino a **5 Gb/s** in modalità **Central Switching**. Questa caratteristica consente un'**ottimizzazione delle prestazioni** della rete, centralizzando la gestione del traffico e migliorando l'**efficienza operativa**. Una delle caratteristiche più apprezzabili del 9800-CL è la sua **compatibilità** con i principali **hypervisor**, tra cui **KVM**, **Hyper-V** e **VMware**, che lo rendono adatto per ambienti **virtualizzati**. Inoltre, il controller supporta **implementazioni su cloud**, compatibile con piattaforme come **AWS**, **Azure** e **Google Cloud**. Questa **flessibilità** consente alle aziende di scegliere tra una gestione **on-premises** o **cloud**, a seconda delle **esigenze specifiche**, senza compromettere la **performance** o la **sicurezza** della rete. Nel caso in cui, al momento dell'installazione, non fosse disponibile un **hypervisor**, il 9800-CL

può essere temporaneamente attivato in modalità **EWC** (**Embedded Wireless Controller**) all'interno degli **Access Points (AP)**. Questa modalità consente di avviare la rete wireless senza **interruzioni**, garantendo la **continuità del servizio**. Successivamente, è possibile migrare senza costi aggiuntivi al 9800-CL, che fornirà una **gestione centralizzata avanzata** e **prestazioni superiori**. Rispetto alla versione **L** del 9800, il modello 9800-CL offre **vantaggi significativi**, soprattutto in termini di **flessibilità** e **scalabilità**. La versione CL, infatti, supporta una gestione più **dinamica** delle risorse, riducendo la necessità di **hardware fisico** e consentendo un'**implementazione più rapida** e conveniente in ambienti **virtualizzati**. Inoltre, l'**integrazione nativa** con piattaforme **cloud** e la capacità di migrare facilmente da una configurazione basata su **AP** alla versione centralizzata CL, senza necessità di interventi aggiuntivi, lo rende una **scelta ideale** per le aziende in crescita e quelle che richiedono una **gestione agile e scalabile** della propria infrastruttura wireless.

2.9 Realizzazione mappature per copertura Wi-Fi

Nel progetto in questione, è prevista l'installazione di **17 Access Point** per la gestione della rete wireless con un AP di riserva. Poiché la parte produttiva dell'azienda non sarà coperta integralmente in questa fase, l'attenzione sarà concentrata sulla realizzazione della copertura Wi-Fi nelle **aree uffici**. Il posizionamento corretto di ciascun Access Point è cruciale per garantire una connessione stabile, sicura e ad alte prestazioni, riducendo al minimo eventuali interferenze o zone morte nella copertura. Per determinare il posizionamento ottimale degli Access Point, è stata utilizzata una simulazione tramite il software **Ekahau Site Survey**, uno strumento professionale molto diffuso per la pianificazione, progettazione e ottimizzazione di reti Wi-Fi. Questo software consente di eseguire un'analisi dettagliata della copertura wireless, simulando l'ambiente fisico e fornendo dati su diversi parametri, tra cui la **forza del segnale**, la **larghezza di banda**, la **capacità di supportare più dispositivi simultaneamente** e la presenza di **interferenze**.

2.10 Processo di simulazione e posizionamento degli access point

Il primo passo nella simulazione con Ekahau consiste nella creazione di un modello digitale dell'ambiente in cui verrà distribuito il segnale Wi-Fi. Ciò implica l'importazione di una mappa dettagliata dei piani dell'edificio, compresi i muri, i quali possono essere muri portanti oppure di cartongesso, le porte, le finestre e altre caratteristiche strutturali che possono influenzare il segnale radio. Il software tiene conto delle specifiche architetture fisiche e materiali che possono riflettere, assorbire o ostacolare la propagazione del segnale. **Successivamente**, vengono definite le specifiche della rete wireless, come il tipo di Access Point (modello, frequenze supportate, potenza di trasmissione, ecc.) e i requisiti di copertura (come la velocità minima di connessione e la qualità del segnale nelle diverse aree). In questa fase si stabiliscono anche gli obiettivi di copertura. **Una volta definito** l'ambiente e le specifiche, il software esegue una simulazione per determinare il posizionamento ottimale degli Access Point. Ekahau fornisce una serie di mappe e report che visualizzano la forza del segnale (espressa in dBm), le zone di sovrapposizione dei segnali e le possibili aree di interferenza. Vengono evidenziati anche eventuali punti critici, come aree in cui il segnale potrebbe essere

troppo debole o in cui la copertura potrebbe non soddisfare gli standard di prestazione in base anche allo standard scelto. **Sulla base dei risultati ottenuti** dalla simulazione, il posizionamento degli Access Point viene ottimizzato. In particolare, si cerca di evitare collocazioni che possano portare a interferenze tra i dispositivi o a zone morte, ossia aree in cui il segnale Wi-Fi è insufficiente per garantire una connessione stabile. Gli Access Point vengono disposti in modo da massimizzare la copertura nelle aree più critiche, come le postazioni di lavoro negli uffici, cercando di minimizzare i problemi di interferenza, che potrebbero derivare da pareti, mobili o dispositivi elettronici. **Un ulteriore step importante** consiste nella verifica della capacità della rete Wi-Fi simulata, per accertarsi che la copertura progettata possa supportare il numero di dispositivi previsti senza compromettere la qualità del servizio. Ekahau consente di monitorare anche il carico di traffico previsto, assicurando che ogni Access Point possa gestire adeguatamente il numero di connessioni simultanee necessarie.

2.11 Vantaggi dell'uso di Ekahau

L'utilizzo di Ekahau Site Survey offre numerosi vantaggi, tra cui la possibilità di eseguire simulazioni approfondite per ottimizzare la progettazione della rete Wi-Fi. La simulazione consente di determinare con precisione il posizionamento degli Access Point, evitando installazioni inefficaci che potrebbero compromettere la qualità della rete. Inoltre, il software permette di eseguire simulazioni non solo per gli Access Point, ma anche per dispositivi mobili, garantendo che la rete sia progettata per offrire prestazioni eccellenti su ogni tipo di dispositivo connesso. **Un buon posizionamento iniziale degli Access Point**, basato sulle simulazioni, riduce significativamente la necessità di costose modifiche dopo l'installazione, come l'aggiunta di ulteriori dispositivi per risolvere problemi di copertura. Ekahau permette anche di lavorare con le diverse bande di frequenza, tra cui 2.4GHz, 5GHz e 6GHz, ottimizzando la rete per ogni tipo di dispositivo e ambiente, e assicurando che la copertura sia omogenea e senza interferenze in tutte le aree critiche. **Grazie alla visualizzazione dei punti critici**, è possibile ottimizzare la rete per garantire la massima velocità e stabilità della connessione Wi-Fi. Il software consente di visualizzare le aree con segnale debole o interferenze, permettendo di prendere decisioni informate per migliorare la qualità complessiva del servizio. Inoltre, **la simulazione consente di fare previsioni** su come la rete potrebbe evolvere nel tempo, facilitando la pianificazione di eventuali espansioni o modifiche future senza compromettere l'integrità della rete. Ekahau offre la possibilità di monitorare anche la capacità della rete, assicurando che possa gestire un numero crescente di dispositivi e traffico senza perdita di performance. [Eka23]

Figura 2.5: Ekahau

Un esempio pratico di mappatura della rete Wi-Fi può essere osservato nelle figure seguenti. Queste mappe mostrano la distribuzione del segnale Wi-Fi in un ambiente aziendale, evidenziando le aree con segnale forte e quelle con segnale debole. Grazie a queste mappature, è possibile identificare facilmente le zone in cui il posizionamento degli Access Point deve essere ottimizzato per garantire una copertura uniforme e una connessione stabile. Le diverse tonalità di colore rappresentano la forza del segnale, con le aree rosse che indicano un segnale debole e quelle verdi un segnale forte. Le immagini forniscono una visione chiara di come le pareti e gli ostacoli fisici possano influenzare la propagazione del segnale, permettendo agli ingegneri di prendere decisioni informate per migliorare l'efficienza della rete.

Figura 2.6: Piano terra e produzione

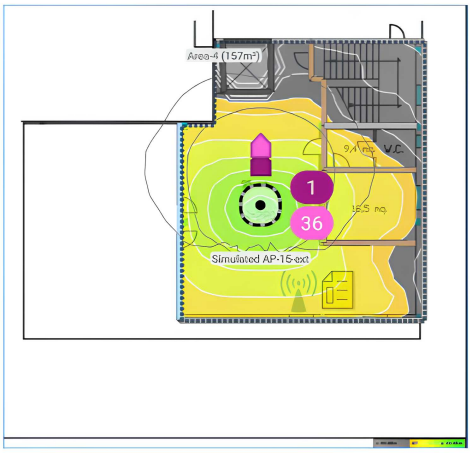

Figura 2.7: Piano Sottotetto

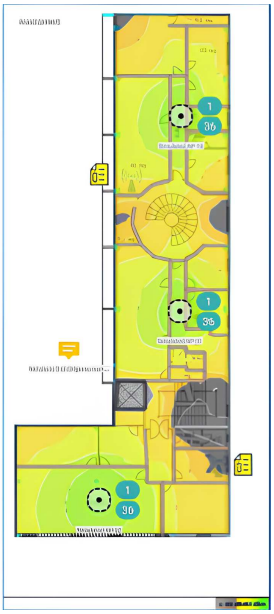

Figura 2.8: Piano Primo

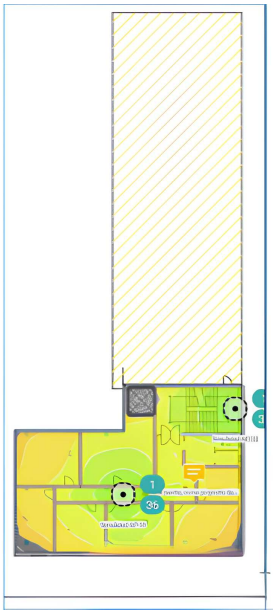

Figura 2.9: Piano Secondo

3. Fasi di Aggiornamento e Configurazione della rete: migrazione tra vecchi e nuovi dispositivi

Per garantire una transizione senza intoppi, è necessario assicurarsi che le nuove configurazioni siano allineate alle impostazioni della rete preesistente, in modo da evitare disservizi e assicurare la continuità operativa. La seguente descrizione illustra il processo di aggiornamento e configurazione, passo dopo passo. Il primo passo è recarsi presso il cliente e salvare le configurazioni degli switch e degli altri dispositivi di rete esistenti. Questo è fondamentale per avere una copia di backup della configurazione attuale, che servirà da riferimento per riprodurre e adattare le impostazioni sui nuovi dispositivi. La configurazione degli switch e del WLC (Wireless LAN Controller) include informazioni cruciali come:

- **Le VLAN (Virtual Local Area Network) configurate**
- **Le politiche di sicurezza e di accesso**
- **Le configurazioni di routing, tra cui i percorsi statici o dinamici**
- **I profili di accesso degli utenti per i dispositivi wireless**

Questa fase di backup permette di prevenire la perdita di configurazioni importanti, ed è utile anche in caso di necessità di rollback in caso di problemi.

