Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Informatica

Sistema di networking per una piccola e media impresa

Tesi di laurea triennale

Relatore

Prof. Claudio Palazzi

Laureando

Davide Sgrazzutti
Matricola
1127436

Anno Accademico 2023-2024

Sommario

Il presente documento descrive il lavoro svolto durante il periodo di stage, della durata di circa trecentoventi ore, dal laureando Davide Sgrazzutti presso l'azienda VEM Sistemi S.p.A. In questa tesi verranno presentati i principali compiti svolti nell'ambito delle reti di medie e piccole dimensioni.
In primo luogo era richiesto lo sviluppo di una rete in grado di gestire la quantità di traffico di una piccola e media impresa. Per fare questo lo studente ha svolto un periodo di studio delle tecnologie di networking più adatte e già consolidate nel mercato IT per trovare una soluzione efficace e duratura nel tempo a seconda delle esigenze che si sono presentate durante la progettazione della rete. Come ultimo obiettivo c'è stata la ricerca di una possibile integrazione con le nuove soluzioni che il mercato IT sta offrendo in questi anni nell'ambito networking.

Ringraziamenti

Innanzitutto, vorrei esprimere la mia gratitudine al Prof. Claudio Palazzi per avermi seguito e consigliato per la stesura della tesi.

Desidero ringraziare con affetto i miei genitori per il sostegno, il grande aiuto e per essermi stati vicini in ogni momento durante gli anni di studio.

Ho desiderio di ringraziare poi i miei amici per tutti i bellissimi anni passati insieme e le mille avventure vissute.

Padova, Aprile 2024 Davide Sgrazzutti

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

1.1 L'azienda

VEM Sistemi S.p.A. fornisce servizi e soluzioni in ambito ICT integrando le migliori tecnologie del settore con la propria pluriennale competenza. Intuire e prevedere l'andamento del mercato per anticipare le esigenze dei clienti sono aspetti della propria cultura aziendale. La visione olistica che caratterizza VEM permette di offrire servizi di integrazione di sistemi eterogenei, dal cloud all'automazione dell'edificio, dalla mobility al data center, dalla collaboration alla security, fino al Custom Application Development, per consentire di cogliere il meglio dalla tecnologia in completa sicurezza.

1.2 Prodotti e servizi

L'azienda è specializzata in soluzioni ICT che includono vari settori dell'informatica cercando di garantire sempre uno sviluppo e innovazione a tutte le soluzioni proposte. I prodotti offerti da Vem Sistemi sono rivolti a varie categorie di clienti che vanno da banche e assicurazioni, pubblica amministrazione, grandi medie o piccole imprese, aziende di moda e anche singoli professionisti.
Di seguito sono descritti i prodotti di vem:

- **Networking**: rete, wired o wireless, rappresenta un vero e proprio abilitatore che consente a persone, sistemi, servizi e processi di comunicare e lavorare in maniera sicura, resiliente e adattiva
- **Data center infrastructure**: dalla progettazione, alla costruzione alla manutenzione dell'intera infrastruttura data center, secondo i più importanti standard internazionali
- **Collaboration**: l'integrazione di presence information, web e video conferencing, Voip e messaggistica consente di collaborare in maniera facile, sicura e produttiva su qualunque device
- **Facility**: rendere gli edifici più intelligenti per migliorare la sicurezza e il comfort di chi li occupa e ottimizzarne l'efficienza energetica
- **Security & IT Governance**: al fianco delle aziende per gestire e mitigare i rischi informatici e tentativi di frode associati con l'IT

- **Distributed Cloud**: Elaborazione, rete, storage e virtualizzazione all'interno di un'architettura scalabile e modulare gestita come singolo sistema

Capitolo 2

Lo stage

2.1 Introduzione

Lo scopo dell'attività di stage è quello di analizzare, progettare e realizzare una soluzione di networking per una piccola e media impresa. La realizzazione di tale rete verrà prima simulata tramite un software e successivamente collaudata fisicamente tramite le apparecchiature fornite dall'azienda.
In questo periodo storico in cui ogni azienda accede con i propri dispositivi alla rete generando una elevata quantità di traffico avere una rete che permette di gestire un grande flusso di informazioni senza trovarsi davanti ad una congestione di dati risulta fondamentale. La rete che andrà a realizzare dovrà tenere conto anche dell'aumento del traffico dei prossimi anni garantendo una soluzione durevole nel tempo.

2.2 Panoramica del progetto

Le conoscenze apprese durante lo svolgimento dello stage consistono di progettare una soluzione che possa raggiungere gli obiettivi prefissati, oltre che a potenziare le competenze dello studente in ambito nell'ambito networking. Il progetto di stage è costituito principalmente da:

- Attività di design infrastruttura e dimensionamento/scelta apparati
- Attività di installazione e configurazione apparati di rete
- Attività di installazione e configurazione software di rete
- Attività di messa in sicurezza di una rete

Alla base di tutto ci saranno delle periferiche rappresentate generalmente da pc o anche da altri dispositivi collegati a determinati switch. A seconda dei casi studiati tramite l'azienda riguardanti medie o piccole imprese verranno valutate varie soluzioni di networking per trovare una soluzione che riesca a soddisfare le esigenze più comuni di varie reti, realizzando infine uno schema che possa racchiudere la soluzione migliore.

2.3 Obiettivi dello stage

2.3.1 Problemi riscontrati

Durante l'attività di stage sono state riscontrate alcune difficoltà e limitazioni tecnologiche che hanno richiesto più tempo del previsto per essere risolte. Le due problematiche principali riscontrate sono state le seguenti:

- Durante il periodo di progettazione c'era la necessità di testare la rete generando un alto volume di traffico e questo ha richiesto la ricerca di uno strumento utile a risolvere questo problema. Per risolvere il problema alla fine lo studente ha potuto installare la propria soluzione presso un cliente il quale possedeva una infrastruttura capace di generare alte quantità di traffico sotto la supervisione del tutor aziendale.

- L'installazione fisica degli apparati ha richiesto più tempo del previsto in quanto sono necessari numerosi step per preparae i dispositivi come l'installazione del sistema operativo dell'apparato e la sua configurazione.

2.3.2 Risultati ottenuti

Al termine dell'attività di stage la rete è stata collaudata con successo. Presso uno dei clienti di Vem sistemi sono stati installati i dispositivi selezionati durante la progettazione e controllato che tutti i dispositivi di rete avessero la configurazione e gli indirizzi ip stabiliti. Le configurazioni dei dispositivi sono state testate e collaudate più volte tramite i laboratori dell'azienda e dunque non ci sono state modifiche sostanziali da fare. Tuttavia dopo l'installazione delle periferiche c'e' stata necessità di un'attivita' di presidio per essere totalmente sicuri dell'operativita' della rete. In conclusione e' stata realizzata una rete testata e funzionante che ha soddisfatto a pieno le esigenze di design del cliente.

2.4 Altri Obiettivi

2.4.1 Obiettivo aziendale

L'obiettivo a fine stage è stato quello di realizzare una rete in grado di poter funzionare e perdurare nel tempo fornendo alte prestazioni per tutti gli utenti collegati alla rete. Le finalità sono le seguenti:

- Individuare i dispositivi utili a gestire un grande carico di dati

- Avere una soluzione che riesca anche ad essere riutilizzata in più contesti e durevole nel tempo

Per ogni cliente l'azienda ha sempre creato delle soluzioni personalizzate come giusto che sia ma in contesti molto simili alcune soluzioni possono risolvere problemi del tutto analoghi. Trovare una soluzione in grado di risolvere problemi identici in diversi contesti e avere una soluzione durevole nel tempo era un altro degli obiettivi aziendali di questo stage.

2.4.2 Obiettivo formativo

L'obiettivo formativo per il tirocinante è stato quello di acquisire solide nozioni di networking in modo da realizzare delle soluzioni per più tipi di aziende anche a livello enterprise e che siano durevoli nel tempo. Con la continua evoluzione delle reti e il crescere del traffico tale problema va oltre le difficoltà dello studente e le conoscenze acquisite in ambito networking saranno una base per quello che verrà appresso durante il periodo di lavoro.

2.4.3 Risultati attesi

Di seguito sono elencati gli obiettivi che devono essere conseguiti nel corso delle attività di stage. Questi obiettivi sono stati concordati di comune accordo tra il tutor aziendale e il tutor interno.

Obbligatorio	Apprendimento concetti networking con test in laboratorio
Obbligatorio	Conoscenza ecosistema Cisco
Obbligatorio	Analisi infrastrutture e configurazione apparati di rete
Obbligatorio	Attività di design infrastrutture e dimensionamento/scelta apparati
Obbligatorio	Attività di installazione, configurazione e troubleshooting
Obbligatorio	Attività di messa in sicurezza di una rete
Obbligatorio	Realizzazione di documentazione intero progetto
Desiderabile	Autonomia della gestione con il cliente per raccogliere nuove richieste
Opzionale	Sopralluoghi on site

Tabella 2.1: Obiettivi attività di stage.

Capitolo 3

Tecnologie di Networking

In questo capitolo saranno trattate le principali tecnologie di networking. Ogni tecnologia delle seguenti è stata prima studiata e analizzata per vedere se potesse essere compatibile ai fini dello stage.

