UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

"Reti LAN enterprise: configurazione e verifica comportamentale dell'implementazione estesa dei protocolli 802.1ax"

Relatore: Prof. Nicola Zingirian

Laureando: Tommaso Boatto

ANNO ACCADEMICO 2022 – 2023

Data di laurea 21/03/2023

Indice

Sommario

La tesi presenta la metodologia e i risultati di un progetto di tirocinio svolto presso l'ospedale "Santa Maria degli Angeli" a Pordenone dal 24/10/2022 al 01/12/2022. L'attività di tirocinio ha avuto luogo nel Reparto di Ingegneria Clinica Informatica della struttura ospedaliera, dedicato a gestirne tutti i servizi tecnici. Il progetto è stato realizzato in collaborazione con il personale del reparto per mettere in esercizio una nuova infrastruttura di rete dati. A tale scopo il progetto ha selezionato una soluzione di *networking* proposta da una multinazionale di nome Extreme Networks, già precedentemente individuata dalla azienda ospedaliera. Gli obiettivi principali dell'esperienza sono stati la configurazione di tutti i nodi e degli apparati della rete dati basata su una tecnologia che prende il nome commerciale di Fabric Connect. A seguito dell'avvio della infrastruttura, il progetto ha anche previsto l'attivazione di tutti i servizi e protocolli necessari al funzionamento dei nodi ed è terminato dopo una campagna di test che hanno verificato il corretto funzionamento della rete e della nuova tecnologia.

Capitolo 1

Introduzione

1.1 Contesto dello sviluppo del progetto

Il progetto è stato svolto nel Reparto di Ingegneria Clinica Informatica dell'Ospedale di Santa Maria di Pordenone. Il reparto gestisce l'infrastruttura informatica e di telecomunicazione dell'Ospedale, inclusi i macchinari biomedicali, e la telefonia con l'aiuto di fornitori esterni. La gestione dell'infrastruttura è un punto critico e delicato, in quanto tutti i reparti hanno necessità di comunicare tra di loro anche per procedure *mission critical*, da cui nasce l'esigenza di una rete veloce, stabile, sicura e ad alta affidabilità, poiché i dati devono poter viaggiare ad alta velocità e preservando la loro integrità. Per ottenere questi risultati, sistemisti ed altri dipendenti lavorano continuamente per garantire un'infrastruttura solida e performante.

Il sistemista di rete si occupa principalmente della gestione e della manutenzione di pressoché tutti gli elementi dell'infrastruttura di rete presente nelle aziende odierne, come l'hardware (apparecchiature di rete), il software (di gestione, di analisi, ecc..), gli strumenti di sicurezza ed anche la rete dati interna. Gli aspetti legati alla cybersecurity sono anche divenuti un obiettivo molto importante per il Reparto che è responsabile anche della protezione dell'infrastruttura IT aziendale, con metodologie e software appositi. Per poter diventare sistemista sono necessarie alcune competenze come la conoscenza dei sistemi operativi, del funzionamento e della struttura delle reti, dei linguaggi di programmazione e dei possibili tipi di minacce informatiche.

1.2 **Tecnologie e Soluzioni**

L'attività principalmente svolta durante il tirocinio ha riguardato la configurazione del prodotto "Fabric Connect"[1] dell'azienda Extreme Networks[1], sugli apparati facenti parte di un prototipo di rete precedentemente studiato e messo a punto dal Reparto. Il prodotto "Fabric Connect" è un'implementazione di alcuni protocolli già esistenti e largamente conosciuti ed utilizzati, ossia l'IEEE 802.1aq e l'IEEE 802.1ah-2008, e di loro estensioni.

Il protocollo 802.1aq prende il nome di SPB (Shortest Path Bridging), esso nasce con l'obiettivo di rimuovere alcune limitazioni date da precedenti protocolli, per poter dare maggiore stabilità alla rete, supportare applicazioni con percorsi simmetrici del traffico nelle reti fabric (architettura di rete divisa in due o tre layer altamente interconnessi) e per ridurre la complessità del livello di core tramite il protocollo IS-IS (Intermediate System to Intermediate System). L'IEEE 802.1ah invece, è un protocollo che fornisce la possibilità di configurare un maggior numero di istanze di servizio nella rete e incapsula o decapsula il traffico dell'utente finale ai confini della rete del provider.