3.1 Configurazione e ottimizzazione degli switch

Una volta ottenuto il backup, si passa alla configurazione dei nuovi switch. Questi dispositivi devono essere configurati per replicare le stesse impostazioni della rete esistente, in modo da mantenere una coerenza nella segmentazione della rete e nella gestione delle risorse. Le **VLAN**, che definiscono i diversi segmenti di traffico sulla rete, devono essere configurate in modo identico rispetto ai vecchi switch. Nel corso del documento è stato spesso fatto riferimento al termine "VLAN" senza mai attribuirgli una spiegazione, la quale verrà fornita a breve per spiegare nel dettaglio che cosa sia e quale ruolo svolga all'interno di una rete. Una VLAN è una **rete locale virtuale** [ITi24] che consente di **segmentare logicamente una rete fisica in più reti distinte**. Questo approccio permette di **separare il traffico** di dispositivi collegati alla stessa infrastruttura fisica, migliorando la **sicurezza, la gestione e le prestazioni**

della rete. Ogni VLAN agisce come una rete separata, **isolando il traffico tra i dispositivi appartenenti a VLAN diverse**, anche se sono fisicamente collegati agli stessi switch. Ad esempio, in un ufficio, è possibile utilizzare una VLAN per i computer amministrativi e un'altra per i dispositivi guest, **evitando che i dati delle due reti si mescolino**. Vengono identificate tramite un **ID VLAN** e sono configurate sugli switch utilizzando il protocollo **802.1Q**, che aggiunge un'etichetta ai pacchetti di dati per identificarne l'appartenenza a una VLAN specifica. Inoltre, è necessario configurare correttamente il **trunking** (anche questo termine verrà spiegato nella sezione subito successiva a questa), per consentire il passaggio del traffico multi-VLAN attraverso le porte fisiche, ottimizzando la distribuzione del traffico. Altri aspetti fondamentali della configurazione includono le **politiche di qualità del servizio (QoS)** per garantire la priorità di traffico per applicazioni critiche come la telefonia VoIP o il traffico video. [Inf24b] Infine, sono stati configurati lo **Spanning Tree Protocol (STP)** [Cis24a] e i **Port Channel** per migliorare la stabilità, la ridondanza e la capacità della rete. L'**STP** è una tecnologia di livello 2 sviluppata per evitare i loop di rete in topologie complesse in cui esistono percorsi ridondanti tra switch. I loop di rete, che si verificano quando un pacchetto di dati continua a circolare indefinitamente, possono causare gravi problemi di prestazioni e persino il blocco dell'intera rete. Per evitare ciò, l'**STP** seleziona un singolo percorso attivo verso ogni segmento di rete, bloccando temporaneamente i percorsi ridondanti. Questo avviene tramite un processo di selezione di un **root bridge**, ossia lo switch centrale della topologia, con cui ogni altro switch stabilisce un percorso ottimale. L'**STP** blocca i percorsi alternativi finché non sono necessari; se un percorso attivo si guasta, il protocollo è in grado di riattivare automaticamente un percorso precedentemente bloccato, assicurando la continuità del traffico. Grazie ad esso, le reti Ethernet possono utilizzare la ridondanza senza incorrere in loop, mantenendo stabilità e affidabilità. Il **Port Channel**, noto anche come **EtherChannel** nei dispositivi Cisco, è invece una tecnologia che permette di aggregare più link fisici in un singolo collegamento logico. Questo migliora la capacità di banda tra due dispositivi di rete e aggiunge ridondanza. In altri modi, una connessione **Port Channel** permette di utilizzare contemporaneamente più porte fisiche tra due switch o tra uno switch e un router, sommandone la capacità. Se una delle porte fisiche all'interno del **Port Channel** si guasta, le altre restano attive, evitando l'interruzione del collegamento. Il **Port Channel** distribuisce il traffico di rete tra i vari link fisici in base a un algoritmo di bilanciamento del carico, che seleziona la porta fisica su cui trasmettere in base a parametri come l'indirizzo MAC o IP, la porta TCP o UDP, o altre caratteristiche del traffico. Insieme, **STP** e **Port Channel** ottimizzano la resilienza e le prestazioni della rete. Lo **STP** elimina i loop e gestisce la ridondanza a livello di topologia di rete, mentre il **Port Channel** sfrutta al massimo i collegamenti fisici disponibili, aumentandone la capacità e aggiungendo un ulteriore livello di tolleranza ai guasti. Quando combinati, questi due strumenti consentono di costruire reti di livello 2 più robuste e ad alte prestazioni, che supportano in modo efficiente la crescente domanda di connettività e affidabilità delle reti moderne. In aiuto dell'STP, è stato implementato lo **Storm Control**, una funzionalità fondamentale nelle reti di comunicazione moderne, utilizzata per prevenire fenomeni di congestione causati da traffico eccessivo, come broadcast storm, multicast storm e unicast storm. Questi eventi si verificano quando un volume anomalo di pacchetti broadcast, multicast o unicast sconosciuti sovraccarica gli switch di rete, con potenziali conseguenze come perdita di pacchetti, degrado delle prestazioni o addirittura il collasso dell'infrastruttura. Il principio di funzionamento dello Storm Control si basa sul monitoraggio del traffico in ingresso su ogni porta dello

switch. Quando il traffico supera una soglia predefinita, configurabile dall'amministratore di rete, lo switch può intervenire per limitarlo. Le azioni correttive includono lo scarto dei pacchetti eccedenti, la riduzione della velocità di trasmissione o la generazione di allarmi per il monitoraggio. Un meccanismo chiave del controllo è l'isteresi, che evita attivazioni instabili definendo una soglia di disattivazione inferiore a quella di attivazione. L'implementazione dello Storm Control è particolarmente utile in contesti come le reti aziendali, i data center e le infrastrutture pubbliche, dove garantisce stabilità e protezione contro eventi di congestione accidentale o attacchi mirati. Tuttavia, la funzionalità presenta anche limiti: se configurata in modo troppo restrittivo, può bloccare traffico legittimo, e non fornisce un'analisi dell'origine del problema, concentrandosi solo sul traffico anomalo. Una configurazione accurata è quindi essenziale per ottimizzarne l'efficacia. [Clo24]

```
Esempio di Port-Channel con e senza Spanning Tree

interface Port-channel1
description
switchport mode trunk
storm-control broadcast level 0.50
storm-control multicast level 1.00


interface Port-channel2
description
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
spanning-tree bpduguard enable
```

Figura 3.1: C9300X con moduli SFP

3.2 Differenza tra porte: TRUNK e ACCESS

Nella sezione precedente sono state introdotte le porte in modalità **trunk**; tuttavia, per descriverne al meglio il funzionamento, risulta necessario metterle a confronto con altre porte denominate **access**. Questo confronto permette di evidenziare le differenze principali tra le due configurazioni e di chiarire i contesti di utilizzo specifici. Le porte **access** e **trunk** sono configurazioni comuni sugli switch e svolgono ruoli fondamentali nella gestione del traffico di rete, in particolare in ambienti che richiedono la segmentazione del traffico. Ogni tipo di porta si distingue per il modo in cui gestisce i dati e li instrada all'interno della rete. Una porta **access** è progettata per collegare dispositivi finali, come computer, stampanti o terminali, a una singola rete virtuale. In pratica, trasmette esclusivamente il traffico relativo a quella rete, garantendo che i dispositivi connessi possano comunicare correttamente all'interno del segmento di appartenenza. Inoltre, il traffico su queste porte non è etichettato, poiché viene implicitamente associato alla configurazione predefinita. Al contrario, una porta **trunk** è configurata per trasportare dati provenienti da più reti virtuali contemporaneamente. Queste porte vengono utilizzate per connettere dispositivi di rete come switch o router che necessitano di gestire segmenti multipli. Grazie al protocollo **802.1Q**, ogni frame di dati è contrassegnato con un identificativo che ne specifica l'origine, permettendo a un singolo collegamento fisico di supportare più segmenti logici. Le porte trunk sono etichettate in modi diversi a seconda del produttore dell'apparato di rete. Nei dispositivi **Cisco**, le porte configurate in modalità trunk sono associate al termine "**trunk**".

```
Interface              IP-Address       OK? Method Status       Protocol
GigabitEthernet0/1     192.168.1.3      YES unset  up           up
GigabitEthernet0/2     192.168.20.20    YES unset  up           up
GigabitEthernet0/3     192.168.30.36    YES unset  up           up
GigabitEthernet0/4     192.168.50.52    YES unset  up           up
GigabitEthernet0/5     unassigned       YES unset  admin        down
```

A scopo informativo, in questo progetto non sono stati utilizzati switch **HP Aruba**, però si tiene a sottolineare come invece viene utilizzato il termine **tagged** per indicare le porte che trasportano traffico appartenente a più VLAN, oppure **untagged** per rappresentare una porta in modalità access. Cisco è preferito rispetto a HP Aruba per la sua affidabilità, scalabilità e sicurezza avanzata, ideali per grandi aziende e reti complesse. Inoltre, offre una gamma completa di soluzioni integrate e un forte supporto. Aruba, d'altra parte, è una buona scelta per piccole e medie imprese grazie a costi più bassi e una gestione semplificata.

```
   Interface  Name     MAC Address         VLAN   Type         Admin  Oper
1  User VLAN           00:11:22:33:44:55   10     untagged      up     up
2  Server VLAN         00:11:22:33:44:56   20     untagged      up     up
3  Trunk to Core       00:11:22:33:44:57   10,20  tagged        up     up
4  Trunk to Server     00:11:22:33:44:58   10,20  tagged        up     up
5          -           00:11:22:33:44:59   none     -           down   down
```

Nel progetto, le porte **trunk** sono state configurate esclusivamente per connettere gli **Access Point, il server e i firewall**. In questo modo, il traffico proveniente da dispositivi wireless, distribuito su diverse reti virtuali, può essere gestito attraverso un unico collegamento fisico. Questa configurazione consente di segmentare e isolare il

traffico wireless, garantendo **sicurezza** e **flessibilità** senza la necessità di connessioni dedicate per ogni segmento.

```
Esempio di Porta Trunk

interface GigabitEthernet1/0/19
description FW01 (LAN)
switchport mode trunk
switchport nonegotiate
power inline never
channel-group 2 mode active
spanning-tree portfast trunk
spanning-tree bpduguard enable


Esempio di Porta Access

interface GigabitEthernet1/0/1
description
switchport mode access
switchport nonegotiate
power inline never
storm-control broadcast level 5.00
storm-control multicast level 10.00
spanning-tree portfast
spanning-tree bpduguard enable
```