3.1 Switch CISCO

Uno switch Cisco è un dispositivo di rete progettato per indirizzare e instradare il traffico di dati all'interno di una rete locale (LAN). È un componente fondamentale nelle reti aziendali e domestiche in quanto consente di collegare più dispositivi, come computer, stampanti, telefoni IP e altri dispositivi di rete, consentendo di comunicare tra loro.
Le principali funzioni di uno switch Cisco includono:

- **Instradamento dei pacchetti**: uno switch è in grado di determinare a quale porta inviare i pacchetti in base all'indirizzo MAC dei dispositivi collegati alle sue porte. Ciò consente di trasmettere dati solo al dispositivo di destinazione anziché inviarli a tutti i dispositivi nella rete, migliorando l'efficienza della rete.
- **Segmentazione della rete**: gli switch Cisco consentono di creare segmenti di rete separati (VLAN) per dividere logicamente la rete in gruppi di dispositivi. Questa segmentazione aiuta a migliorare la sicurezza e l'efficienza della rete, limitando la comunicazione tra dispositivi solo all'interno della stessa VLAN.
- **QoS (Quality of Service)**: supportano la gestione della qualità del servizio, che consente di assegnare priorità al traffico di dati critico, come il traffico VoIP o videoconferenze, per garantire una migliore esperienza utente.
- **Sicurezza della rete**: gli switch Cisco possono implementare funzioni di sicurezza avanzate, come il rilevamento delle intrusioni e il controllo degli accessi, per proteggere la rete da minacce esterne e interne.

- **Monitoraggio e gestione:** molti switch Cisco offrono funzionalità di monitoraggio e gestione centralizzata attraverso protocolli come SNMP (Simple Network Management Protocol) e interfacce web. Ciò consente agli amministratori di rete di monitorare le prestazioni della rete e apportare modifiche necessarie.

Cisco è uno dei principali produttori di dispositivi di rete e offre una vasta gamma di switch con diverse funzionalità e capacità per soddisfare le esigenze delle diverse reti. Gli switch Cisco sono ampiamente utilizzati in reti aziendali di varie dimensioni per garantire la connettività e la sicurezza dei dispositivi collegati. La scelta di utilizzare questo determinato vendor è dovuta anche alla pluriennale esperienza dell'azienda con questi specifici apparati.

3.2 VLAN

Una VLAN (Virtual Local Area Network) in un contesto Cisco è una rete virtuale creata all'interno di uno o più switch per separare logicamente dispositivi all'interno di una rete fisica. Questa tecnologia consente di suddividere una rete locale in segmenti logici, isolando gruppi di dispositivi in modo che possano comunicare solo tra loro, indipendentemente dalla loro posizione fisica nella rete. Le VLAN sono ampiamente utilizzate per migliorare la sicurezza, l'efficienza e la gestibilità delle reti.
Utilizzare la tecnologia VLAN è risultato molto utile per i seguenti motivi:

- **Segmentazione della rete**: le VLAN consentono di creare segmenti di rete logici in modo da separare i dispositivi. Ad esempio, è possibile creare una VLAN per i dipendenti, una per i visitatori e una per i dispositivi VoIP. Questa segmentazione contribuisce a ridurre il traffico in broadcast e migliora l'isolamento tra gruppi di dispositivi.

- **Sicurezza**: le VLAN permettono di isolare gruppi di dispositivi, impedendo loro di comunicare direttamente con dispositivi in altre VLAN. Questo aiuta a proteggere i dati sensibili e a limitare l'accesso non autorizzato alla rete.

- **Efficienza del traffico**: con l'uso di VLAN, il traffico di rete può essere instradato in modo più efficiente. Ad esempio, il traffico di una VLAN non deve essere trasmesso a dispositivi in VLAN diverse, riducendo il traffico inutile e migliorando le prestazioni della rete.

- **Gestibilità**: le VLAN semplificano la gestione della rete. È possibile assegnare facilmente dispositivi alle VLAN e applicare politiche di rete specifiche a ciascuna VLAN. Inoltre, la configurazione delle VLAN è spesso gestita attraverso interfacce di gestione web o protocolli di gestione di rete come SNMP.

- **Flessibilità**: Cisco offre switch con funzionalità avanzate di gestione delle VLAN. È possibile creare VLAN statiche o dinamiche, consentendo una maggiore flessibilità nella configurazione della rete.

Per configurare le VLAN su switch Cisco, è necessario accedere all'interfaccia di amministrazione del dispositivo (generalmente tramite SSH o Telnet) dove successivamente è possibile creare, modificare ed eliminare le VLAN e assegnargli porte specifiche.

3.3 Spanning Tree Protocol

Lo Spanning Tree Protocol (STP) è un protocollo di rete utilizzato per prevenire i loop di rete. L'obiettivo principale del protocollo STP è garantire che ci siano percorsi di comunicazione senza loop nelle reti Ethernet, impedendo così che il traffico porti alla saturazione o addirittura che blocchi la rete stessa. Il loop di rete si verifica quando ci sono collegamenti multipli tra i dispositivi di rete, come switch o bridge, e può portare a problemi di congestione e rallentamenti. Il protocollo STP funziona selezionando un singolo percorso logico senza loop all'interno della topologia di rete e disabilitando gli altri percorsi. Questo percorso viene chiamato "albero di copertura" o "albero di spanning," da cui deriva il nome "Spanning Tree Protocol." Il processo del Spanning Tree Protocol segue i seguenti passaggi:

- **Elezioni del bridge root**: inizialmente, tutti i dispositivi nella rete partecipano a elezioni per determinare quale dispositivo sarà il "bridge root". Il bridge root è il dispositivo di riferimento per l'intera rete e il punto di partenza per la creazione dell'albero di spanning.
- **Calcolo del costo del percorso**: ogni dispositivo calcola un "costo" per raggiungere il bridge root. Il costo dipende dalla latenza o dalla velocità della connessione. Questo aiuta a determinare il percorso più efficiente per raggiungere il bridge root.
- **Selezione del percorso migliore**: ogni dispositivo seleziona il percorso più economico per raggiungere il bridge root. Questo percorso diventa il percorso attivo.
- **Blocco delle porte**: tutti gli altri percorsi vengono disabilitati attraverso l'invio di pacchetti BPDU (Bridge Protocol Data Units) che notificano agli altri dispositivi della rete quali percorsi sono stati selezionati e quali sono stati bloccati. Questo impedisce la formazione di loop nella rete.
- **Monitoraggio dinamico**: monitora costantemente la topologia di rete e, se si verificano cambiamenti, come il fallimento di un collegamento o l'aggiunta di un nuovo dispositivo, il protocollo può ricalcolare il percorso più efficiente e apportare le modifiche necessarie.

Il protocollo STP è standardizzato secondo IEEE 802.1D e ha diverse varianti e miglioramenti, come RSTP (Rapid Spanning Tree Protocol) e MSTP (Multiple Spanning Tree Protocol), che sono più veloci e consentono la gestione di più alberi di spanning su diverse VLAN. L'obiettivo principale rimane comunque la prevenzione dei loop di rete e l'assicurazione di una rete Ethernet stabile e affidabile.

3.4 Cisco Stack Technology

Cisco Stack è una tecnologia che permette di collegare tra loro più dispositivi di rete, come degli switch, creando un singolo sistema logico e gestibile. Questo approccio consente una maggiore flessibilità nella progettazione delle reti e fornisce numerosi vantaggi in termini di prestazioni e affidabilità. Gli switch impiegati in uno stack Cisco condividono un'unica configurazione e operano come un'entità coesa, semplificando notevolmente la gestione delle reti complesse.

I vantaggi della tecnologia Cisco Stack si possono racchiudere in tre punti fondamentali:

- **Riduzione del carico di Lavoro amministrativo**: uno dei principali vantaggi offerti dalla tecnologia Cisco Stack è la semplificazione delle attività amministrative. Con un'unica interfaccia di gestione, gli amministratori di rete possono configurare e monitorare l'intero stack senza la necessità di affrontare singolarmente ogni dispositivo. Ciò riduce significativamente il tempo e lo sforzo necessari per mantenere e aggiornare la rete.

- **Aumento della scalabilità**: Cisco Stack consente un facile aumento della capacità della rete. Aggiungere un nuovo switch allo stack è un processo agevolato, e il sistema si adatta automaticamente all'espansione, garantendo una scalabilità senza intoppi. Questo è particolarmente vantaggioso per le aziende in crescita che necessitano di adattare la propria infrastruttura di rete alle nuove esigenze.

- **Miglioramento delle prestazioni**: l'architettura di Cisco Stack offre prestazioni avanzate attraverso la condivisione di risorse e la distribuzione intelligente del traffico. Gli switch nello stack operano come un unico punto di gestione del traffico, ottimizzando le prestazioni della rete e riducendo i possibili colli di bottiglia.

La configurazione di uno stack Cisco inizia con il collegamento fisico degli switch. Una volta stabilita la connessione, la configurazione logica è semplificata, poiché le impostazioni sono condivise automaticamente tra i dispositivi. Questo elimina la necessità di configurare manualmente ogni singolo switch. La manutenzione, come gli aggiornamenti del Firmware, può essere eseguita in modo centralizzato, riducendo al minimo l'impatto sulle operazioni aziendali. Sebbene la tecnologia Cisco Stack offra numerosi vantaggi, è importante considerare attentamente le esigenze specifiche dell'azienda prima di implementarla. La topologia della rete, la scala delle operazioni e altri fattori devono essere valutati per garantire una transizione senza intoppi e massimizzare i benefici della tecnologia Cisco Stack.

3.5 ACL

ACL, o Access Control List, è un insieme di regole che vengono utilizzate per controllare il flusso di traffico all'interno di una rete o di un dispositivo di rete, come uno switch, un router o un firewall. Le ACL definiscono quali pacchetti di dati sono autorizzati o negati a passare attraverso un dispositivo o a raggiungere una destinazione specifica sulla rete e sono utilizzate per implementare politiche di sicurezza, filtrare il traffico indesiderato o consentire l'accesso solo a determinate risorse di rete. Sono composte da regole o voci e ogni regola specifica un criterio basato su informazioni come l'indirizzo IP di origine o di destinazione, il numero di porta, il protocollo e altre informazioni pertinenti. Esistono due tipi principali di ACL:

- **ACL di tipo standard**: queste ACL si basano principalmente sull'indirizzo IP di origine e possono consentire o negare il traffico in base a tali indirizzi.