Il Fabric Connect ha infine un'ulteriore funzionalità, interamente realizzata mediante software chiamata "Fabric Attach"[1]. Essa permette a nuovi dispositivi, soprattutto quelli che non supportano il Fabric Connect/SPB di essere configurati ed inseriti nella rete in maniera autonoma e senza appunto dover mettere mano sui dispositivi di rete, riducendo drasticamente i costi necessari all'aggiunta o modifica di servizi/dispositivi. Il funzionamento del Fabric Attach è basato sull'LLDP (Link Layer Discovery Protocol)[2], definito dallo standard IEEE 802.1AB, utilizzato dai dispositivi per comunicare informazioni riguardanti l'identità del dispositivo stesso (gestione delle porte, degli indirizzi IP, delle VLAN, ecc..).

---

[1] Azienda americana con sede a San Jose, in California, che si occupa di progettare, sviluppare e produrre apparecchiature di rete software per la gestione della rete, la sicurezza, l'analisi di rete, le policy e il controllo degli accessi.

Capitolo 2

Organizzazione del tirocinio

2.1 **Obiettivi**

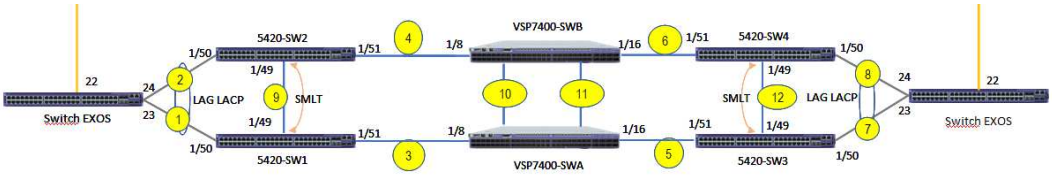
L'obiettivo iniziale del progetto è stato la messa a punto della rete, in maniera tale da poter disporre, ancor prima di implementare il Fabric Connect, una rete correttamente configurata in modo da prevenire per quanto possibile ogni successivo problema. Gli apparati di rete inseriti nel prototipo non erano mai stati usati prima e neanche configurati.
L'obiettivo successivo, dopo la prova di conformità alle specifiche del prototipo, è stata la configurazione del "Fabric Connect" sul prototipo di rete e il test di funzionalità e prestazione della rete utilizzando opportuni software.

2.2 **Fasi del lavoro**

Il lavoro svolto durante l'esperienza di tirocinio è stato diviso in più fasi, in modo tale da poter procedere da un punto a quello successivo del progetto, essendo sicuri che il lavoro precedentemente svolto fosse corretto e non portasse errori o situazioni anomale alla fase successiva. Infatti, ancor prima di metter mano sulle apparecchiature di rete fisiche, abbiamo diviso il lavoro nelle seguenti fasi, le quali risultano altamente interconnesse, poiché ognuna di esse prende come input, i risultati ottenuti nei punti precedenti:

- predisposizione e configurazione delle macchine fisiche che compongono la rete: le apparecchiature di rete utilizzate sono ancora “vergini”, cioè si trovano alle impostazioni di fabbrica, vanno quindi avviate per la prima volta e va aggiornato il firmware interno all’ultima release disponibile.

- si sono predisposte le macchine, una volta aggiornate e configurate, secondo un prototipo di rete già creato precedentemente e si sono cablate secondo le specifiche del modello in questione. L’immagine sottostante raffigura lo schema del prototipo:



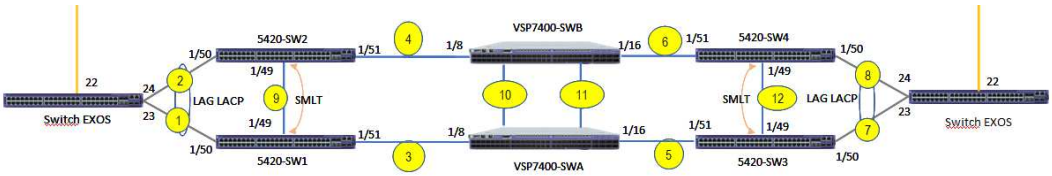
come possiamo vedere la rete in questione è composta da 8 switch di Extreme Networks, i quali si dividono in due modelli: 5420M-48W-4YE e VSP7400-48Y, verranno successivamente presentati meglio.