3.3 Firewall: tipologie e funzioni nella protezione delle reti

Per il cliente, è stato configurato un **firewall** in grado di monitorare e proteggere efficacemente la rete aziendale, applicando politiche di sicurezza personalizzate. Il **firewall** è uno strumento fondamentale per la sicurezza informatica, progettato per monitorare e controllare il traffico di rete in entrata e in uscita, proteggendo la rete da accessi non autorizzati, malware e altre minacce. Il suo funzionamento si basa su un set di regole di sicurezza predefinite che determinano se il traffico può essere consentito o bloccato. Solitamente posizionato tra una rete privata, come una rete aziendale, e una rete pubblica, come Internet, il **firewall** agisce come una barriera per prevenire attacchi esterni e garantire la sicurezza interna. Esistono diversi tipi di **firewall**, che si distinguono per il livello di analisi e le capacità di protezione. Il **firewall stateless** è il tipo più semplice. Funziona analizzando i singoli pacchetti di dati in transito, senza tener conto delle connessioni stabilite precedentemente. Ogni pacchetto viene esaminato in modo sequenziale, cioè indipendentemente dal contesto. Le decisioni vengono prese basandosi solo su informazioni contenute nell'intestazione del pacchetto, come l'indirizzo IP e la porta, senza analizzare lo stato della connessione o se il pacchetto faccia parte di una sessione legittima. Questo rende il **firewall stateless** molto veloce, ma anche meno sicuro, poiché non è in grado di riconoscere attacchi complessi che si sviluppano su più pacchetti o sessioni. Il **firewall stateful**, invece, tiene traccia delle connessioni attive e delle sessioni di rete. Quando un pacchetto arriva, il **firewall** può

verificare se esso appartiene a una connessione già esistente, grazie alla tabella di stato che mantiene. Questo approccio consente al **firewall** di applicare politiche più complesse, come il blocco dei pacchetti provenienti da connessioni non autorizzate. Poiché può riconoscere il traffico "**legittimo**" proveniente da una connessione già stabilita, il **firewall stateful** offre una protezione più robusta rispetto al **firewall stateless**, che non ha una visione globale dello stato delle connessioni. [Forb] Il **firewall proxy** agisce come intermediario tra gli utenti e le risorse esterne. Analizzando il traffico a livello applicativo, è in grado di esaminare il contenuto dei pacchetti, permettendo di bloccare traffico indesiderato anche a livello di applicazione. Questo tipo di **firewall** è in grado di filtrare traffico specifico delle applicazioni, come **HTTP** o **FTP**, e garantire un livello di protezione più profondo, ma può risultare più lento rispetto ai **firewall stateless** e **stateful** a causa dell'elaborazione intensiva dei pacchetti. [Fora] I **firewall** di nuova generazione (**NGFW**) combinano le caratteristiche di **firewall stateful** con funzionalità avanzate come il rilevamento delle intrusioni (**IDS/IPS**), l'ispezione profonda dei pacchetti (**DPI**), il filtraggio a livello applicativo e il controllo del traffico basato su identità e applicazioni. Questi **firewall** sono progettati per affrontare minacce sofisticate e applicare politiche di sicurezza molto dettagliate, distinguendo tra utenti, applicazioni e contenuti specifici. Un **firewall** svolge un ruolo cruciale nella protezione delle reti aziendali, principalmente impedendo che il traffico dannoso raggiunga la rete interna. La sua funzione principale è quella di proteggere contro gli accessi non autorizzati, proteggere dal malware e isolare segmenti di rete per evitare la diffusione di minacce. Inoltre, i **firewall** permettono agli amministratori di rete di definire politiche di sicurezza per controllare chi può accedere a determinate risorse e in quali condizioni. Con l'evoluzione delle minacce informatiche, i **firewall** si sono adattati, integrando funzionalità avanzate come l'analisi profonda dei pacchetti (**DPI**), il controllo delle applicazioni, i sistemi di rilevamento e prevenzione delle intrusioni (**IDS/IPS**) e la gestione del traffico basata su identità, permettendo di offrire una protezione molto più dettagliata e di rilevare minacce sofisticate. Tuttavia, è fondamentale che i **firewall** siano parte di una strategia di sicurezza integrata, che includa anche altre misure di protezione, come il monitoraggio continuo, politiche di accesso restrittivo e la gestione delle minacce interne. Per consentire al **firewall** di comunicare efficacemente con tutti i segmenti di rete, è necessario che supporti l'interconnessione tra più **VLAN**, cosa resa possibile tramite l'utilizzo delle porte in **trunk**.

3.4 Configurazione del Wireless Lan Controller

Una volta completata la configurazione degli switch, il passo successivo consiste nell'impostazione del **Wireless LAN Controller** (**WLC**), un elemento chiave per la gestione efficiente e centralizzata della rete wireless. Il **WLC** svolge un ruolo cruciale poiché consente di amministrare centralmente tutti gli **Access Point** (**AP**) collegati alla rete, fornendo un controllo uniforme sulle configurazioni, sulle politiche di accesso e sulle impostazioni di sicurezza. Attraverso la gestione centralizzata, si riduce la necessità di configurare manualmente ogni singolo **Access Point**, rendendo la rete wireless più scalabile, uniforme e facilmente amministrabile. Per garantire una transizione fluida dalla rete preesistente alla nuova configurazione, il **WLC** deve essere programmato per gestire e trasmettere gli stessi **SSID** (**Service Set Identifier**) precedentemente utilizzati. Il mantenimento degli stessi **SSID** è fondamentale perché permette agli utenti di continuare a connettersi alla rete senza dover modificare le loro impostazioni di connessione, migliorando l'esperienza utente e riducendo la probabilità di interruzioni. Oltre

alla configurazione degli **SSID**, è indispensabile replicare e, se necessario, rafforzare le politiche di sicurezza wireless già implementate. I metodi di autenticazione avanzati, come **WPA2** e **WPA3**, sono fondamentali per proteggere l'accesso alla rete, e devono essere configurati per offrire la massima sicurezza. **WPA2** rimane ampiamente utilizzato, ma **WPA3** offre protezioni più robuste contro attacchi di tipo brute-force e spoofing, e per questo dovrebbe essere preferito se supportato dai dispositivi. Se nella rete è previsto un sistema di autenticazione centralizzato, è essenziale configurare il server **RADIUS** (**Remote Authentication Dial-In User Service**). Questo server consente una gestione centralizzata degli accessi, fornendo autenticazione, autorizzazione e registrazione delle attività di accesso degli utenti. Configurare correttamente il server **RADIUS** permette di migliorare il livello di sicurezza della rete, garantendo che solo utenti autorizzati possano accedere a determinati **SSID** o segmenti della rete. Un altro aspetto tecnico fondamentale nella configurazione del **WLC** riguarda la gestione delle frequenze radio e dei canali Wi-Fi. In un ambiente denso di dispositivi, come un ufficio con numerosi computer, telefoni e tablet connessi, l'uso ottimale delle frequenze e dei canali diventa essenziale per ridurre le interferenze e massimizzare la copertura della rete wireless. Il **WLC** deve quindi essere configurato per distribuire i canali Wi-Fi in modo efficiente, evitando sovrapposizioni che potrebbero causare congestioni di rete o interferenze, soprattutto se la rete opera su entrambe le bande **2.4 GHz** e **5 GHz**. Alcuni **WLC** offrono funzionalità avanzate di gestione dinamica delle frequenze, che rilevano automaticamente i canali meno affollati e spostano gli **Access Point** su canali meno utilizzati, migliorando così la qualità della connessione per tutti i dispositivi connessi. Infine, se il roaming tra **Access Point** è un requisito fondamentale della rete, è necessario configurare attentamente le impostazioni di mobilità. Il roaming è cruciale in ambienti in cui gli utenti si spostano frequentemente, come campus universitari, grandi uffici o stabilimenti industriali, poiché consente ai dispositivi di passare da un **AP** all'altro senza interruzioni nella connessione o perdita di sessione. Per garantire un roaming fluido, il **WLC** deve essere configurato per supportare la mobilità degli utenti tra diversi **AP**, mantenendo le sessioni attive senza richiedere nuove autenticazioni o disconnessioni, un aspetto essenziale per applicazioni sensibili come le chiamate **VoIP**, le videochiamate o le app in tempo reale. Sebbene fosse stato inizialmente proposto un **WLC** diverso, si è infine deciso di adottare il **WLC 9800-L**, un modello fisico avanzato, messo a disposizione dalla società appartenente a un grande gruppo aziendale di cui fa parte anche l'azienda che ha richiesto il network refresh.

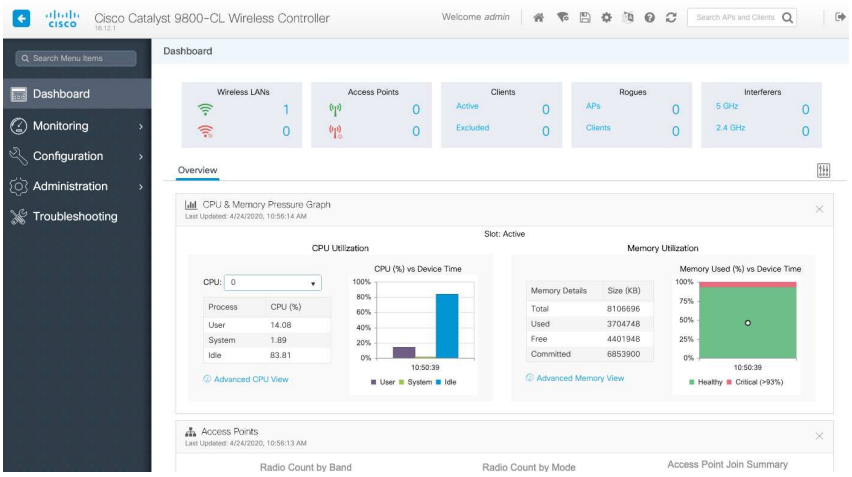

Figura 3.2: WLC 9800-CL

3.5 Local Switching e Central Switching

Nel contesto delle reti wireless gestite da un WLC, uno degli aspetti fondamentali da considerare è la modalità di switching dei dati tra gli AP e la rete centrale. Esistono due principali modalità di switching: il **local switching** e il **central switching**, ciascuna con vantaggi e svantaggi specifici in base alle esigenze della rete. Il **central switching** implica che il traffico tra gli AP e i dispositivi connessi venga instradato verso il **Wireless LAN Controller**, che funge da punto centrale di gestione per tutta la rete. In questa configurazione, i dati sono centralizzati, il che consente una gestione più coerente delle politiche di rete, della sicurezza e del controllo della qualità del servizio. Il **central switching** è ideale in scenari dove la **centralizzazione della gestione** e l'**uniformità delle politiche di accesso** sono essenziali. Tuttavia, questo modello può introdurre una maggiore **latenza** e un aumento della **congestione sulla rete di backhaul**, poiché tutto il traffico wireless deve passare attraverso il controller centrale. D'altro canto, il **local switching**, ossia la modalità scelta da noi, si riferisce alla modalità in cui i dati vengono instradati direttamente tra l'**Access Point** e la **destinazione finale** senza passare attraverso il **Wireless LAN Controller**. In pratica, il traffico destinato a un client che si trova nello stesso segmento di rete locale dell'AP viene gestito localmente, riducendo la **latenza** e migliorando la **velocità di comunicazione**. Questo tipo di switching è particolarmente utile in ambienti con traffico intenso o in scenari in cui è richiesta una **bassa latenza**, come per applicazioni in tempo reale o videochiamate. Inoltre, consente di distribuire meglio il carico sulla rete, evitando il **sovraccarico del WLC**. La scelta tra **local** e **central switching** dipende principalmente dalle specifiche esigenze dell'infrastruttura di rete. Ad esempio, in ambienti aziendali con molti dispositivi mobili, il **central switching** può essere vantaggioso per garantire una **gestione centralizzata** e una **sicurezza uniforme**, mentre in ambienti ad alta densità di traffico o con un alto numero di connessioni simultanee, il **local switching** può ridurre la **latenza** e migliorare le **prestazioni complessive della rete**.