- **ACL di tipo esteso**: queste ACL considerano una gamma più ampia di criteri, come indirizzi IP di origine e destinazione, numeri di porta, protocolli, ecc. Sono più flessibili rispetto alle ACL di tipo standard.

Le regole in un ACL vengono valutate in sequenza dall'alto verso il basso. La prima regola che corrisponde al pacchetto determina il comportamento applicato a quel pacchetto. Se una regola corrisponde e permette il pacchetto, le regole successive non vengono valutate. Se una regola corrisponde e nega il pacchetto, le regole successive vengono ignorate. Ad esempio, è possibile consentire solo il traffico da una determinata sottorete o negare il traffico da una determinata origine. Nelle ACL, spesso vengono utilizzate maschere wildcard per definire intervalli di indirizzi IP o combinazioni di bit. Queste maschere consentono di definire regole più specifiche. Durante la fase di progettazione sono risulsate uno strumento fondamentale nella gestione delle reti, consentendo di controllare e filtrare il traffico in modo da garantire la sicurezza e l'efficienza della rete.

3.6 DHCP Server

Una delle caratteristiche più interessanti dei switch Cisco è la possibilità di utilizzare un server DHCP interno al dispositivo per l'assegnazione degli indirizzi IP alle periferiche della rete. La scelta di utilizzare un server interno piuttosto che uno esterno è dovuta al risparmio di una nuova macchina utilizzata solo per questo determinato compito.

3.6.1 Cos'e' e come funziona

Un server DHCP (Dynamic Host Configuration Protocol) è un dispositivo o un'applicazione software che fornisce la configurazione di rete dinamica ai dispositivi client in una rete, consentendo loro di ottenere automaticamente gli indirizzi IP, le informazioni sulla subnet, i gateway predefiniti, i server DNS e altre informazioni di configurazione necessarie per la comunicazione in rete. Il server DHCP funziona nel seguente modo :

- **Richiesta del client**: quando un dispositivo client, come un computer o un dispositivo mobile, si connette a una rete, cerca un server DHCP per ottenere le informazioni di configurazione di rete. Invia una richiesta DHCP (nota come DHCP discover) in modo broadcast sulla rete.
- **Risposta del server DHCP**: il server DHCP rileva la richiesta del client e risponde inviando un pacchetto di risposta DHCP (nota come DHCP offer) contenente le informazioni di configurazione, come l'indirizzo IP assegnato, la maschera di sottorete, il gateway predefinito e i server DNS.
- **Richiesta del client**: il client riceve l'offerta da uno o più server DHCP presenti nella rete e quindi invia una richiesta DHCP (DHCP request) per confermare l'accettazione dell'offerta da un server specifico.
- **Conferma del server DHCP**: il server DHCP selezionato dal client conferma la richiesta inviando una risposta DHCP (DHCP acknowledge). Il client quindi applica le informazioni di configurazione ricevute.

Il server DHCP è essenziale in reti in cui è richiesta una configurazione automatica dei dispositivi client, come in reti aziendali o nelle reti dei fornitori di servizi Internet (ISP). I vantaggi di utilizzare un server DHCP sono i seguenti:

- **Automazione**: semplifica notevolmente la configurazione dei dispositivi client, evitando la necessità di inserire manualmente le informazioni di rete.
- **Gestione centralizzata**: un server DHCP consente di gestire in modo centralizzato e dinamico l'assegnazione degli indirizzi IP e altre informazioni di rete. Questo facilita l'aggiornamento e la manutenzione della configurazione di rete.
- **Prevenzione di conflitti di indirizzi**: il server DHCP può monitorare gli indirizzi IP assegnati e garantire che non vengano assegnati duplicati, riducendo così i conflitti di indirizzi IP nella rete.
- **Risparmio di tempo**: semplifica notevolmente la configurazione iniziale e la gestione continua dei dispositivi nella rete, risparmiando tempo e sforzi amministrativi.

Alla fine un server DHCP risulta essere un componente chiave nella gestione delle reti e svolge un ruolo fondamentale nella configurazione automatica dei dispositivi client.

Capitolo 4

Progettazione della rete

Durante il periodo di stage lo studente ha potuto visionare diverse soluzioni che Vem Sistemi ha proposto nel tempo ai suoi clienti. In questo modo sono stati presi in considerazione alcuni dati che risultano molto importanti per costruire una soluzione che racchiuda gran parte se non tutte le esigenze network delle piccole e medie imprese che Vem ha soddisfatto nel tempo.

4.1 Dati raccolti

Si è visto che molto spesso ogni cliente possedeva più stabilimenti interni alla propria azienda con varie zone distinte per esigenze specifiche. I reparti che più frequentemente sono emersi visionando i clienti sono gli uffici direzionali , i reparti di produzione e infine i reparti logistici (magazzini).
Negli uffici troviamo in media:

- Impiegati generici 25 persone
- Ufficio Marketing 10 persone
- Ufficio IT 5 persone
- Predisposizione per il WiFi 4 punti di rete
- Punti di rete per la Videosorveglianza 3

In più negli uffici direzionali ogni impiegato oltre al proprio terminale disponeva anche di un proprio telefono e delle periferiche condivise da tutti come ad esempio le stampanti.

Nel reparto produzione troviamo in media:

- Macchine utensili 30 punti rete
- Computer di linea 10 punti rete
- Predisposizione per il Wifi 10 punti rete
- Punti di rete per la Videosorveglianza 12 punti rete
- Telefoni 10

Nel reparto magazzino troviamo in media:

- Computer di magazzino 5 punti rete
- Predisposizione per il WiFi 4 punti rete
- Punti di rete per la Videosorveglianza 10 punti rete
- Telefoni 5

Vengono riassunti nella tabella della seguente pagina

Nome gruppo	Punti rete necessari	Reparto di riferimento
Impiegati generici	25 + x	Uffici generici
Impiegati Marketing	10 + x	Uffici generici
Ufficio IT	5 + x	Uffici generici
Predisposizione per il WiFi negli uffici	4 + x	Uffici generici
Punti di rete per la Videosorveglianza negli uffici	3 + x	Uffici generici
Macchine utensili	30 + x	Reparto Produzione
Computer di linea	10 + x	Reparto Produzione
Predisposizione per il Wifi della produzione	10 + x	Reparto Produzione
Punti di rete per la Videosorveglianza della produzione	12 + x	Reparto Produzione
Telefoni 10 in produzione	10 + x	Reparto Produzione
Punti rete per i computer di magazzino	5 + x	Magazzino
Predisposizione per il WiFi in magazzino	4 + x	Magazzino
Videosorveglianza in magazzino	10 + x	Magazzino
Telefoni in magazzino	5 + x	Magazzino

Tabella 4.1: Divisione punti rete per reparto

x = numero variabile di terminali da collegare in rete che possono essere aggiunti in futuro

Reparto	Punti rete necessari
Uffici generici	47 + x
Reparto Produzione	72 + x
Magazzino	24 + x

Tabella 4.2: Divisione punti rete totale per reparto

Negli uffici generici non vengono conteggiati i telefoni in quanto è stata trovata una soluzione che permette di utilizzare uno stesso punto di rete per collegare un terminale come un computer insieme ad un telefono, ovviamente con due indirizzi ip diversi.

4.2 Calcolo quantità switch

Ogni cliente nel proprio futuro potrebbe prendere decisioni diverse perciò non si è grado con certezza di stabilire quante periferiche di rete verranno aggiunte in ogni reparto. Verranno presi i valori nella tabella della sezione precedente e utilizzati come valori minimi da soddisfare.

Reparto	Punti rete necessari	Switch necessari
Uffici generici	> 47	48p + 24p
Reparto Produzione	> 72	2 * 48p
Magazzino	> 24	48p

Tabella 4.3: Tabella calcolo switch necessari

Troviamo due tipologie di switch a 24 porte e a 48 porte. Per permettere che in futuro ci sia la possibilità di collegare più periferiche senza dover riprogettare una parte della rete vengono presi di solito gli switch a 48 porte. Nel caso degli uffici generici dove i punti rete necessari vengono già soddisfatti da uno switch di 48 porte si è deciso di affiancare uno switch a 24 porte.

4.3 La segmentazione delle rete tramite il subnetting

La segmentazione di una rete attraverso il subnetting è un processo mediante il quale una rete IP viene suddivisa in sottoreti più piccole, chiamate subnet. Questo approccio offre diversi vantaggi in termini di gestione, sicurezza e prestazioni. Il subnetting consente di separare il traffico di rete in gruppi più piccoli. Ciò può migliorare l'efficienza della rete, limitare la congestione del traffico e fornire una migliore gestione delle risorse. Le subnet possono essere considerate come "isole" di rete e limitando la comunicazione tra di loro è possibile ridurre il rischio di accessi non autorizzati o diffusione di minacce da una parte all'altra della rete. Suddividere una rete aiuta a gestire in modo più efficiente gli indirizzi IP. Ciascuna subnet avrà un proprio range di indirizzi, semplificando l'assegnazione e l'amministrazione degli indirizzi stessi. Ogni subnet rappresenta un dominio di broadcast separato ed inoltre segmentando la rete, si riduce l'ampiezza del dominio stesso, limitando la quantità di traffico trasmesso in ciascuna subnet. La segmentazione della rete può migliorare le prestazioni ed è subito evidente specialmente in reti di grandi dimensioni dove il traffico stesso è minimizzato. E' possibile implementare politiche di sicurezza specifiche per ciascuna subnet, ad esempio è possibile applicare filtri di sicurezza o regole di accesso in base alle esigenze specifiche di ciascuna area della rete. Questa tecnica semplifica la manutenzione e l'isolamento dei problemi. In caso di guasti o problemi in una subnet, la restante parte della rete può continuare a funzionare senza essere influenzata. Tutto questo rende facile gestire e adattarsi ad una crescita futura perché nuove subnet possono essere aggiunte senza dover riprogettare l'intera struttura di rete.