- dopo aver predisposto e cablato le macchine secondo le specifiche, si è passati ad attivare i servizi ed i protocolli necessari al funzionamento del Fabric configurando anche gli altri protocolli necessari ad un corretto ed efficiente funzionamento dei vari collegamenti tra i macchinari (SMLT, LAG LACP).

- prima dei test specifici, si è verificato il funzionamento della rete provando la connettività a livello rete (tramite l’utility “ping”) tra i nodi periferici della rete. L’ultima fase ha previsto lo studio del comportamento della rete sotto alcune condizioni imposte esternamente, ed il test di alcuni parametri della rete che ne indicheranno poi la qualità degli strumenti utilizzati e del lavoro svolto, saranno anche poi indicatori della robustezza della rete Fabric.

2.3 **Materiali e strumenti utilizzati**

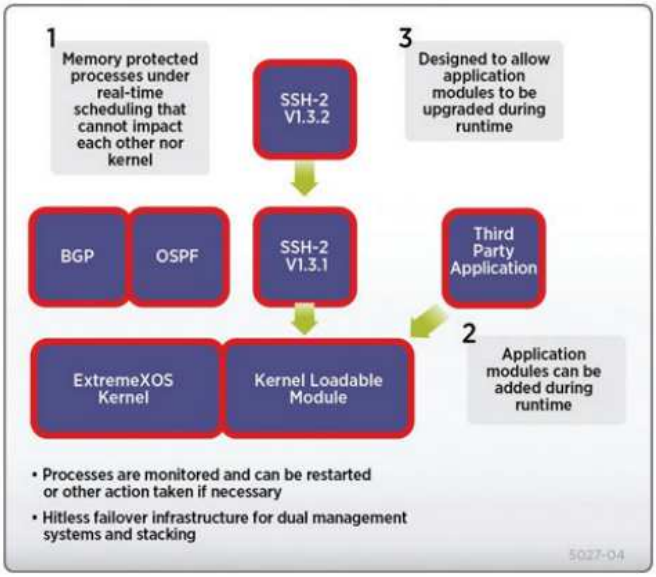
Riprendiamo il modello di rete sopra indicato:



possiamo distinguere due tipi di switch di rete:

- Extreme Networks 5420M-48W-4YE, Fa parte della serie 5420, una famiglia di switch di edge[3] ad alte performance ed alta affidabilità, progettata per le reti enterprise di ultima generazione. Switch di edge significa che è situato nel punto di interconnessione di due reti, tipicamente le reti LAN alle reti del provider di servizi internet (ISP). Le due linee arancioni in figura rappresentano il collegamento verso il router del provider dell'azienda. Li troviamo ai lati della rete denominati "Switch EXOS", ma anche all'interno della rete come possiamo evincere dai nomi indicati, poiché per scelte aziendali e per la loro flessibilità e potenza possono essere impiegati anche nella parte di "core" della rete, ossia quella compresa tra gli switch di edge. Essi sono dotati di 48 porte da 10/100/1000Base-T da 90W e in Full/Half-Duplex, 4 porte in fibra SFP28 da 1/10/25Gbps (SFP28 indica un tipo di ricetrasmittente basata su SFP+,che supporta velocità fino a 10Gb/s, mentre SFP28 supporta fino a 25Gb/s), 1 ingresso per la seriale con connettore RJ-45, per collegamento tramite porta seriale ed un ingresso 10/100/1000Base-T per la gestione fuori banda[6]. Quest'ultima porta consente di collegarsi allo switch in maniera isolata per operazioni di controllo e gestione. Sono presenti anche tre porte USB, di cui due di tipo A ed una Micro-B, che non sono state utilizzate nel nostro caso, assieme ad altri due ingressi in fibra SFP. Qui di seguito un'immagine dell'apparecchiatura in questione:

Queste macchine sono dotate di un firmware EXOS, ossia il software utilizzato negli switch più recenti dell'azienda americana, facente parte della seconda generazione di sistemi operativi Extreme ed è basato su kernel Linux. Esso è un sistema operativo modulare, ossia le varie funzionalità di cui dispone sono divise in più gruppi o moduli, ognuno dotato della propria interfaccia. Tale sistema operativo promette alcuni vantaggi come un'architettura ad alta affidabilità, ricchezza di protocolli a livello L2 e L3, un accesso sicuro alla rete basato sulle policy o sulla gestione delle identità, ecc.. . Qui di seguito un'immagine che rappresenta l'architettura modulare dell'EXOS[4]:



In realtà in questa configurazione di rete, solo SW1 e SW2 sono dotati dell'EXOS, mentre SW1, SW2, SW3 e SW4 sono stati aggiornati al VOSS, altro sistema operativo di Extreme tipicamente utilizzato sulla serie VSP. Questa scelta è motivata dal fatto che

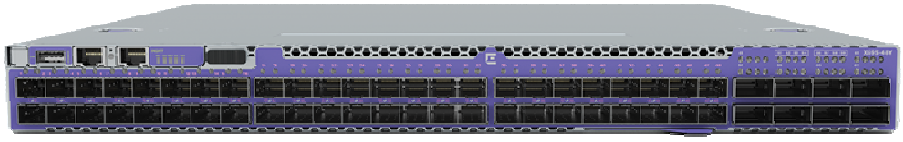
il VOSS è leggermente più semplice da utilizzare ed EXOS invece dispone di più funzionalità orientate alla sicurezza e alla sua gestione, infatti gli switch che si interfacciano al router dell'ISP dell'azienda, come sopra menzionato, ne sono dotati.

In quest'altra immagine possiamo invece vedere i protocolli supportati da EXOS per i vari modelli dai quali è supportato :

	X435	X440-G2	X450-G2	X460-G2	5320	5420	5520	5720	X465	X590	X620	X670-G2	X690	X695	X870
Switching															
IEEE 802.1D – 1998 Spanning Tree Protocol	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1D – 2004 Spanning Tree Protocol (STP and RSTP)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1Q – 2003 (formerly IEEE 802.1s) Multiple Instances of STP, MSTP	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
EMISTP, Extreme Multiple Instances of Spanning Tree Protocol	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
PVST+, Per VLAN STP (802.1Q interoperable)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Standby Router Protocol (ESRP)	-	AE	AE	AE	•	•	•	•	AE	AE	AE	AE	AE	AE	AE
IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.3ad Static load sharing configuration and LACP based dynamic configuration	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AX-2008 Link Aggregation	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Software Redundant Ports	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Multi-Switch Link Aggregation Groups (M-LAG)	-	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AB – LLDP Link Layer Discovery Protocol	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Discovery Protocol (EDP)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Cisco Discovery Protocol (CDP) v1	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Cisco Discovery Protocol (CDP) v2[17]	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Loop Recovery Protocol (ELRP)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Link State Monitoring (ELSM)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1ag L2 Ping and traceroute, Connectivity Fault Management	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T Y.1731 Frame Delay	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T Y.1731 Frame Loss	-	-	-	•	•	•	•	•	•	•	-	•	•	•	•
IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management	-	•	•	•	•	•	•	•	•	•	•	•	•	•	•