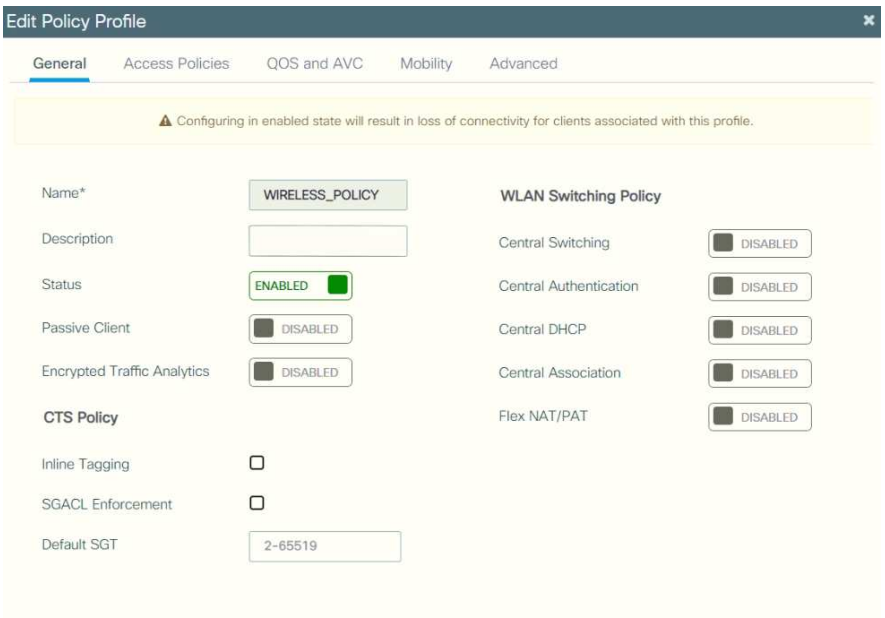

Figura 3.3: Local Switching

3.6 Configurazione degli Access Point

Infine, si procede alla configurazione degli **Access Point** (**AP**). Gli **Access Point** sono dispositivi di rete che fungono da ponti tra la rete cablata e i dispositivi wireless. Ogni **Access Point** crea una zona di copertura wireless, consentendo ai dispositivi mobili di connettersi alla rete cablata tramite il Wi-Fi. In sostanza, gli **AP** ampliano l'area di accesso alla rete, permettendo agli utenti di spostarsi liberamente senza perdere la connessione. Per ottenere una gestione centralizzata, gli **AP** devono essere registrati correttamente con il **Wireless LAN Controller** (**WLC**), che provvede a configurare e gestire automaticamente tutte le impostazioni di ciascun dispositivo, riducendo la necessità di configurazione manuale su ogni singolo punto di accesso. La configurazione degli **AP** include la creazione e l'associazione degli **SSID** configurati nel **WLC**, assicurando che gli utenti possano connettersi alla rete wireless utilizzando le stesse credenziali e impostazioni preesistenti. Un altro aspetto cruciale della configurazione riguarda l'ottimizzazione delle potenze di trasmissione degli **AP**, un parametro fondamentale per garantire che i segnali Wi-Fi non si sovrappongano tra gli **AP** adiacenti. La gestione delle potenze di trasmissione permette di evitare interferenze tra i segnali radio e di assicurare una copertura adeguata in tutte le aree, migliorando l'affidabilità e la qualità della connessione wireless. Inoltre, una corretta distribuzione degli **Access Point** è essenziale per coprire in modo uniforme le aree critiche della rete, come le postazioni di lavoro negli uffici. La disposizione degli **AP** deve essere progettata in modo da minimizzare le zone morte, ossia quelle aree prive di segnale, e ridurre al minimo le interferenze tra i dispositivi. Una volta configurati, gli **Access Point** devono essere testati per garantire che il traffico wireless venga gestito correttamente. Questo include il test della connettività tra gli switch, il **WLC** e gli **AP**, per verificare che tutti i dispositivi siano correttamente integrati e che la rete funzioni senza interruzioni. Inoltre, è fondamentale controllare la qualità del segnale nelle diverse aree, utilizzando strumenti di misurazione per valutare la copertura e le prestazioni della rete Wi-Fi. Durante i test, si deve monitorare attentamente la performance della rete Wi-Fi, verificando che i dispositivi si connettano senza problemi agli **AP** e che il roaming tra **AP** avvenga senza interruzioni, soprattutto se gli utenti si spostano da una zona all'altra. In questo modo, si può garantire una connessione stabile e continua per tutte le persone e i dispositivi connessi alla rete, assicurando che la rete wireless soddisfi le esigenze dell'intero ufficio. [Cis24b]

4. Installazione dei dispositivi e survey definitivo

L'installazione dei dispositivi di rete rappresenta un passaggio cruciale nella fase finale della progettazione e configurazione di un'infrastruttura di rete. Dopo aver configurato in modo dettagliato gli **switch**, il **WLC** e gli **AP**, la fase successiva è l'installazione fisica e la predisposizione degli spazi necessari per l'alloggiamento e la gestione dei dispositivi di rete. L'installazione in loco deve essere svolta con grande attenzione per garantire non solo il corretto funzionamento dei dispositivi, ma anche la sicurezza e l'accessibilità per eventuali interventi di manutenzione futura.

4.1 Installazione degli switch nei rack

La scelta dell'armadio rack è uno degli aspetti più rilevanti in questa fase. Un armadio rack adeguato è fondamentale per ospitare correttamente tutti i dispositivi, come **switch**, **router**, **WLC** e eventuali server o altri apparati di rete. Il rack deve essere scelto in base a diversi fattori, tra cui le dimensioni fisiche dei dispositivi, la capacità di supportare il peso, la ventilazione per evitare il surriscaldamento e la gestione efficiente dei cavi. È essenziale che l'armadio abbia spazio sufficiente per permettere un buon flusso d'aria, poiché la dissipazione del calore è cruciale per evitare il surriscaldamento dei dispositivi, che potrebbe compromettere le performance o causare guasti. Inoltre, il rack deve essere dotato di un sistema di gestione dei cavi, che permetta di organizzare in modo ordinato i cavi di rete e alimentazione, evitando ingombri che possano ostacolare l'accesso ai dispositivi o compromettere la sicurezza. La scelta di un armadio rack con opzioni di accesso frontale e posteriore facilita la manutenzione e l'espansione futura della rete, consentendo interventi rapidi senza la necessità di smontare l'intera configurazione. Una volta che tutti i dispositivi nuovi sono stati correttamente alloggiati nell'armadio rack, è necessario procedere con le ultime configurazioni **on-site**, che sono fondamentali per finalizzare l'installazione e garantire che tutto funzioni correttamente. Queste configurazioni includono il controllo finale della connettività tra i vari dispositivi, come gli **switch**, il **WLC**, e gli **AP**, e l'eventuale aggiustamento delle impostazioni di rete in base alle specifiche necessità del sito. Un passo fondamentale è anche il test di connettività, che deve essere eseguito tra gli **switch** e il **WLC**, verificando che la comunicazione tra i vari dispositivi della rete sia stabile e che tutte le interfacce siano correttamente configurate. Successivamente, si procede con l'attivazione e verifica del Wi-Fi, assicurandosi che gli **AP** siano correttamente registrati al **WLC** e che gli SSID siano associati come previsto. La qualità del segnale Wi-Fi viene misurata per garantire che le aree critiche, come le postazioni di lavoro o le sale comuni, siano coperte in modo ottimale. Infine, un'altra parte importante delle configurazioni **on-site** riguarda

il monitoraggio della rete e l'ottimizzazione del traffico. Questo include l'analisi delle prestazioni della rete wireless e cablata, per verificare eventuali colli di bottiglia e assicurarsi che i dispositivi connessi alla rete possano comunicare senza interruzioni. È essenziale anche controllare le impostazioni di sicurezza, come l'autenticazione degli utenti via **RADIUS** e i metodi di crittografia (**WPA2** o **WPA3**), per garantire che la rete sia protetta contro accessi non autorizzati. In questo processo, è fondamentale monitorare anche la gestione della banda e l'assegnazione delle risorse in base alle necessità aziendali, soprattutto se vengono utilizzati applicazioni critiche come la telefonia **VoIP** o videoconferenze, per le quali la qualità del servizio (**QoS**) deve essere configurata correttamente.

Figura 4.1: Sala CED

4.2 Cablaggio effettuato

In una rete aziendale o in un data center, il **cablaggio strutturato** è un elemento cruciale per garantire l'affidabilità, la velocità e la scalabilità delle comunicazioni. Questo cablaggio è progettato per gestire il traffico dati tra i vari componenti della rete, tra cui i rack di **core** e **edge**. Di seguito, descriverò in dettaglio il cablaggio effettuato per questi due rack, facendo riferimento a concetti come **bretelle**, **patch**, e le differenze tra **rame** e **fibra ottica**.

4.2.1 Rack core

Il rack del core rappresenta il **cuore pulsante della rete**, ovvero la **sezione centrale** dove vengono collocati i principali dispositivi che hanno il compito di **gestire, controllare e instradare il traffico di dati** verso le diverse sezioni della rete aziendale o infrastrutturale. All'interno di questo rack trovano posto **apparecchiature fondamentali** come **router, switch core, e firewall**, che lavorano sinergicamente per garantire una **trasmissione efficiente e sicura dei dati**. Il cablaggio presente in questa parte cruciale della rete è spesso realizzato in **fibra ottica**. Questa scelta non è casuale: la fibra ottica offre una **velocità di trasmissione dei dati estremamente elevata**, combinata con la capacità di **coprire lunghe distanze** senza degrado significativo del segnale. Inoltre, la **bassa latenza garantita** dalla fibra ottica è un

aspetto essenziale per la **gestione del traffico di rete a livello core**, dove ogni millisecondo può fare la differenza per mantenere **elevate prestazioni e affidabilità** dell'intera infrastruttura. Grazie a queste caratteristiche, il rack del core diventa un **punto strategico per il funzionamento della rete**, poiché da esso dipendono non solo la **velocità e la stabilità delle comunicazioni interne**, ma anche la **capacità di adattarsi rapidamente** alle crescenti esigenze di **traffico e connettività** delle organizzazioni moderne.

4.2.2 Rack edge

Il rack edge, a differenza del rack del core, si trova posizionato alla **"periferia" della rete**, in prossimità degli **utenti finali** o delle **connessioni locali**. Questo tipo di rack riveste un **ruolo cruciale** nel connettere i **dispositivi terminali** utilizzati quotidianamente, come **PC, telefoni VoIP e access point Wi-Fi**, agli **switch di edge** o ai **gateway**, che a loro volta instradano il traffico verso il core della rete. L'architettura del rack edge è progettata per **gestire efficacemente il traffico locale** generato dagli utenti e per garantire che le connessioni siano **stabili, sicure e performanti**. I dispositivi presenti in questo rack sono generalmente meno complessi rispetto a quelli del core, ma non meno importanti: tra questi figurano **switch di accesso**, **gateway** e talvolta **dispositivi di sicurezza** come firewall locali. Il cablaggio nel rack edge gioca un **ruolo fondamentale** e si adatta alle **esigenze specifiche di connettività**. Nella maggior parte dei casi, vengono utilizzati **cavi in rame** per la **connessione diretta degli utenti finali**, grazie alla loro **economicità e semplicità di installazione**, che li rende ideali per **collegamenti su brevi distanze**. Tuttavia, nelle situazioni in cui è necessario un **trasporto dati ad alta velocità** e su **distanze più lunghe**, come nel caso delle **connessioni di backhaul**, viene spesso impiegata la **fibra ottica**. Grazie a questa configurazione, il rack edge non solo assicura una **connettività ottimale per gli utenti finali**, ma funge anche da **ponte fondamentale tra la periferia e il core della rete**. Questo **ruolo intermedio** lo rende un elemento strategico per garantire che i **dati prodotti a livello locale** possano essere instradati in modo **efficiente** verso le **risorse centrali**, senza compromessi in termini di **velocità, latenza o affidabilità**.