4.4 Costruzione della tabella di subnetting

Tenendo conto dei dati ricavati nella sezione 4.1 si è potuto costruire la tabella di subnetting per riuscire a ottenere un indirizzamento ip appropriato per ogni gruppo di utenti. Durante la costruzione della tabella si è scelto di raggruppare tutti i punti per la rete Wifi, per la sorveglianza e per i telefoni in determinati gruppi. Questo perché anche se essendo fisicamente in reparti diversi a livello logico di rete risulta più semplice raggrupparli e di conseguenza gestirli.

Nome gruppo	ID VLAN	ID RETE	Maschera di rete	Punti rete necessari	Indirizzi disponibili tramite subnetting
Impiegati generici	10	10.0.10.0	255.255.255.0	> 25	254
Impiegati Marketing	20	10.0.20.0	255.255.255.0	>10	254
Ufficio IT	30	10.0.30.0	255.255.255.0	> 5	254
Macchine utensili	40	10.0.40.0	255.255.255.0	> 30	254
Computer di linea	50	10.0.50.0	255.255.255.0	> 10	254
Punti di rete per il Wifi	60	10.0.60.0	255.255.255.0	> 5	254
Punti di rete per la videosorveglianza	70	10.0.70.0	255.255.255.0	> 18	254
Punti rete per i computer di magazzino	80	10.0.80.0	255.255.255.0	> 25	254
Punti rete per telefoni	90	10.0.90.0	255.255.255.0	> 55	254

Tabella 4.4: Tabella di subnetting

4.4.1 Maschera di rete

La subnet mask "255.255.255.0" può essere assegnata a qualsiasi indirizzo IP di qualsiasi classe. Gli ultimi 8 bit dell'indirizzo IP sono riservati per gli host, mentre i primi 24 bit sono riservati per la rete.
Poiché ci sono 8 bit riservati per gli host, ci sono $2^8 = 256$ indirizzi IP disponibili per gli host in quella subnet. Tuttavia, due indirizzi sono riservati per scopi speciali:

- L'indirizzo IP di rete (con tutti gli 8 bit degli host impostati a zero) è riservato e non può essere assegnato a un host. Ad esempio, se l'indirizzo di rete è "192.168.1.0", l'indirizzo "192.168.1.0" non può essere assegnato.
- L'indirizzo di broadcast (con tutti gli 8 bit degli host impostati a uno) è riservato. Ad esempio, se l'indirizzo di rete è "192.168.1.0", l'indirizzo di broadcast sarà "192.168.1.255".

Quindi, il numero effettivo di indirizzi IP disponibili per gli host è 256 - 2 = 254 nella subnet con la subnet mask "255.255.255.0".

4.4.2 Indirizzi IP privati

Il numero di PC o dispositivi che si possono collegare ad una rete dipende dalla classe di indirizzi IP privati che si sta utilizzando e dalla suddivisione della rete in sottoreti. Analizziamo le tre classi di ip privati disponibili:

- **Classe A privata (intervallo 10.0.0.0 - 10.255.255.255)**: Gli indirizzi della classe A offrono un'ampia gamma di indirizzi (circa 16 milioni). Si può collegare un grande numero di PC o dispositivi, rendendola adatta per organizzazioni molto estese.
- **Classe B privata (intervallo 172.16.0.0 - 172.31.255.255)**: La classe B privata fornisce meno indirizzi rispetto alla classe A, ma comunque un numero significativo (circa 1 milione di indirizzi). È adatta per reti di medie dimensioni.
- **Classe C privata (intervallo 192.168.0.0 - 192.168.255.255)**: La classe C privata offre il numero più limitato di indirizzi (circa 65.000). È spesso utilizzata per reti più piccole o per suddivisioni in sottoreti.

Tutte le classi soddisfacevano di gran lunga il numero necessario di indirizzi IP richiesti per ogni reparto. A questo punto si è pensato di utilizzare la classe A per pura comodità assegnando ad ogni gruppo di utenti un indirizzo IP che al suo interno contenga nel terzo ottetto lo stesso numero della VLAN che gli è stata assegnata. Ad esempio per il primo gruppo di utenti Impiegati generici è stata assegnata la VLAN 10 e di conseguenza si è pensato di assegnare i loro indirizzi all'interno del range 10.0.10.1-254 e la loro rete avrà come ID rete 10.0.10.0.

Per identificare la rete a cui appartiene un host ad esempio con l'indirizzo IP "10.0.10.154" insieme alla subnet mask "255.255.255.0", è possibile eseguire una semplice operazione di AND bit per bit tra l'indirizzo IP e la subnet mask. L'operazione di AND tra i bit di corrispondenti posizioni restituisce l'indirizzo di rete.

Indirizzo IP:	10.0.10.154	->	00001010.00000000.00001010.10011010
Subnet Mask:	255.255.255.0	->	11111111.11111111.11111111.00000000
			Ora eseguiamo l'operazione di AND bit per bit:
AND Result:	10.0.10.0	->	00001010.00000000.00001010.00000000

Tabella 4.5: Calcolo ID Rete host

4.5 Architettura di rete

Le reti informatiche possono essere classificate in diverse tipologie in base alle loro dimensioni, alla loro estensione geografica e alle loro funzioni. Le reti LAN (Local Area Network) coprono un'area limitata, come un edificio o un campus, e sono comunemente utilizzate per connettere dispositivi all'interno di un'organizzazione. Le reti MAN (Metropolitan Area Network) si estendono su un'area geografica più ampia, come una città, mentre le reti WAN (Wide Area Network) connettono dispositivi su distanze ancora più grandi, attraversando città, paesi o continenti. La scelta dell'architettura di rete dipende spesso dalle esigenze specifiche dell'organizzazione. La Tier 3 Architecture di Cisco è una soluzione avanzata che offre una rete altamente affidabile e scalabile. La Tier 3 Architecture prevede la presenza di router che gestiscono il traffico e instradano i dati tra le diverse reti. Cisco è rinomata per la qualità e l'affidabilità dei suoi prodotti di rete, e la Tier 3 Architecture offre un elevato livello di performance, sicurezza e flessibilità. L'implementazione di questa architettura consente un controllo più granulare del traffico di rete e fornisce un ambiente robusto per le comunicazioni aziendali su vasta scala.

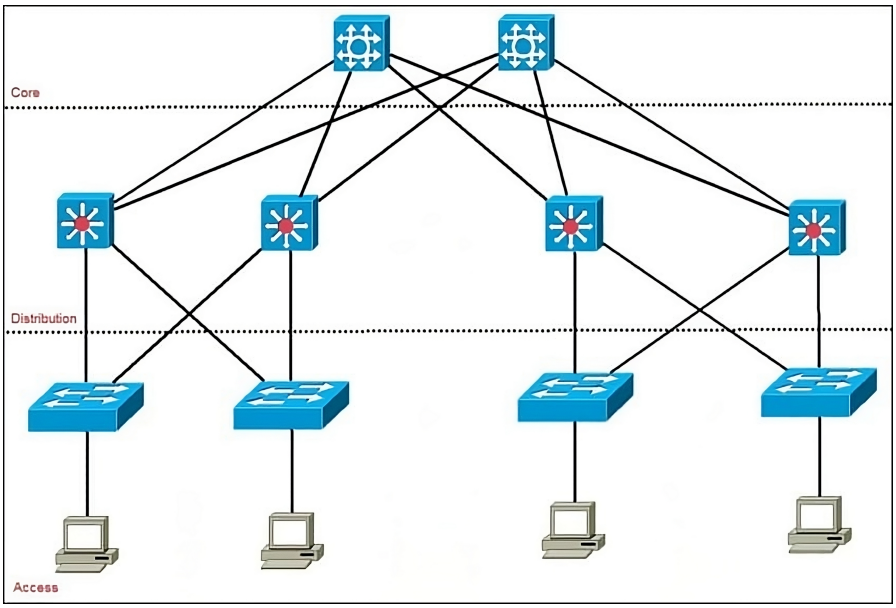

Figura 4.1: Cisco three-layer hierarchical model

4.5.1 Access Layer

L'Access Layer rappresenta la prima interfaccia tra gli utenti e i dispositivi finali con la rete. Questo strato è fondamentale per stabilire connessioni affidabili e gestire l'accesso alla rete. È il punto di ingresso dove utenti, come computer o dispositivi mobili, si collegano fisicamente alla rete attraverso switch di accesso e access point wireless. Nell'Access Layer, la priorità è fornire una connettività locale efficiente all'interno di una stessa rete, garantendo che gli utenti possano comunicare tra loro senza problemi. Questo strato gioca un ruolo cruciale nel suddividere il dominio di collisione e migliorare le prestazioni complessive della rete locale. Oltre alla semplice connettività, l'Access Layer gestisce la sicurezza dell'accesso. Include misure come l'autenticazione degli utenti, il controllo degli accessi basato su ruoli e la sicurezza fisica degli switch e degli access point. Queste caratteristiche sono fondamentali per proteggere la rete da accessi non autorizzati. Inoltre, con l'evoluzione delle reti, l'Access Layer può essere coinvolto nella creazione e gestione delle VLAN (Virtual Local Area Network), che suddividono la rete fisica in segmenti logici. Questa pratica favorisce la sicurezza, la gestione del traffico e la flessibilità nella progettazione della rete. Complessivamente, l'Access Layer è la porta d'ingresso che consente agli utenti di connettersi alla rete in modo sicuro ed efficiente, svolgendo un ruolo critico nel facilitare la comunicazione all'interno di un'organizzazione.