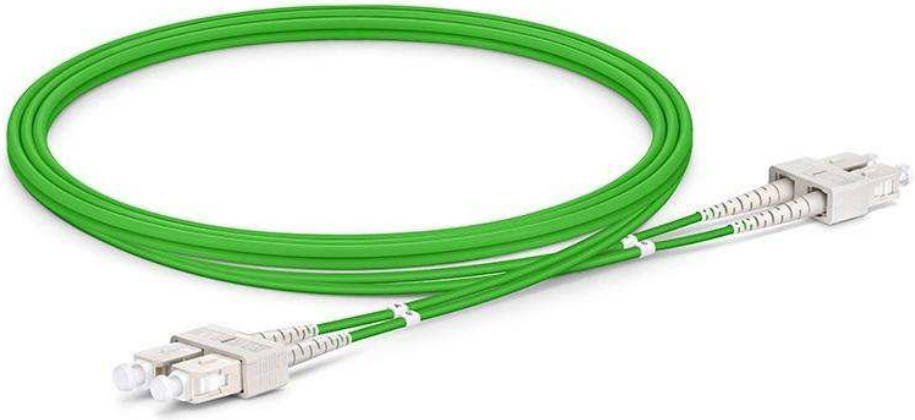
- Extreme Networks VSP7400-48Y-8C. Fa parte della serie 7400, la quale costituisce una famiglia di switch core[5] /aggregazione. Uno switch di aggregazione è solitamente posto al centro dell'architettura di rete, ed è responsabile della gestione dei dati provenienti dagli switch collegati direttamente agli utenti finali, per appunto raccogliere i dati, operando alcune azioni come routing locale, filtraggio, bilanciamento del traffico e gestione delle priorità dei QoS (strumenti o tecniche per ottenere una qualità del servizio desiderata). La classe di switch 7400-48Y è caratterizzata da 48 porte in fibra da 10/25Gb/s che supportano le fibre con connettore SFP28, precedentemente

descritto, 8 porte da 100Gb/s con connettore QSFP28(QSFP sta per “Quad SFP” in quanto può trasportare 4 canali contemporaneamente, in questo caso QSFP28 ne trasporta 4 da 25Gb/s), una porta ethernet seriale con connettore RJ-45 per la connessione da terminale, un’altra porta ethernet fino a 1Gbps per la gestione fuori banda, come nel caso del 5420M ed alcune porte USB per collegare lo switch ad un supporto di memoria esterno[6]. Qui di seguito una foto del VSP7400:



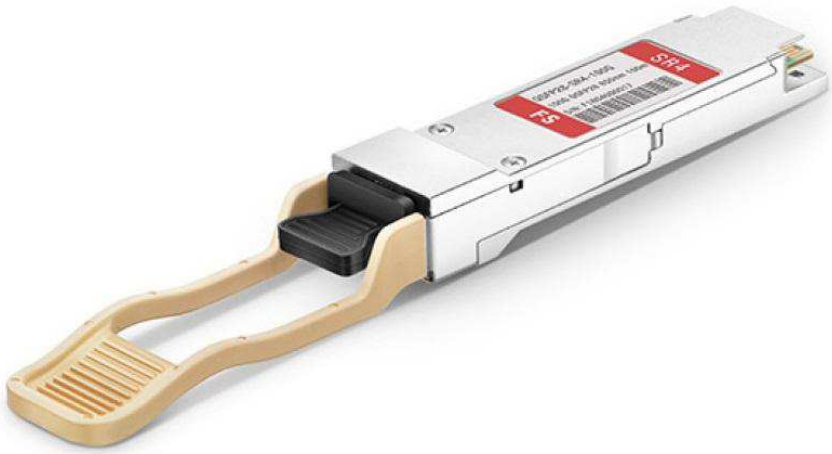
Questa famiglia di switch di rete è dotata di un altro sistema operativo rispetto alla serie 5420M, ossia il VOSS (può essere comunque installato sulla serie 5420M,infatti gli switch 5420M SW1,SW2,SW3,SW4 sono stati aggiornati al VOSS) sistema operativo attualmente utilizzato dalla famiglia di switch VSP 4000, 7200, 7400, 8000 e 8600.

- Fibre ottiche FS OM5 multimodali: esse vengono utilizzate per realizzare tutti i collegamenti indicati nel modello di rete, si usa la fibra invece dei cavi in rame per motivi di velocità chiaramente, poiché è impensabile di trasmettere certe quantità di dati tramite cavi di rame standard. Vengono utilizzate fibre multimodali perchè sono destinate ad un utilizzo in locali chiusi, mentre quelle monomodali, che possono raggiungere i 40km senza compromettere il segnale, sono più adatte ad applicazioni a lunga distanza.



- Connettori FS SFP28: essi sono dei connettori utilizzati per adattare l'ingresso degli switch alle fibre ottiche. Questo tipo viene impiegato nei collegamenti tra gli switch della serie 5420M con velocità massima 25Gbps[7].