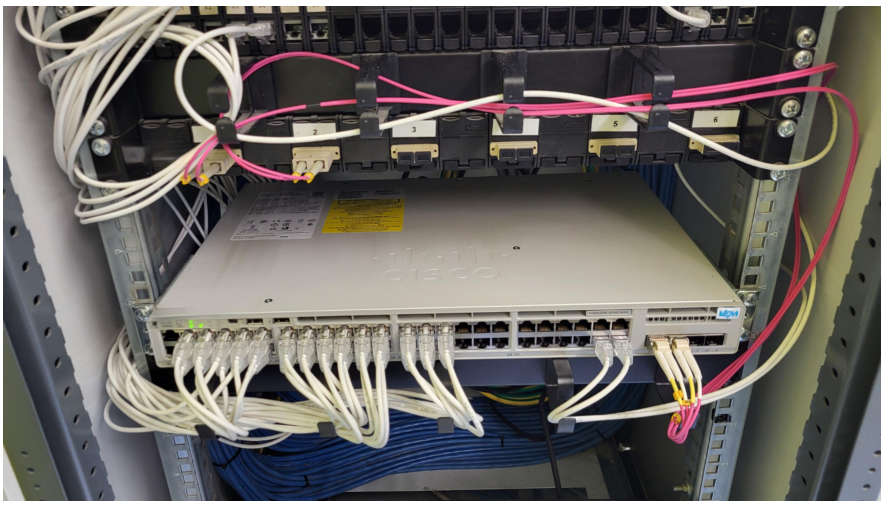

Figura 4.2: Sala ufficio

4.2.3 Bretella di rete e patch di rete

Una **bretella** è un tipo di cavo utilizzato per connettere due dispositivi simili tra loro, come due **switch** o due **server**, senza la necessità di un intermediario come un **router**. A differenza di un cavo di rete standard, la bretella è progettata per incrociare i segnali in modo che i pin **trasmissione** di un dispositivo siano connessi ai pin di **ricezione** dell'altro. Ad esempio, un cavo **crossover** (bretella) è usato quando si collega direttamente un dispositivo di rete a un altro senza passare per un **hub** o uno **switch**. Tuttavia, nella maggior parte delle configurazioni moderne, gli **switch** supportano la **Auto-MDI/MDIX**, che permette loro di "adattarsi" automaticamente al tipo di cavo (normalmente, o bretella o patch). Un **cavo patch** è un cavo più corto utilizzato per fare connessioni temporanee o permanenti tra dispositivi all'interno di un **rack** o tra il pannello di distribuzione (**patch panel**) e il dispositivo di rete (**switch**, **router**, **server**). A differenza della bretella, il cavo patch è solitamente un cavo **diritto** (con i fili connessi in modo uniforme su entrambe le estremità) e viene usato per connettere apparati che necessitano di una comunicazione standard tra loro. I **cavi patch** sono utilizzati per collegare il **pannello patch** (che centralizza tutte le connessioni di rete) agli **switch**, e successivamente a dispositivi come **server** o **access point**. [Opt23]

4.2.4 Rame vs fibra ottica: caratteristiche e differenze

Il **rame** è particolarmente utilizzato per cavi **twisted pair** (come i cavi **Cat5e**, **Cat6**, **Cat6a**), dove i fili di rame sono intrecciati per ridurre le interferenze elettromagnetiche. Questo tipo di cablaggio è comunemente impiegato per **reti locali** (LAN) e altre applicazioni di comunicazione dati, grazie alla sua semplicità e al costo relativamente basso rispetto ad altre tecnologie come la **fibra ottica**. Un aspetto importante del rame è che, nonostante le sue buone caratteristiche di conduzione, è soggetto a **interferenze elettromagnetiche** (EMI), che possono compromettere la qualità del segnale. Inoltre, la distanza massima che un segnale può percorrere attraverso il cavo in rame prima di degradarsi è limitata: generalmente, il rame è efficace su distanze fino a 100 metri. Oltre questa distanza, è necessario usare **ripetitori** per amplificare il segnale. La **fibra ottica** è invece una tecnologia di trasmissione dati che utilizza fibra di vetro o fibra plastica per trasmettere segnali sotto forma di **luce**. È costituita da un **nucleo** di vetro o plastica, che è circondato da uno strato di materiale riflettente chiamato **cladding**, che aiuta a mantenere la luce all'interno del nucleo, impedendo che fuoriesca e garantendo la trasmissione del segnale su lunghe distanze. La luce che viaggia lungo il nucleo della fibra trasporta il segnale, anziché il flusso di elettricità come nel caso del rame. Una delle principali caratteristiche della fibra ottica è la sua capacità di trasmettere dati su distanze molto più lunghe rispetto al rame, senza subire degrado significativo del segnale. Infatti, le **fibre ottiche** possono trasmettere dati su decine o centinaia di chilometri senza la necessità di ripetitori, mentre i cavi in rame, come detto, sono limitati a circa 100 metri. Inoltre, la fibra ottica ha una **larghezza di banda** significativamente più alta rispetto al rame, il che significa che può supportare velocità di trasmissione molto più elevate, ideali per applicazioni ad alta richiesta di dati, come i **data center**, le **reti a banda larga** e la trasmissione **video**. La fibra ottica è anche immune dalle **interferenze elettromagnetiche** (EMI), una delle principali limitazioni del rame. Questo la rende ideale per ambienti in cui sono presenti forti interferenze o per applicazioni che richiedono alta **affidabilità**, come le **telecomunicazioni** e la trasmissione di dati **critici**. Nonostante i numerosi vantaggi,

la fibra ottica ha anche alcune limitazioni. In primo luogo, è più costosa sia in termini di materiale che di installazione rispetto al rame. La fibra è anche più fragile e richiede una maggiore attenzione durante l'installazione e la manutenzione. Inoltre, l'installazione della fibra ottica richiede attrezzature specializzate per il **taglio**, la **fusione** e il **collegamento** dei cavi. [Ami24]

4.2.5 Tipologie di fibra ottica e le loro caratteristiche

Per comprendere al meglio la **fibra ottica** e le difficoltà poste durante l'installazione, bisogna anche fare alcune delucidazioni in merito alle varie **tipologie di fibra ottica** esistenti. [Edg24]

- **Monomodale**: La **fibra ottica monomodale** è una tipologia di fibra progettata per trasmettere segnali luminosi lungo un **singolo percorso** o **modalità**. Questo consente alla luce di viaggiare in modo più diretto, riducendo le **distorsioni** e la **dispersione del segnale**, il che la rende ideale per le **comunicazioni su lunga distanza ad alta velocità**. Una delle caratteristiche distintive della fibra monomodale è il suo **nucleo molto piccolo**, che di solito ha un diametro compreso tra **8 e 10 micrometri**, molto più ridotto rispetto alla fibra multimodale. A causa di questa ridotta dimensione, la fibra monomodale consente solo un **singolo percorso per la luce**, mentre la fibra multimodale permette a più percorsi di luce di viaggiare attraverso il nucleo. La riduzione dei percorsi di luce significa che il **segnale rimane coerente nel suo viaggio**, evitando interferenze che potrebbero danneggiare la qualità del segnale, fenomeno che invece si verifica più frequentemente nelle fibre multimodali.

- **OM1**: La **fibra OM1** è la più vecchia tra quelle multimodali ed è caratterizzata da un **nucleo con un diametro di 62,5 micrometri**. È in grado di supportare velocità fino a **1 Gbps** su distanze relativamente brevi, circa **275 metri** per trasmissioni a **850 nm**. Sebbene OM1 sia stata utilizzata in molte **reti locali (LAN)** e per altre applicazioni a bassa velocità, oggi è considerata obsoleta per le esigenze moderne di rete, sostituita da fibre con prestazioni superiori come OM3 e OM4.

- **OM2**: La **fibra OM2**, con un nucleo di **50 micrometri**, è un'evoluzione di OM1 e consente velocità di trasmissione fino a **1 Gbps** su distanze fino a **550 metri**, sempre a **850 nm**. OM2 è stata una scelta popolare per le **reti aziendali** e le applicazioni di comunicazione più tradizionali, ma anche questa tecnologia è meno usata oggi, a favore di fibre con maggiore capacità di banda e distanza come OM3 e OM4.

- **OM3**: La **fibra OM3** ha un nucleo di **50 micrometri** come OM2, ma è progettata per supportare velocità di trasmissione molto più elevate, fino a **10 Gbps**. A **850 nm**, OM3 può coprire distanze fino a **300 metri**, ed è ottimizzata per applicazioni ad alta velocità come i **data center** e le **reti ad alta larghezza di banda**. La fibra OM3 è ideale per ambienti che richiedono prestazioni superiori ma su distanze non troppo lunghe.

- **OM4**: La **fibra OM4**, anch'essa con un nucleo di **50 micrometri**, rappresenta la versione più avanzata e ad alte prestazioni tra le fibre multimodali. OM4 offre una **larghezza di banda superiore** rispetto a OM3, permettendo velocità fino

a **10 Gbps** su distanze di **550 metri**. È progettata per applicazioni ad altissima velocità come le connessioni a **40 Gbps** e **100 Gbps** e per supportare le esigenze delle **reti moderne** e dei **data center di nuova generazione**. OM4 è la scelta ideale per ambienti dove è richiesta una capacità di trasmissione molto alta su lunghe distanze.

Tutto quanto descritto finora sui vari tipi di fibra ottica è stato necessario per spiegare il contesto in cui si colloca la **fibra OM2** utilizzata dal cliente. La fibra **OM2**, pur essendo stata una scelta valida in passato, oggi è considerata ormai datata rispetto alle moderne esigenze di rete, che richiedono prestazioni superiori in termini di velocità di trasmissione e capacità di banda . Di seguito, verranno anche riportati alcuni log per comprendere al meglio le problematiche avute. la spiegazione sarà possibile trovarla al sottocapitolo 5.3.4:

```
Nov  6 18:34:56 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low alarm; Operating value: -21.15 dBm, Threshold value: -21.04 dBm.
Nov  6 18:44:57 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -21.04 dBm, Threshold value: -17.03 dBm.
Nov  6 18:54:57 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.67 dBm, Threshold value: -17.03 dBm.
Nov  6 19:04:58 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.88 dBm, Threshold value: -17.03 dBm.
Nov  6 19:14:59 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.67 dBm, Threshold value: -17.03 dBm.
Nov  6 19:24:59 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.88 dBm, Threshold value: -17.03 dBm.
Nov  6 19:35:00 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.99 dBm, Threshold value: -17.03 dBm.
Nov  6 19:45:00 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.88 dBm, Threshold value: -17.03 dBm.
Nov  6 19:55:01 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.88 dBm, Threshold value: -17.03 dBm.
Nov  6 20:05:02 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -21.04 dBm, Threshold value: -17.03 dBm.
Nov  6 20:15:02 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.83 dBm, Threshold value: -17.03 dBm.
Nov  6 20:25:03 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low alarm; Operating value: -21.21 dBm, Threshold value: -21.04 dBm.
Nov  6 20:35:03 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.78 dBm, Threshold value: -17.03 dBm.
Nov  6 20:45:04 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -21.04 dBm, Threshold value: -17.03 dBm.
Nov  6 20:55:04 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low alarm; Operating value: -21.33 dBm, Threshold value: -21.04 dBm.
Nov  6 21:05:05 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low alarm; Operating value: -21.33 dBm, Threshold value: -21.04 dBm.
Nov  6 21:15:06 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.93 dBm, Threshold value: -17.03 dBm.
Nov  6 21:25:06 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.88 dBm, Threshold value: -17.03 dBm.
Nov  6 21:35:07 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.78 dBm, Threshold value: -17.03 dBm.
Nov  6 21:45:08 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.88 dBm, Threshold value: -17.03 dBm.
Nov  6 21:55:08 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.78 dBm, Threshold value: -17.03 dBm.
Nov  6 22:05:09 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.67 dBm, Threshold value: -17.03 dBm.
Nov  6 22:15:09 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Twe2/0/6: Rx power low warning; Operating value: -20.78 dBm, Threshold value: -17.03 dBm.
```