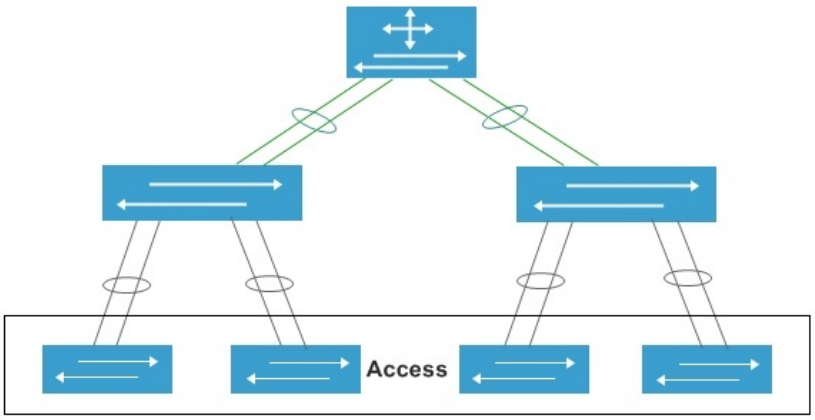

Figura 4.2: Access Layer

4.5.2 Distribution Layer

Il Distribution Layer, o strato di distribuzione, è una componente essenziale di un'architettura di rete. Questo strato agisce come intermediario tra l'Access Layer, dove gli utenti e i dispositivi finali si connettono alla rete, e il Core Layer, che gestisce il trasporto veloce del traffico attraverso la rete. Una delle principali funzioni del Distribution Layer è l'aggregazione del traffico proveniente dagli switch di accesso. Questo processo consente di semplificare la gestione del traffico e migliorare le prestazioni della rete all'interno dell'organizzazione. Oltre all'aggregazione del traffico, il Distribution Layer svolge un ruolo chiave nella sicurezza della rete. Implementa politiche di filtraggio del traffico e controlli di sicurezza per proteggere la rete da potenziali minacce e accessi non autorizzati. Il Distribution Layer contribuisce anche all'implementazione di politiche di Qualità del Servizio (QoS). Ciò significa che può garantire che il traffico critico, come voce o video, riceva la priorità necessaria sulla rete per garantire una qualità adeguata del servizio. Un aspetto cruciale del Distribution Layer è la creazione di una rete scalabile e ridondante. Ciò significa che, in caso di guasto, sono presenti percorsi alternativi per instradare il traffico, garantendo un'elevata disponibilità del servizio.

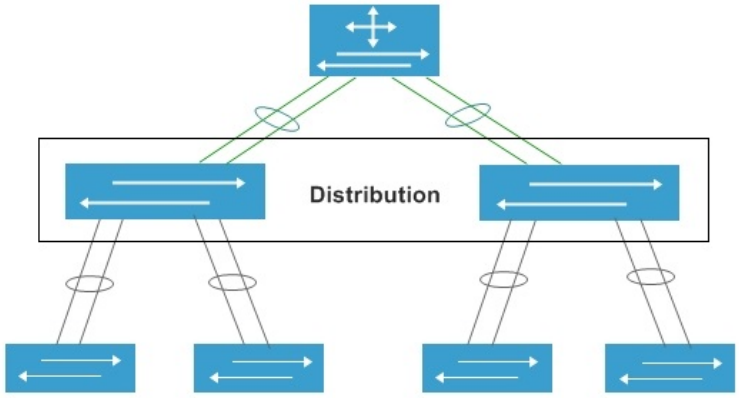

Figura 4.3: Distribution Layer

4.5.3 Core Layer

Il Core Layer rappresenta il cuore pulsante della Tier 3 Architecture. Questo strato è progettato per facilitare il trasporto rapido ed efficiente del traffico attraverso la rete. La sua funzione primaria è di fornire un elevato livello di larghezza di banda e velocità, garantendo che i dati possano fluire senza ostacoli tra i vari dispositivi e i segmenti della rete. Al contrario degli strati di Access e Distribution, il Core Layer è meno coinvolto nelle operazioni di filtraggio del traffico o nella sicurezza di accesso. La sua priorità principale è garantire un trasporto veloce e affidabile del traffico. Inoltre, il Core Layer è progettato per garantire una ridondanza efficiente e un'elevata disponibilità della rete. Ciò significa che, in caso di guasto in una parte della rete, il traffico può essere instradato attraverso percorsi alternativi per evitare interruzioni significative. Nell'ambito del Core Layer, vengono spesso utilizzate le connessioni in fibra ottica che consentono di soddisfare le esigenze di reti aziendali complesse e ad elevate prestazioni. Il Core Layer risulta essere il componente chiave per garantire ad una rete di trasmettere dati ad alta velocità e con affidabilità, svolgendo così un ruolo cruciale nell'assicurare che le operazioni aziendali possano avvenire in modo efficiente e senza interruzioni.

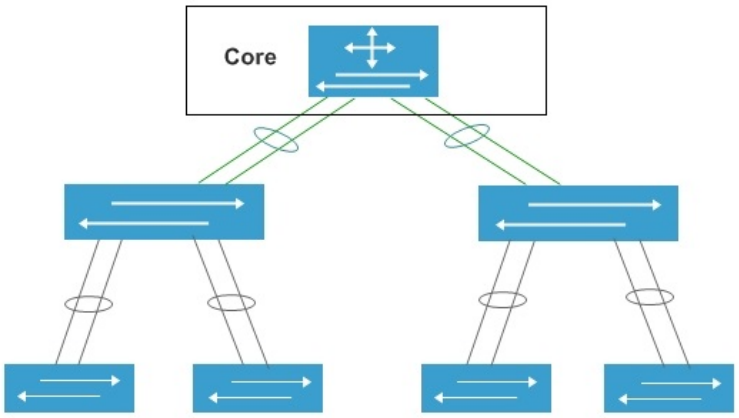

Figura 4.4: Core Layer

4.6 Simulazione tramite Cisco packet tracer

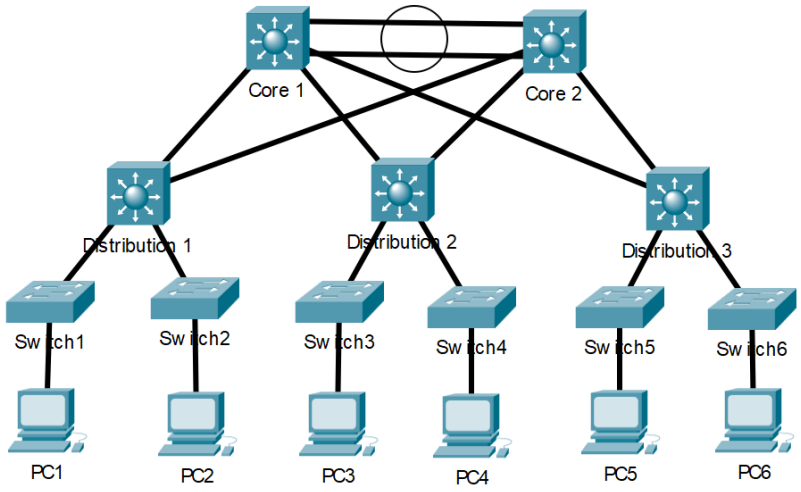

Figura 4.5: Schema di rete simulato tramite Cisco Packet Tracer

La simulazione tramite Cisco Packet Tracer rappresenta uno strumento fondamentale dato che offre la possibilità di creare e configurare reti complesse in un ambiente virtuale, consentendo ai progettisti di rete di sperimentare e testare configurazioni con dispositivi di rete Cisco in modo sicuro e senza la necessità di hardware fisico. Simulando il comportamento di router, switch e altri dispositivi di rete è possibile visualizzare il flusso dei dati e permette di capire se le configurazioni progettate portano ai risultati prestabiliti. Ogni utente è stato simulato tramite un pc generico che può rappresentare qualsiasi tipo di macchina che va da un semplice terminale come un computer fino ad una macchina di produzione. Partendo dalla tabella 4.3 nella sezione 4.2 si è deciso di simulare sia gli switch a 48 porte che quelli a 24 porte con la stessa periferica di rete che Cisco Packet Tracer mette a disposizione. Tutti gli switch dal numero 1 al numero 6 sono stati simulati con dei modelli della serie Cisco Catalyst 2960. Per ogni reparto è stato inserito uno switch di distribuzione. La ripartizione degli switch per zone è la seguente:

- **Uffici generici**: switch distribution 1 insieme agli switch 1 e 2.
- **Reparto produzione**: switch distribution 2 insieme agli switch 3 e 4.
- **Magazzino**: switch distribution 3 insieme agli switch 5 e 6.

Anche se nella tabella 4.3 della sezione 4.2 era previsto un solo switch a 48 porte nel reparto magazzino abbiamo inserito 2 switch per puro scopo simulativo. Infine nel distribution layer e nel core layer sono stati utilizzati gli switch della serie Cisco Catalyst 3560. La serie Cisco Catalyst 2960 e 3560 nella realtà sono prodotti non più supportati da Cisco e rimpiazzati con la serie 9000 ma ai fini simulativi sono risultati ottimi.

4.7 Programmazione degli apparati di rete Cisco

4.7.1 Configurazione switch access layer

Andremo a configurare il primo switch del reparto uffici riportato nella figura 4.5 come Switch 1. Cisco Packet Tracer permette di configurare ogni dispositivo tramite un proprio terminale dedicato.

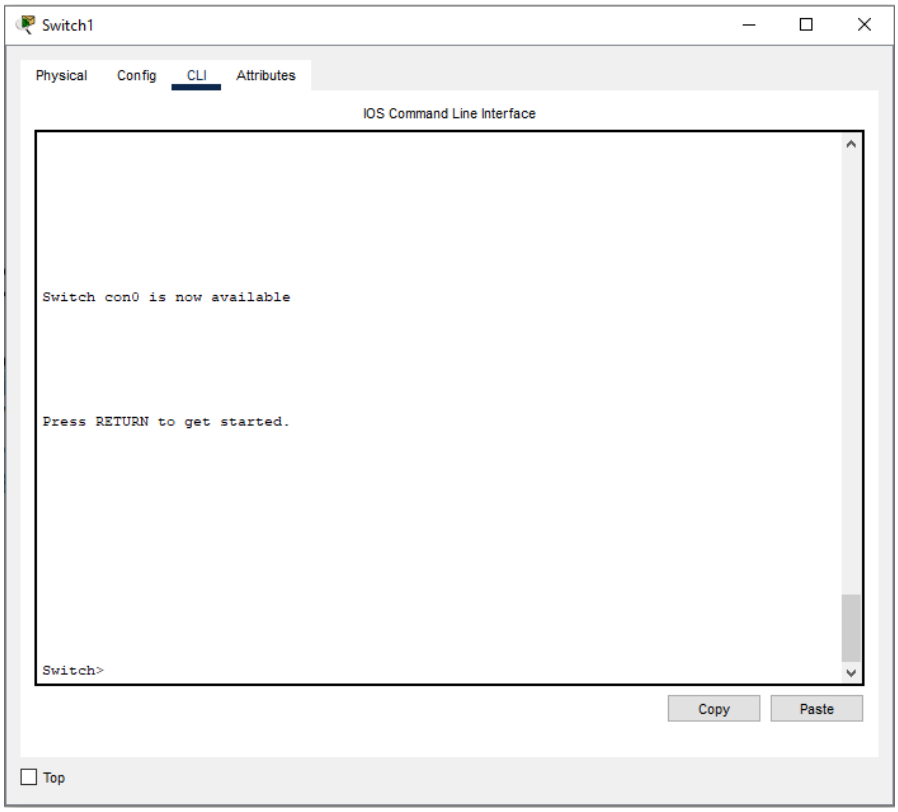

Figura 4.6: Terminale Switch 1

Per entrare in modalità configurazione useremo i seguenti comandi

Switch>enable

Switch#configure terminal

Vogliamo configurare questo switch per gestire i terminali degli impiegati generici e tenendo conto degli indirizzi scelti nella tabella 4.4 sappiamo che dovremo creare una VLAN dedicata a loro con i seguenti comandi:

Switch(config)#vlan 10

Switch(config-vlan)#name Impiegati generici

exit

Assegneremo tutte le porte fisiche dove andranno collegati i terminali alla vlan 10 con i comandi:

Switch(config)#interface range FastEthernet 0/1-24

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

exit

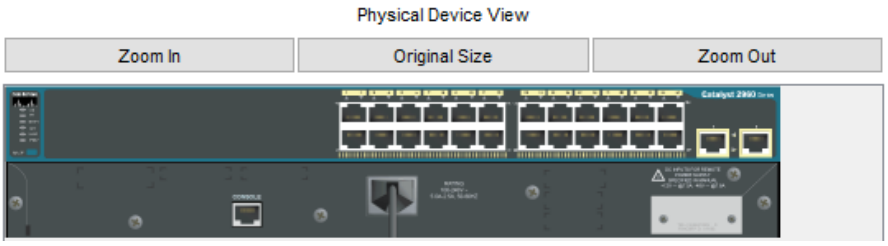

Figura 4.7: Switch Cisco 2960 simulato in packet tracer

Le porte GigabitEthernet 0/1-2 sono dedicate per il collegamento fisico allo switch Distribution 1.
Per proteggere le porte verso gli host da manomissioni o errati collegamenti e garantire che solo un dispositivo possa essere collegato per volta utilizziamo la funzionalità di Port Security. La funzione Port Security limita il numero di indirizzi MAC che possono essere appresi su una porta specifica e può anche spegnere la porta se vengono rilevate violazioni.

Switch(config)#interface range FastEthernet 0/1-24

Switch(config-if-range)#switchport port-security

Switch(config-if-range)#switchport port-security maximum 1

Switch(config-if-range)#switchport port-security violation shutdown

exit

Switchport port-security maximum 1: consente solo il collegamento di un unico dispositivo (un indirizzo MAC) su ciascuna porta.
Switchport port-security violation shutdown: se un secondo dispositivo tenta di collegarsi alla porta, la porta viene messa nello stato di "shutdown" (spenta) e richiede l'intervento manuale per essere riattivata.
Salviamo la configurazione con il comando:

Switch#write memory

A questo per verificare la corretta configurazione dello switch andremo ad utilizzare il comando:

Switch#show running-config

e il terminale stamperà a video la configurazione finale dello switch.

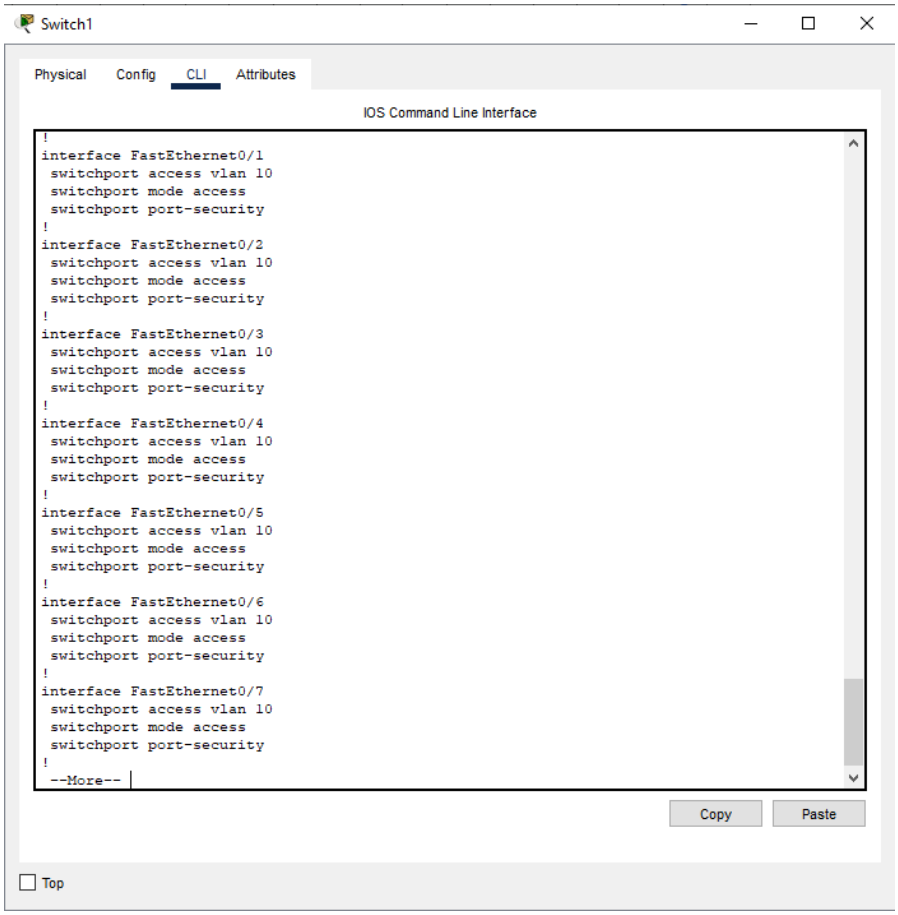

Figura 4.8: Switch 1 configurazione finale

Ripetiamo la configurazione per tutti gli altri switch dal numero 2 al numero 6 ricordandoci di creare sempre la VLAN desiderata e assegnare le porte fisiche alla VLAN che vogliamo noi. Ad esempio nello switch 2 che si trova sempre nel reparto uffici sappiamo in questo caso dai dati della tabella 4.1 che avremo minimo altri 10 impiegati del reparto marketing e 5 impiegati dell'ufficio IT. Ricordandoci che abbiamo a disposizione 24 porte possiamo decidere di dedicare 15 al reparto marketing e 9 agli impiegati IT di conseguenza andremo a creare una configurazione del tipo:

Switch(config)#vlan 20

Switch(config-vlan)#name Ufficio Marketing

Switch(config)#vlan 30

Switch(config-vlan)#name Ufficio IT

Switch(config)#interface range FastEthernet 0/1-15

Switch(config-if-range)#switchport mode access vlan 20

Switch(config-if-range)#switchport port-security

Switch(config-if-range)#switchport port-security maximum 1

Switch(config-if-range)#switchport port-security violation shutdown

Switch(config)#interface range FastEthernet 0/16-24

Switch(config-if-range)#switchport mode access vlan 30

Switch(config-if-range)#switchport port-security

Switch(config-if-range)#switchport port-security maximum 1

Switch(config-if-range)#switchport port-security violation shutdown

exit

4.7.2 Configurazione switch distribution layer

Andremo a configurare il primo switch di distribuzione chiamato Distribution 1 nella figura 4.5. Dato che questo switch si occuperà di collegare gli switch access del reparto uffici con il core andremo per prima cosa a creare tutte le vlan presenti nel reparto uffici.
Creazione delle vlan:

Switch>enable

Switch#configure terminal

Switch(config)#vlan 10

Switch(config-vlan)#name Impiegati-generici

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name Impiegati-marketing

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name Ufficio-IT

exit

Subito dopo andremo a configurare le varie interfacce collegate agli switch di accesso e ai core switch.