Figura 4.3: Log switch core

```
Nov  6 10:10:23 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.23 dBm, Threshold value: -17.03 dBm.
Nov  6 10:20:24 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.17 dBm, Threshold value: -17.03 dBm.
Nov  6 10:30:24 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -17.84 dBm, Threshold value: -17.03 dBm.
Nov  6 10:40:24 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.23 dBm, Threshold value: -17.03 dBm.
Nov  6 10:50:25 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.06 dBm, Threshold value: -17.03 dBm.
Nov  6 11:00:25 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -17.84 dBm, Threshold value: -17.03 dBm.
Nov  6 11:10:25 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.28 dBm, Threshold value: -17.03 dBm.
Nov  6 11:20:26 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.11 dBm, Threshold value: -17.03 dBm.
Nov  6 11:30:26 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -17.89 dBm, Threshold value: -17.03 dBm.
Nov  6 11:40:26 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.28 dBm, Threshold value: -17.03 dBm.
Nov  6 11:50:27 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.03 dBm, Threshold value: -17.03 dBm.
Nov  6 12:00:27 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.11 dBm, Threshold value: -17.03 dBm.
Nov  6 12:10:27 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.28 dBm, Threshold value: -17.03 dBm.
Nov  6 12:20:28 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -17.89 dBm, Threshold value: -17.03 dBm.
Nov  6 12:30:28 MEST: %SFF8472-3-THRESHOLD_VIOLATION: Te1/1/1: Rx power low warning; Operating value: -18.23 dBm, Threshold value: -17.03 dBm.
```

Figura 4.4: Log switch MAG

4.3 Problematiche riscontrate durante la fase di installazione

Durante la fase finale di testing delle modifiche apportate alla struttura della rete, è importante considerare che, nonostante una pianificazione accurata e l'implementazio-

ne delle migliori pratiche, potrebbero comunque emergere problematiche impreviste. Queste possono derivare da vari fattori, come **errori nei cablaggi**, **configurazioni errate** o **incompatibilità hardware**, che potrebbero ostacolare il corretto funzionamento della rete o impedire l'esecuzione dei test con successo. Anche in un ambiente controllato, in cui si è cercato di minimizzare i rischi, è sempre possibile che si verifichino **inconvenienti** che richiedano un'attenta analisi e risoluzione. Pertanto, è fondamentale mantenere un approccio **flessibile** e una pronta disponibilità ad affrontare qualsiasi difficoltà possa emergere durante questa fase cruciale di **validazione e ottimizzazione della rete**.

4.3.1 Verifica e diagnosi dei cavi di rete con tester ethernet: Fluke

Un esempio tipico di problema, potrebbe essere un **cablaggio eseguito in maniera errata dal cliente**, il quale impediva il passaggio del test effettuato tramite il tester **"Fluke"**. Il tester **Fluke per cavi Ethernet** è uno strumento progettato per verificare l'integrità e le prestazioni dei cavi di rete, in particolare quelli utilizzati per le connessioni Ethernet, come i cavi **Cat 5e, Cat 6 e Cat 6a**. Questi tester sono essenziali per garantire che i cablaggi di rete siano correttamente installati e funzionino in modo ottimale, senza interruzioni o degradi delle prestazioni che potrebbero influire sulla trasmissione dei dati. Il tester **Fluke per cavi Ethernet** funziona principalmente per eseguire due tipi di test fondamentali: il **test di continuità** e il **test delle prestazioni**. Il **test di continuità** verifica che ogni filo all'interno del cavo sia correttamente connesso da un'estremità all'altra, senza interruzioni o cortocircuiti. Questo è fondamentale per garantire che i segnali elettrici possano viaggiare correttamente attraverso il cavo, senza subire perdite o distorsioni. Oltre alla continuità, un tester **Fluke per cavi Ethernet** esegue anche una verifica della **mappatura del cablaggio**, assicurando che i fili siano connessi correttamente secondo lo schema di cablaggio scelto, ad esempio **T568A o T568B**, che definiscono come i cavi devono essere ordinati e collegati alle estremità del connettore RJ45. Un errore di cablaggio in queste connessioni può compromettere gravemente le prestazioni della rete, causando **perdite di segnale, disconnessioni o addirittura l'impossibilità di stabilire una connessione di rete.** Inoltre, i tester avanzati **Fluke** offrono funzionalità di **misurazione della capacità di trasmissione del cavo**, eseguendo test che simulano il traffico di rete per determinare se il cavo è in grado di supportare la velocità di trasmissione desiderata, ad esempio **1 Gbps (Gigabit Ethernet)** o **10 Gbps (10 Gigabit Ethernet)**. Questo test si estende anche alla misura di **resistenza al cross-talk**, un fenomeno in cui i segnali di un filo influenzano i segnali di un altro filo adiacente, causando interferenze che riducono la qualità della comunicazione. Inoltre, i tester **Fluke** possono rilevare altre problematiche comuni come la **lunghezza del cavo** e le **perdite di segnale**, assicurandosi che il cavo non superi la lunghezza massima supportata dalle specifiche Ethernet, che per esempio è di **100 metri per le connessioni Gigabit**. Alcuni modelli avanzati di tester **Fluke** sono dotati anche di funzionalità che permettono di generare e diagnosticare **segnali di test**, simulando condizioni di rete reali per fornire un'analisi completa delle prestazioni del cavo in condizioni operative. Questo è particolarmente utile per chi si occupa di **installazioni complesse di reti cablate**, dove è cruciale verificare che il cablaggio sia pronto a sostenere il carico di traffico previsto senza incorrere in problemi di latenza o velocità. [Net24b]

4.3.2 Buffer overflow e limiti di velocità nella rete

Durante la fase finale di testing delle modifiche apportate alla rete, si sono verificati alcuni problemi legati al **buffer** e alla **velocità di trasmissione dei dati**. Il **buffer** è una memoria temporanea utilizzata per immagazzinare i pacchetti di dati mentre vengono trasferiti tra due dispositivi di rete. Se il **buffer** non è in grado di gestire correttamente il volume di traffico che passa attraverso la rete, si verificano **buffer overflow** o **latenza**, che possono rallentare significativamente il flusso dei dati. Questo problema può derivare da una **gestione inadeguata delle risorse di rete**, da un **cattivo dimensionamento dei buffer** stessi o da una **congestione delle porte di rete**. Durante la fase di testing delle modifiche alla rete, è emerso un problema significativo legato alla **velocità di trasmissione dei dati**. In particolare, uno degli **switch utilizzati**, diverso da quelli installati, ha avuto difficoltà nella **negoziazione della velocità delle porte**, stabilendo una connessione a **100Mb/s** anziché a **1Gb/s**, come previsto per quel collegamento. Questo problema di **negoziazione della porta** si verifica quando due dispositivi di rete cercano di stabilire la velocità di trasmissione ottimale tra di loro. Tuttavia, a causa di **limitazioni hardware** o **configurazioni non corrette**, uno dei dispositivi potrebbe non essere in grado di negoziare correttamente una velocità superiore, forzando la connessione a una velocità inferiore. Nel caso specifico, lo **switch HP** ha negoziato la velocità a **100Mb/s**, mentre il dispositivo **Cisco** dall'altro lato ha stabilito una velocità di **1Gb/s**, creando così un **disallineamento tra le due parti della connessione**. Questo tipo di problema ha un impatto diretto sulle **prestazioni della rete**, in quanto i dispositivi che comunicano a velocità differenti non riescono a sfruttare appieno la capacità della connessione. La **differenza di velocità** tra i due dispositivi riduce la banda disponibile, aumentando il rischio di **congestione** e di **colli di bottiglia nel traffico dati**. Inoltre, una connessione lenta come quella a **100Mb/s** non solo limita il **throughput**, ma può anche contribuire a **buffer overflow**, ossia un sovraccarico del buffer, che si verifica quando il traffico in ingresso supera la capacità del buffer stesso, causando la **perdita** o il **ritardo dei pacchetti**. Questo fenomeno può compromettere ulteriormente la **velocità di trasmissione** e la **stabilità della rete**, poiché i pacchetti persi o ritardati devono essere ritrasmessi, aggravando il traffico. [Rob23]

4.3.3 Configurazione errata delle policy di rete e DNS

Un altro problema riscontrato riguarda le **policy di rete**, che sono risultate non correttamente configurate. Le **policy** sono insieme di regole e configurazioni stabilite all'interno di un sistema, di una rete o di un'organizzazione per definire comportamenti specifici e determinare come le risorse vengono gestite o utilizzate. Nel caso delle reti e delle connessioni a Internet, le **policy possono includere regole** relative al controllo dell'accesso, la gestione del traffico, la sicurezza e altre configurazioni per garantire che i sistemi si comportino come previsto. Ad esempio, una **policy** potrebbe stabilire che tutte le richieste **DNS** di una rete aziendale debbano essere indirizzate a un **server DNS interno**, invece di utilizzare uno pubblico come quello di Google. Il **DNS** (Domain Name System) è un sistema che traduce i nomi di dominio in indirizzi IP, permettendo ai dispositivi di connettersi ai server web, ai servizi online e a molte altre risorse su Internet. È fondamentale per la navigazione nel web, poiché gli **utenti normalmente utilizzano nomi di dominio**, mentre i **computer e i server usano indirizzi IP** per identificare e connettersi tra loro. Senza il DNS, sarebbe necessario ricordare gli indirizzi IP di tutti i siti che si vogliono visitare. Il problema sembrava

derivare dal fatto che il sistema stava tentando di comunicare con un **DNS sbagliato**. Piuttosto che utilizzare un **server DNS interno**, che sarebbe stato in grado di risolvere i nomi di dominio e gli indirizzi IP specifici per la rete aziendale, il sistema cercava di utilizzare un **DNS pubblico**, in questo caso, il DNS di Google. I server **DNS pubblici** non sono configurati per **gestire correttamente i nomi interni della rete aziendale**, quindi la comunicazione non riusciva. Inoltre, se il traffico veniva indirizzato a un **DNS esterno** senza una **policy di routing adeguata**, la **connessione non riusciva a stabilirsi correttamente**, poiché non c'era il percorso corretto per raggiungere il DNS e risolvere i nomi interni. Un **DNS interno** è un server DNS che si trova all'interno di una rete aziendale o privata, ed è utilizzato per risolvere i nomi di dominio specifici per quella rete. Questo è utile, per esempio, per risolvere i nomi dei server aziendali o per gestire altre risorse interne che non sono accessibili pubblicamente. Se la rete è configurata per utilizzare un DNS pubblico, come quello di Google, invece di un DNS interno, non è possibile risolvere i nomi di dominio che appartengono alla rete privata. Un altro aspetto importante è la **policy di routing** che determina come il traffico viene instradato verso l'esterno. Se manca una **policy di routing adeguata**, il traffico che cerca di uscire dalla rete aziendale verso Internet potrebbe non trovare il percorso corretto, proprio come nel nostro caso, il traffico non poteva fluire verso l'esterno, vista la mancanza di questa **policy**.