Verso lo switch 1

Switch(config-vlan)#interface FastEthernet0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

exit

#Verso lo switch 2

Switch(config-vlan)#interface FastEthernet0/2

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan add 20,30

exit

Infine configuriamo le interfacce collegate ai due core

Switch(config)#interface GigabitEthernet0/1

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

Switch(config-if)#interface GigabitEthernet0/2

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

exit

Il comando switchport trunk encapsulation dot1q è utilizzato nelle configurazioni delle porte di switch di rete Cisco per specificare il metodo di encapsulation dei frame quando una porta viene configurata come trunk. Questo comando indica che il protocollo di encapsulation utilizzato è IEEE 802.1Q, che è uno standard per l'implementazione di trunking VLAN.
Mentre il comando switchport mode trunk è un comando di configurazione su uno switch Cisco che imposta una specifica porta Ethernet in modalità trunk. Una porta in modalità trunk è progettata per gestire il traffico di più VLAN, permettendo così la comunicazione tra più reti.
Quando una porta è configurata come trunk, può trasmettere e ricevere pacchetti VLAN contrassegnati con tag. Questi tag identificano a quale VLAN appartiene ciascun pacchetto, consentendo così agli switch di gestire il traffico di più VLAN attraverso la stessa interfaccia fisica.
Infine andremo a configurare il protocollo STP. Il protocollo STP è configurato in modalità Rapid PVST (Per-VLAN Spanning Tree) per garantire la correzione delle loop all'interno della rete. Useremo il seguente comando:
Switch(config)#spanning-tree mode rapid-pvst

Questa configurazione si ripete anche per il secondo e il terzo distribution switch cambiando le vlan gestite sulle interfacce collegate agli switch nel layer access.

4.7.3 Configurazione switch core layer

La configurazione delle VLAN sui Core Switch coinvolge l'assegnazione degli indirizzi IP alle interfacce VLAN e la configurazione di routing inter-VLAN. Il comando ip routing viene utilizzato su uno switch Cisco per abilitare il routing IP sulla piattaforma. Quando questo comando viene inserito nella configurazione globale dello switch, attiva la funzionalità di routing del dispositivo, consentendogli di instradare pacchetti tra diverse reti IP e trasformandolo in un router. Per fare ciò useremo il seguente comando:

Switch(config)#ip routing

Adesso andremo a creare tutte le VLAN di tutta la rete dato che i core switch dovranno gestire l'instradamento dell'intero traffico:

Switch(config)#vlan 10

Switch(config-vlan)#name Impiegati-generici

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name Ufficio-marketing

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name Ufficio-IT

Switch(config-vlan)#vlan 40

Switch(config-vlan)#name Macchine-utensili

Switch(config-vlan)#vlan 50

Switch(config-vlan)#name Computer-di-linea

Switch(config-vlan)#vlan 60

Switch(config-vlan)#name Wifi

Switch(config-vlan)#vlan 70

Switch(config-vlan)#name Videosorveglianza

Switch(config-vlan)#vlan 80

Switch(config-vlan)#name Computer-magazzino

Switch(config-vlan)#vlan 90

Switch(config-vlan)#name Telefoni

Un SVI, o Interfaccia Virtuale VLAN (Switched Virtual Interface), è una rappresentazione virtuale di un'interfaccia di rete associata a una VLAN su uno switch. Le SVI sono utilizzate per consentire al traffico IP di fluire dentro e fuori di una VLAN su uno switch di livello 3 e questo permette a uno switch di eseguire il routing del traffico tra VLAN diverse. Di seguito vengono configurate tutte le SVI per ogni VLAN:

```
Switch(config-if)#interface Vlan10
Switch(config-if)#ip address 10.0.10.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan20
Switch(config-if)#ip address 10.0.20.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan30
Switch(config-if)#ip address 10.0.30.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan40
Switch(config-if)#ip address 10.0.40.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan50
Switch(config-if)#ip address 10.0.50.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan60
Switch(config-if)#ip address 10.0.60.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan70
Switch(config-if)#ip address 10.0.70.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan80
Switch(config-if)#ip address 10.0.80.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
Switch(config-if)#interface Vlan90
Switch(config-if)#ip address 10.0.90.254 255.255.255.0
Switch(config-if)#ip access-group ACL_INT in
Switch(config-if)#ip access-group ACL_OUTBOUND out
```

Durante la configurazione delle SVI abbiamo utilizzato altri due comandi

Switch(config-if)#ip access-group ACL_INT in

Switch(config-if)#ip access-group ACL_OUTBOUND out

Questi due comandi impostano per ogni SVI una ACL per regolare il traffico in entrata e il traffico in uscita. A questo punto andiamo a creare entrambe le ACL.
La prima ACL servirà per regolare il traffico in entrata e la chiameremo ACL_INT:

```
Switch(config)#ip access-list extended ACL_INT
Switch(config-ext-nacl)#permit ip 10.0.10.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.20.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.30.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.40.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.50.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.60.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.70.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.80.0 0.0.0.255 any
Switch(config-ext-nacl)#permit ip 10.0.90.0 0.0.0.255 any
Switch(config-ext-nacl)#deny ip any any
```

Mentre la seconda ACL servirà per regolare il traffico in uscita e la chiameremo ACL_OUTBOUND:

```
Switch(config-ext-nacl)#ip access-list extended ACL_OUTBOUND
Switch(config-ext-nacl)#permit tcp any any eq 80
Switch(config-ext-nacl)#permit tcp any any eq 443
Switch(config-ext-nacl)#deny ip any any
```

In uscita abbiamo permesso alla rete che possa trasmattere del traffico HTTP e HTTPS impostando le porte 80 e 443 come le uniche consentite.
Ricordiamo che le regole impostate nelle ACL vengono lette dallo switch in modalità TOP-DOWN quindi consentirà tutto il traffico impostato con il comando permit per poi bloccare tutto il traffico rimanente con la regola deny ip any any.

Per garantire che l'infrastruttura di rete gestisca eventuali fault tra Core switch e che funzioni anche in caso di guasto di uno dei Core è possibile adottare diverse pratiche di ridondanza e tolleranza ai guasti. Nella sezione 3.4 veniva descritta come la Cisco Stack Technology permetta una gestione centralizzata degli switch che si adatta perfettamente alle esigenze dei core. Nella simulazione tramite Cisco Packet Tracer però non risulta possibile simulare questa tecnologia e quindi durante questa fase di progettazione si è deciso di ricorrere al HSRP. HSRP, o Hot Standby Router Protocol, è un protocollo di routing di primo hop redundancy (FHRP) utilizzato per fornire alta disponibilità e ridondanza agli indirizzi gateway predefiniti utilizzati dai dispositivi all'interno di una rete. È comunemente utilizzato in reti con più router, in particolare quando si desidera garantire che vi sia un router attivo che agisce come gateway predefinito, con altri router pronti a prendere il controllo in caso di guasto del router attivo. Di seguito è riportata la configurazione del HSRP per la VLAN 10:

Configurazione HSRP per la VLAN 10 su Core Switch 1

Switch(config)#interface Vlan10

Switch(config-if)#standby 1 ip 10.0.10.254

Switch(config-if)#standby 1 priority 110

Switch(config-if)#standby 1 preempt

Configurazione HSRP per la VLAN 10 su Core Switch 2

Switch(config)#interface Vlan10

Switch(config-if)#standby 1 ip 10.0.10.254

Switch(config-if)#standby 1 priority 100

Switch(config-if)#standby 1 preempt

Il comando standby 1 priority 110 viene utilizzato per impostare la priorità del router HSRP nel contesto di un gruppo HSRP specifico.

- standby 1: Questa parte del comando si riferisce al numero del gruppo HSRP. In un contesto HSRP, un gruppo è un insieme di router che condividono la stessa configurazione e partecipano alla stessa attività HSRP.

- priority 110: Questo comando imposta la priorità del router HSRP all'interno del gruppo HSRP specificato. La priorità è un valore numerico che determina quale router nel gruppo HSRP diventerà il router attivo. Un valore più alto indica una priorità maggiore. Nel nostro caso la priorità viene impostata su 110.

Quando il comando standby 1 priority 110 è configurato su un'interfaccia HSRP, indica che il router nel gruppo 1 avrà una priorità di 110. Se c'è una competizione per il

ruolo di router attivo tra i router nel gruppo HSRP, il router con la priorità più alta diventerà il router attivo. In altre parole, il router HSRP con priorità 110 avrà una probabilità maggiore di diventare il router attivo rispetto a un router con una priorità inferiore, in questo caso il core switch 2 con priorità 100.
Invece il comando standby 1 preempt fa si che il router con la priorità più alta all'interno del gruppo HSRP, nel nostro caso il core switch 1, riprenda immediatamente il ruolo di router attivo non appena diventa disponibile dopo essere stato precedentemente indisponibile o essere stato in uno stato di standby.

Subito dopo sono stati configurati i server DHCP per ogni VLAN. Di seguito vengono riportate le configurazione dei primi due:

Configurazione del pool DHCP per la VLAN 10

Switch(config)#ip dhcp pool VLAN10

Switch(dhcp-config)#network 10.0.10.0 255.255.255.0

Switch(dhcp-config)#default-router 10.0.10.254

Switch(dhcp-config)#dns-server 8.8.8.8

Configurazione del pool DHCP per la VLAN 20

Switch(dhcp-config)#ip dhcp pool VLAN20

Switch(dhcp-config)#network 10.0.20.0 255.255.255.0

Switch(dhcp-config)#default-router 10.0.20.254

Switch(dhcp-config)#dns-server 8.8.8.8

La configurazione degli altri server è del tutto analoga. Ad ogni VLAN viene assegnata il proprio ID RETE come riportato nella tabella 4.4 e gli viene assegnato un gateway tramite il comando default-router.

La Cisco Stack technology permette una connessione ridondante e aumenta la larghezza di banda tra i due dispositivi di rete. Per fare ciò tramite Cisco Packet Tracer abbiamo configurato un port channel (o EtherChannel) tra due i core switch che è anche una pratica comune per fornire una connessione ridondante e aumentare la larghezza di banda tra due dispositivi di rete. La configurazione di un port channel tra due switch Cisco utilizzando il protocollo LACP (Link Aggregation Control Protocol) è la seguente:

```
# Core switch 1

Switch1(config)#interface range fa0/3-4

Switch1(config-if-range)#channel-group 1 mode active

Switch1(config-if-range)#exit

Switch1(config)#interface port-channel 1

Switch1(config-if)#switchport mode trunk

# Core switch 2

Switch2(config)#interface range fa0/3-4

Switch2(config-if-range)#channel-group 1 mode active

Switch2(config-if-range)#exit

Switch2(config)#interface port-channel 1

Switch2(config-if)#switchport mode trunk
```

Una volta terminata la configurazione non resta altro che salvarla e testarla tramite Cisco Packet Tracer.

Capitolo 5

Attività post progettazione

5.1 Installazione degli apparati

L'installazione e la configurazione di dispositivi Cisco richiedono una grande attenzione ai dettagli per garantire un funzionamento efficiente e sicuro nella rete. Seguire le best practice durante questo processo è fondamentale e sotto la supervisione del tutor aziendale sono stati stabiliti dei punti da seguire per l'installazione e la configurazione di dispositivi Cisco:

- **Consultare il datasheet**: prima di iniziare l'installazione, assicurarsi di aver consultato il datasheet del dispositivo Cisco che si sta installando. Il datasheet contiene informazioni cruciali sulle specifiche hardware, i requisiti di alimentazione, le porte e i connettori, le caratteristiche di prestazione e altro ancora.

- **Scegliere una posizione adeguata**: posizionare il dispositivo in una posizione appropriata, evitando ambienti troppo caldi, umidi o polverosi. Assicurarsi che il dispositivo abbia spazio sufficiente per il raffreddamento e che sia accessibile per la manutenzione.

- **Alimentazione e cablaggio**: collegare il dispositivo a una fonte di alimentazione affidabile e adeguata. Utilizzare cavi di rete di alta qualità e verificare che siano collegati correttamente alle porte del dispositivo. Assicurarsi che i cavi siano disposti in modo ordinato per evitare attorcigliamenti o altri problemi fisici.

- **Aggiornamenti del firmware**: prima di iniziare a utilizzare il dispositivo, verificare che esegua la versione più recente del firmware o del sistema operativo. Consultare il sito Web di supporto di Cisco per scaricare gli aggiornamenti necessari e seguire attentamente le istruzioni di aggiornamento.

- **Installazione configurazione**: a questo punto è possibile accedere al dispositivo ed installare la configurazione preparata per il dispositivo. Questa configurazione dovrebbe includere impostazioni di rete, come indirizzi IP, subnet, gateway e altro. Assicurarsi di proteggere l'accesso al dispositivo utilizzando una password.

- **Backup delle configurazioni**: eseguire un backup della configurazione appena creata. In caso di guasti hardware o errori di configurazione, potrebbe essere necessario ripristinare la configurazione.

- **Documentazione**: mantenere una documentazione accurata della configurazione e delle informazioni di installazione, compresi i numeri di serie, le date di installazione e le password di accesso.

5.2 Monitoraggio della rete tramite NOC

Durante l'esperienza di stage lo studente ha potuto visitare il NOC dell'azienda Vem sistemi. Il Network Operations Center (NOC) è un centro operativo specializzato nel monitoraggio e nella gestione delle reti informatiche. La sua funzione principale è vigilare sulla salute e sulla sicurezza della rete aziendale. Il NOC utilizza diversi strumenti, tra cui software di monitoraggio delle prestazioni, analizzatori di flussi di rete e sistemi di gestione delle reti. Monitora costantemente la larghezza di banda, la latenza e altri indicatori chiave delle prestazioni della rete. Inoltre, si occupa della sicurezza della rete, rilevando e rispondendo a eventi sospetti o intrusioni. La gestione degli incidenti è una parte cruciale delle responsabilità del NOC. Quando si verificano problemi il NOC coordina le azioni necessarie per ripristinare la normale operatività. La sua missione è garantire un'alta disponibilità dei servizi di rete, intervenendo tempestivamente in caso di anomalie. Gli interventi vengono effettuati da remoto e solo nel caso di guasti fisici verrà segnalato ai sistemisti della struttura la necessità di intervento manuale direttamente sugli apparati di rete. L'automazione è spesso impiegata per semplificare compiti ripetitivi come gli aggiornamenti o il salvataggio di copie di backup delle configurazioni. Il NOC produce regolarmente report sull'andamento delle prestazioni di rete e sull'efficacia delle misure di sicurezza. Questi report sono utili per l'analisi e il miglioramento continuo della gestione della rete. Infine collabora con altri team, come il Security Operations Center (SOC) per affrontare minacce alla sicurezza e il team di manutenzione per risolvere problemi hardware. Complessivamente, il monitoraggio della rete tramite NOC è fondamentale per garantire un funzionamento efficiente, sicuro e affidabile delle reti aziendali. Non sono state effettuate delle particolari attività dallo studente all'interno del NOC ma è risultato utile visitarlo a scopo didattico.

Conclusioni

Durante il periodo di tirocinio è emerso chiaramente come la progettazione e l'implementazione di un sistema di rete adeguato siano elementi essenziali per sostenere le operazioni quotidiane e la crescita sostenibile delle PMI. L'analisi delle esigenze specifiche delle piccole e medie imprese ha evidenziato la necessità di soluzioni flessibili, scalabili e sicure. L'implementazione di un sistema di networking ben progettato offre diversi vantaggi, tra cui un miglioramento dell'efficienza operativa attraverso la condivisione rapida e sicura delle risorse, la facilitazione della comunicazione interna ed esterna e una maggiore resistenza agli attacchi informatici. La scelta accurata di dispositivi e tecnologie, considerando le esigenze attuali e future, è stata identificata come un passo cruciale nel garantire la sostenibilità del sistema nel lungo termine. E' stato evidenziato come un adeguato piano di gestione e manutenzione del sistema di networking sia fondamentale per garantire un funzionamento continuo e prevenire eventuali interruzioni delle attività aziendali. La formazione degli utenti e la documentazione dettagliata delle procedure operative sono elementi chiave per garantire un utilizzo efficace e sicuro delle risorse di rete. In conclusione, la progettazione e l'implementazione di un sistema di networking su misura per le PMI rappresenta un investimento strategico che può contribuire significativamente al successo e alla crescita sostenibile di tali imprese. Un approccio completo che considera aspetti tecnologici, di sicurezza e di gestione è fondamentale per garantire una rete resiliente e in grado di adattarsi alle mutevoli esigenze del contesto aziendale.

Glossario

Firmware è un tipo di software integrato in dispositivi hardware, come schede madri, stampanti, o dispositivi di rete. È responsabile dell'esecuzione di funzioni specifiche e fornisce istruzioni di basso livello per il controllo e la gestione hardware. E' immagazzinato nella memoria del dispositivo e viene mantenuto anche durante i riavvii. 10

IEEE Institute of Electrical and Electronics Engineers, è un'organizzazione professionale internazionale che sviluppa standard nell'ambito dell'ingegneria elettrica, dell'elettronica e delle tecnologie dell'informazione. Gli standard dell'IEEE sono ampiamente utilizzati per garantire l'interoperabilità e la compatibilità tra dispositivi e sistemi in vari settori, tra cui le reti informatiche e le comunicazioni wireless. 9

LAN Local Area Network (LAN) è una rete informatica limitata a una specifica area geografica, come un edificio o un campus. Le LAN consentono la condivisione efficiente di risorse, come file e stampanti, tra dispositivi quali computer e dispositivi di rete. 7

MAC è il protocollo che regola l'accesso al mezzo trasmissivo in una rete di computer. Definisce le regole per la gestione dell'indirizzamento hardware, il controllo di accesso al canale e la prevenzione delle collisioni tra dispositivi sulla rete. 7

MAN Metropolitan Area Network, è una rete di computer che copre un'area geografica più estesa rispetto a una LAN ma è più limitata rispetto a una WAN (Wide Area Network). Una MAN collega diversi siti all'interno di una città o di un'area metropolitana, fornendo una connettività ad alta velocità per la condivisione efficiente di risorse e dati tra organizzazioni e aziende distribuite all'interno di una stessa regione. 21

SNMP Simple Network Management Protocol è un protocollo di rete standard utilizzato per monitorare e gestire dispositivi di rete, come router, switch e server. SNMP consente agli amministratori di rete di raccogliere informazioni sullo stato e le prestazioni dei dispositivi di rete, nonché di eseguire operazioni di gestione remota, facilitando il monitoraggio e il controllo delle risorse di rete in modo efficiente. 8

WAN Wide Area Network, è una rete di computer estesa su un'ampia area geografica, come un paese o persino a livello globale. Le WAN collegano diverse reti locali (LAN) e/o reti metropolitane (MAN) attraverso tecnologie di comunicazione ad alta velocità, consentendo la condivisione di risorse e dati su lunghe distanze. 21

Bibliografia

Riferimenti bibliografici

Odom, Wendell. *Ccna 200-301 Official Cert Guide Library*. Cisco Pr, 2020.

Tanenbaum, Andrew S. *Reti di calcolatori*. Pearson 5° edizione, 22 maggio 2018.