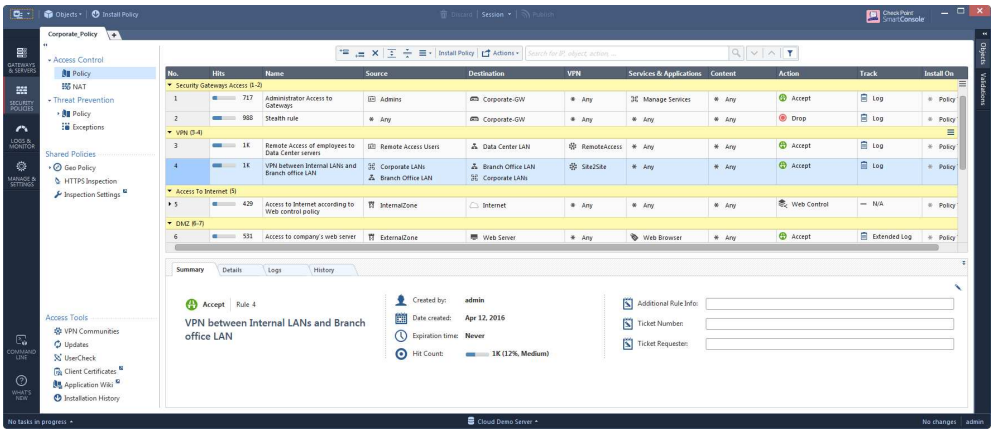

Figura 4.5: Intefaccia CheckPoint

4.3.4 Errore loopback ed error disable

Come ultima problematica, è stato affrontato il tema del **loopback**. Il termine **loopback detected**, ossia l'errore che è uscito dai log degli switch, fa riferimento a una condizione in cui i pacchetti di dati, inviati da un dispositivo di rete, ritornano sulla stessa interfaccia o porta da cui erano stati originariamente trasmessi, creando un loop o ciclo continuo. Questo tipo di situazione è problematico perché genera un traffico di rete ridondante che può **congestionare la rete**, ridurre la **qualità del servizio** e, nei casi più gravi, compromettere completamente il funzionamento della rete. Le cause di un loopback possono essere varie. Una delle principali è un **cablaggio errato**, dove, per esempio, un cavo collega una porta di uno switch alla stessa porta o a un'altra porta in modo da creare un percorso ciclico per i pacchetti. Un altro motivo potrebbe essere una **configurazione errata della rete**, come nel caso di VLAN o spanning tree mal configurati, che portano a percorsi ridondanti non controllati. In alcuni casi, il problema potrebbe anche derivare da un malfunzionamento hardware, ad esempio una porta

difettosa o un modulo che invia erroneamente pacchetti lungo un percorso imprevisto. Gli switch di rete moderni, in particolare quelli dei principali fornitori come Cisco, sono progettati per rilevare automaticamente i loopback. Quando uno switch rileva che i pacchetti inviati da una porta ritornano su di essa, attiva un allarme e segnala la presenza di un errore. Per prevenire che il loop influisca negativamente sull'intera rete, lo switch può disabilitare automaticamente la porta che ha generato il loop, mettendola in uno stato di **error-disable**. In questo modo, la rete non viene danneggiata da un ciclo infinito di pacchetti. [Cis10a] L'**error-disable** si riferisce alla modalità di protezione che uno switch attiva quando rileva un errore che potrebbe danneggiare la rete, come nel caso di un loopback. Quando un errore viene rilevato, lo switch **disabilita** automaticamente la porta coinvolta, impedendo che l'errore si propaghi ulteriormente e comprometta la rete. Una volta che il loop è stato corretto, o che l'errore che ha causato il blocco della porta è stato risolto, è necessario ripristinare la porta per riattivarla [Cis10b]. Il recupero da una condizione di error-disable può avvenire in due modi principali. Il primo è tramite un **intervento manuale** da parte dell'amministratore di rete, che può utilizzare i comandi appropriati per riabilitare la porta. Il secondo metodo prevede il **recupero automatico**, in cui lo switch, se configurato per farlo, tenterà di ripristinare la porta dopo un determinato periodo di tempo, a condizione che la causa dell'errore sia stata risolta. Questo comportamento può essere configurato attraverso il comando **errdisable recovery**, che consente di automatizzare il processo di recupero dopo che uno specifico tipo di errore è stato rilevato, come nel caso di un loopback.

4.4 Survey definitivo

Alla fine del processo di installazione della rete, è stato deciso di utilizzare 16 Access Point invece dei 17 inizialmente previsti. Inizialmente, il cliente aveva acquistato 18 AP, di cui uno destinato come dispositivo di riserva. La configurazione originaria prevedeva quindi l'installazione di 17 AP, ma grazie a una nuova valutazione effettuata a seguito di un'ulteriore diagnosi della rete, si è deciso di ridurre il numero di dispositivi installati a 16, questo perché avrebbero garantito una copertura adeguata, senza compromettere la qualità del segnale o le prestazioni complessive. In questo modo, il numero di AP di riserva è stato incrementato da 1 a 2, garantendo maggiore resilienza in caso di guasti o necessità future. La simulazione iniziale e la successiva verifica sul campo, utilizzando Ekahau, hanno permesso di evitare problemi comuni come l'installazione di dispositivi superflui o mal posizionati, riducendo il rischio di inefficienze nella copertura della rete. Nonostante la riduzione del numero di AP, la rete è risultata completamente performante, con una copertura omogenea in tutte le aree critiche e una capacità di gestire un numero crescente di dispositivi e traffico dati, come si potrà anche osservare dalle piantine sotto elencate:

`Mappatura senza correzioni`

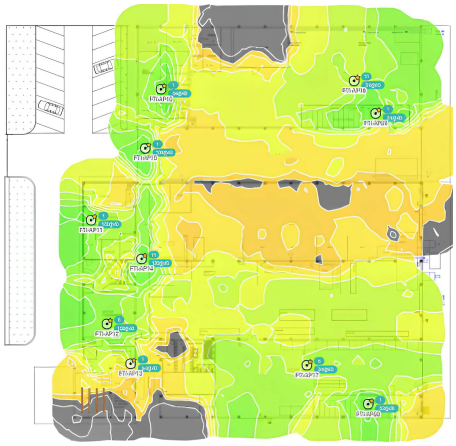

Figura 4.6: Piano terra

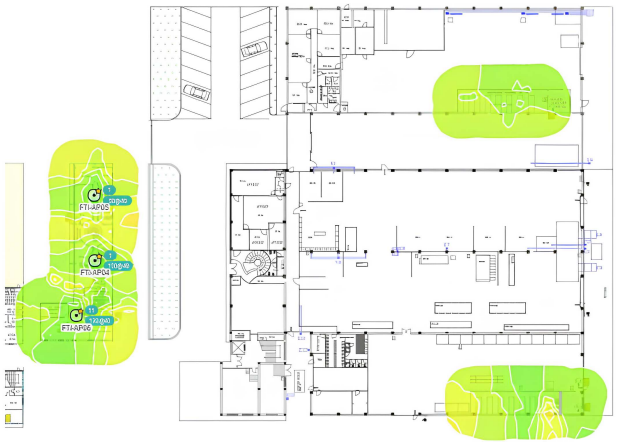

Figura 4.7: Primo piano

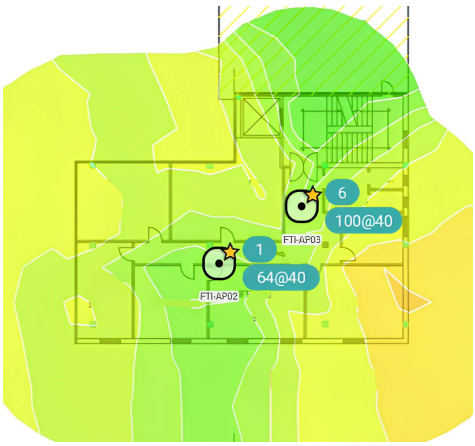

Figura 4.8: Secondo piano

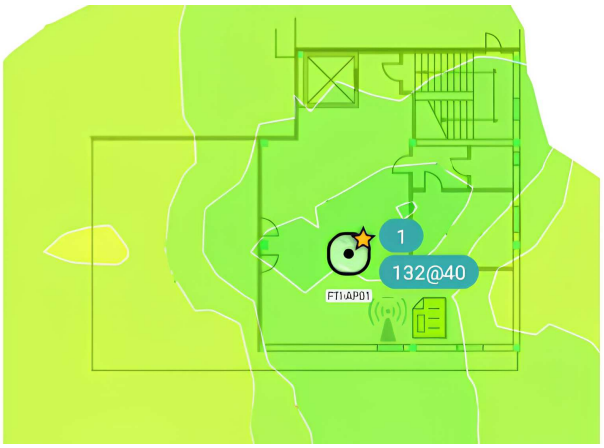

Figura 4.9: Terzo piano

`Mappatura con le correzioni`

Figura 4.10: Piano terra - signal strength

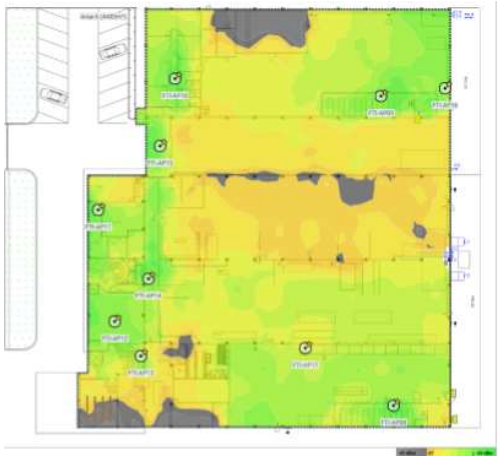

Figura 4.11: Piano terra - excluded areas

Figura 4.12: Primo piano - signal strength

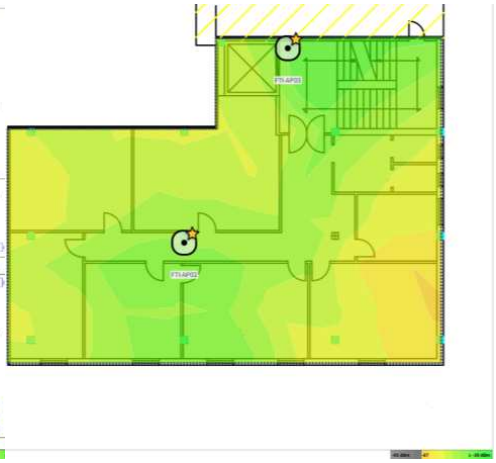

Figura 4.13: Secondo piano - signal strength

Figura 4.14: Terzo piano - signal strength

4.5 Rogue Access Point

Durante l'ultimo survey eseguito, oltre alla verifica delle necessità di copertura e ottimizzazione della rete, è emersa un'importante problematica: la presenza di rogue Access Point all'interno dell'ambiente del cliente. Questi AP non erano stati installati come parte del nuovo progetto di rete, ma appartenevano a vecchi dispositivi precedentemente utilizzati dal cliente. La loro presenza potrebbe rappresentare una minaccia per la sicurezza e l'affidabilità della rete, poiché tali dispositivi non erano più gestiti correttamente e potevano causare interferenze o vulnerabilità. Un Rogue Access Point è un dispositivo illegittimo che si connette a una rete Wi-Fi, di solito configurato da un malintenzionato per estendere il segnale wireless e inserirsi in modo fraudolento in una rete protetta. Questo tipo di attacco viene considerato una variante del Man-in-the-Middle, dove l'attaccante si inserisce tra due parti che intendono comunicare tra loro, facendosi passare per un punto di accesso legittimo. In pratica, un Rogue AP agisce come un punto di accesso non autorizzato, ma che sembra legittimo agli utenti, che si connettono inconsapevolmente. Questi dispositivi non solo compromettono la sicurezza della rete, ma possono anche rubare credenziali di accesso, intercettare il traffico di rete o iniettare malware nei dispositivi connessi. L'attaccante può configurare un Rogue AP con un SSID simile o uguale a quello della rete legittima, ingannando gli utenti che si connettono al punto di accesso errato. Questo tipo di attacco permette all'hacker di intercettare il traffico dati degli utenti o addirittura di rubare informazioni sensibili, come credenziali di login e dati bancari. Un attacco di tipo Rogue AP sfrutta la fiducia degli utenti nei punti di accesso pubblici o aziendali. Ad esempio, in ambienti come aeroporti, ristoranti o hotel, un malintenzionato può creare un AP con un nome molto simile a quello di una rete Wi-Fi legittima, ingannando gli utenti che si connettono involontariamente al dispositivo compromesso. Questa tecnica è conosciuta anche come attacco Evil Twin. Sebbene il termine Rogue AP e Evil Twin vengano spesso usati in modo intercambiabile, esistono alcune differenze tra i due attacchi. Un Rogue AP è solitamente configurato per agire come una rete Wi-Fi separata, ma comunque simile alla rete legittima. L'attaccante può creare un SSID simile, cercando di attirare gli utenti a connettersi al suo dispositivo. Un Evil Twin, d'altra parte, è una versione più sofisticata di un Rogue AP, poiché l'attaccante crea un punto di accesso identico a quello originale, con lo stesso SSID, crittografia di sicurezza e, a volte, anche le stesse credenziali. Questo rende molto più difficile per l'utente distinguere tra la rete legittima e quella fraudolenta, aumentando le probabilità che gli utenti si connettano erroneamente al dispositivo compromesso. L'Evil Twin è quindi un attacco più mirato e dannoso, poiché può raccogliere credenziali di accesso in tempo reale. [Inf24a]

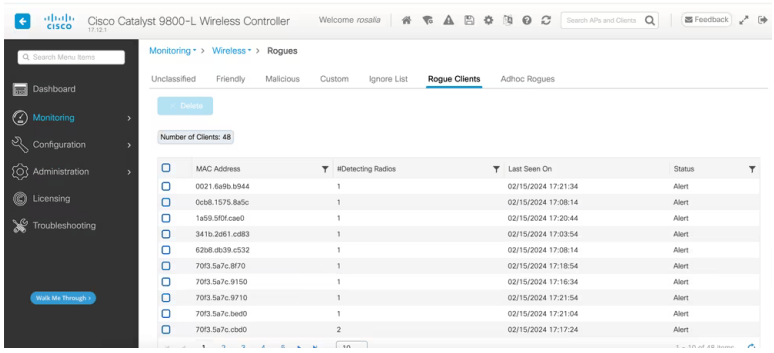

Figura 4.15: Tabella Rogue clients

5. Conclusioni e sviluppi futuri

Il progetto di aggiornamento e ottimizzazione dell'infrastruttura di rete presentato in questa tesi rappresenta un passo significativo verso la modernizzazione di un sistema aziendale critico. Attraverso un'**analisi dettagliata** dell'architettura esistente, sono state identificate le principali **limitazioni**, che includevano non solo l'**obsolescenza di alcuni dispositivi** e **problemi di scalabilità**, ma anche la **mancanza di supporto per tecnologie moderne** quali **Wi-Fi 6** e il **controllo centralizzato avanzato**. L'intervento ha portato a una **trasformazione profonda** del sistema, rispondendo a necessità immediate e creando le basi per una futura evoluzione tecnologica.

L'implementazione della nuova infrastruttura è stata guidata dalla scelta di **soluzioni di ultima generazione**, tra cui gli **switch Cisco 9300X e 9200L**, access point compatibili con **Wi-Fi 6** e un **Wireless LAN Controller 9800-CL**. Questi componenti, integrati in un **progetto sistematico e ben pianificato**, hanno permesso di conseguire risultati significativi, tra cui:

- **Incremento della capacità di banda e riduzione dei colli di bottiglia**: grazie all'utilizzo di tecnologie avanzate come **StackWise** e **Port Channel**, è stato possibile migliorare le **prestazioni complessive** della rete, garantendo maggiore fluidità nel traffico dati;

- **Copertura wireless omogenea e ad alte prestazioni**: l'ottimizzazione del posizionamento degli access point mediante strumenti avanzati come **Ekahau** ha garantito una **copertura capillare**, eliminando le **zone d'ombra** e migliorando l'esperienza degli utenti;

- **Sicurezza rafforzata**: l'adozione di **politiche di segmentazione della rete** e l'utilizzo di **firewall stateful** di nuova generazione hanno reso l'infrastruttura più **sicura**, riducendo il rischio di **accessi non autorizzati** e potenziali **minacce informatiche**;

- **Gestione centralizzata e scalabile**: l'introduzione di strumenti per la **gestione centralizzata** ha ridotto la **complessità operativa** per il team IT, migliorando l'**efficienza** nelle operazioni quotidiane e consentendo interventi più rapidi e mirati.

Questi risultati non solo soddisfano le **necessità immediate** del cliente, ma rappresentano un **elemento chiave** per la costruzione di un'**infrastruttura flessibile e resiliente**, capace di adattarsi alle esigenze tecnologiche e aziendali future. La scelta di **tecnologie scalabili e modulari** consente inoltre un'espansione progressiva senza compromettere le **prestazioni** o la **stabilità** del sistema.

5.1 Sviluppi futuri

Il percorso futuro include l'**adozione di tecnologie SDN (Software-Defined Networking)**, che migliorerebbero la **gestione** e la **sicurezza della rete** grazie a funzionalità come il **controllo basato su policy** e l'**automazione delle configurazioni**, semplificando **operazioni complesse** e riducendo **errori**. Si propone inoltre l'**estensione della copertura wireless** verso **aree produttive** e zone inizialmente escluse, garantendo maggiore **integrazione** tra ambienti operativi e amministrativi per una **connettività omogenea**. La **migrazione verso componenti cloud-native** appare un'opzione vantaggiosa per aumentare **elasticità** e **scalabilità**, con la prospettiva di ridurre i **costi infrastrutturali** a lungo termine senza sacrificare **affidabilità** e **sicurezza**.

Allo stesso tempo, l'**integrazione di tecnologie emergenti** come il **Wi-Fi 6** e il **Wi-Fi 6E** consentirebbe significativi miglioramenti in termini di **velocità**, **latenza** e **gestione del traffico**, rispondendo alle richieste di ambienti con **alta densità di dispositivi**. Per mantenere l'infrastruttura aggiornata e allineata agli **standard più recenti**, saranno necessari **audit regolari** e **aggiornamenti pianificati**, prevenendo **vulnerabilità** e assicurando **prestazioni ottimali**.

Infine, l'**uso di sistemi di analisi predittiva e automazione basati su intelligenza artificiale** potrebbe aggiungere valore, identificando **anomalie**, prevedendo **guasti** e ottimizzando **risorse in tempo reale** per migliorare ulteriormente **affidabilità** ed **efficienza**.

Bibliografia

[Ami24] Bolletta Amica. *Fibra Ottica vs Cavi in Rame: Un Confronto Dettagliato delle Prestazioni*. 2024. URL: https://bollettaamica.com/fibra-ottica-vs-cavi-in-rame-un-confronto-dettagliato-delle-prestazioni/.

[Cab23] CablesAndKits Learning Center. *Difference Between DAC and AOC Cables*. 2023. URL: https://www.cablesandkits.com/learning-center/difference-between-dac-and-aoc-cables.

[Cis10a] Cisco Community. *Detected a Loop Back; Port Has Been Disabled*. 2010. URL: https://community.cisco.com/t5/switching/detected-a-loop-back-port-has-been-disabled/td-p/1529469.

[Cis10b] Cisco Community. *PM-4-ERR_DISABLE : LoopbackErrorDetectedonGi0/2*. 2010. URL: https://community.cisco.com/t5/routing/pm-4-err-disable-loopback-error-detected-on-gi0-2/td-p/1432264.

[Cis24a] Cisco. *Cisco Spanning Tree Protocol*. 2024. URL: https://www.networkstraining.com/cisco-spanning-tree-protocol/.

[Cis24b] Cisco. *Wi-Fi Standards and Frequencies*. 2024. URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/intent-based-networking/solution-overview-c22-739047.html.

[Clo24] NetSec Cloud. *What is Storm Control? Understanding Network Traffic Management*. 2024. URL: https://netseccloud.com/what-is-storm-control-understanding-network-traffic-management.

[Cre22] Coding Creativo. *Tipi di reti*. 2022. URL: https://www.codingcreativo.it/tipi-di-reti/.

[Edg24] EdgeOptic. *Multimode Fiber Types*. 2024. URL: https://edgeoptic.com/kb_article/multimode-fiber-types/.

[Eka23] Ekahau. *Sidekick 2: Mastering the Industry-Standard Wi-Fi Site Survey Solution*. 2023. URL: https://www.ekahau.com/blog/sidekick-2-mastering-the-industry-standard-wi-fi-site-survey-solution/.

[Fora] Fortinet. *Proxy Firewall*. URL: https://www.fortinet.com/resources/cyberglossary/proxy-firewall.

[Forb] Fortinet. *Stateful vs. Stateless Firewall*. URL: https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall.

[IBM24] IBM. *Networking*. 2024. URL: https://www.ibm.com/it-it/topics/networking.

[Inf24a] Onorato Informatica. *Rogue Access Point: cosa sono e come proteggersi*. 2024. URL: https://www.onoratoinformatica.it/wi-fi-hacker-attack/rogue-access-point-che-cosa-sono/.

[Inf24b] Informaticabrutta. *VLAN: Vantaggi e realizzazione*. 2024. URL: https://informaticabrutta.it/vlan-vantaggi-realizzazione/index.html.

[ITi24] ITigic. *What are VLANs and how do they work?* 2024. URL: https://itigic.com/it/what-are-vlans-how-do-they-work-with-usage-examples/.

[Net24a] Netgear. *What is Wi-Fi 6E and How It Works*. 2024. URL: https://www.netgear.com/about/press-release/wi-fi-6e.

[Net24b] Fluke Networks. *LinkIQ 100 Network Cable Tester*. 2024. URL: https://www.fluke.com/en-us/product/network-cable-testers/copper/linkiq-100.

[Opt23] Ascent Optics. *Patch Cable vs Ethernet Crossover Cable*. 2023. URL: https://ascentoptics.com/blog/it/understanding-the-difference-patch-cable-vs-ethernet-crossover-cable/.

[Rob23] Robots.net. *What Is Network Switch Buffer?* 2023. URL: https://robots.net/internet-and-connectivity/wifi-and-ethernet/what-is-network-switch-buffer/.

[Tea24] Digital Teacher. *Reti informatiche: tipologia, topologia e componenti principali*. 2024. URL: https://www.digitalteacher.it/reti-informatiche-tipologia-topologia-e-componenti-principali/.