- Connettori FS QSFP28:essi vengono utilizzati negli ingressi a 100Gbps negli switch VSP7400 poiché supportano una maggiore velocità di trasmissione e ricezione dati rispetto alle SFP28[7].



- HPE ProLiant DL560 Gen10: esso è una macchina che funge principalmente da server per i data center, orientato principalmente ad esigenze applicative e di virtualizzazione. Viene dotato di due processori Intel Xeon Gold 5220 con CPU a 2.20GHz, 18 core per processore e 256GByte di RAM. Come schede di rete utilizza due Mellanox ConnectX-5 EN con uscita in fibra a 25GBps[8].

Tale macchina non viene impiegata direttamente nel modello di rete precedentemente discusso, ma viene utilizzato per scopi di test, su di esso è installato Linux Ubuntu

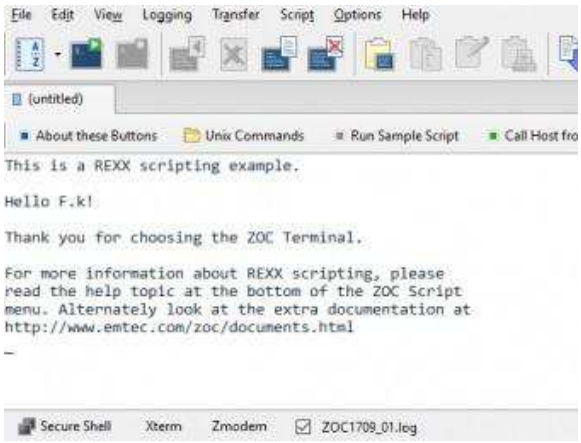
22.04, sul quale viene installato Ostinato 1.1 per scopi di test. Viene collegato alla rete attraverso le due schede di rete di cui è dotato e tramite fibra, indicata nel modello dai due fili gialli uscenti dagli switch EXOS.

- DELL PowerEdge R740xd: anch'esso è un server utilizzato nei data center, dotato di massimo due processori Intel Xeon Gold 6238R e CPU a 2.20GHz, con 28 core a processore e 128 GByte di RAM[9]. Su di esso viene installato VMWare ESXi 8.0, con il quale vengono adoperate due macchine virtuali per i test di ping, con Windows 2019 Standard.

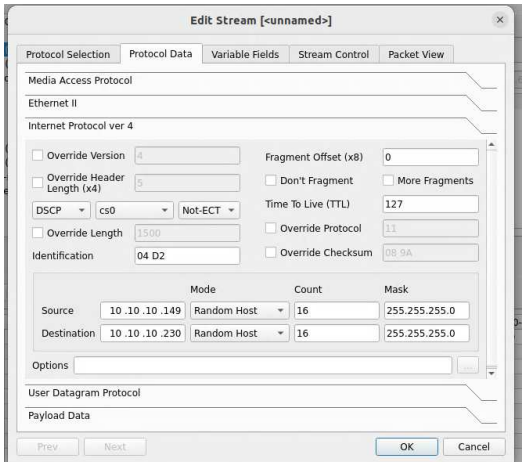
Per la realizzazione del progetto sono stati impiegati i seguenti software:

- ZOC: è un software commerciale sviluppato da EmTec Innovative Software. Si tratta di un emulatore di terminale di tipo client Telnet attraverso una serie di protocolli selezionabili, come l'SSH (V1/V2), modem via porta seriale, ISDN,ecc.. e permette appunto di emulare alcuni terminali (Xterm VT100 di Linux,terminali IBM,ecc..). Durante il lavoro è stato largamente utilizzato per connettersi alle apparecchiature di rete sfruttando il protocollo SSH. Come già menzionato nella descrizione degli switch, essi sono dotati di una porta ethernet per il collegamento seriale, è stata appunto molto utilizzata nella prima fase del

lavoro per collegarsi alle macchine tramite ZOC e poterle così dare una prima configurazione. Il software in questione permette di collegarsi ad un altro host anche tramite protocollo Telnet, in alcuni casi è stato utile per connettersi agli switch tramite la porta di gestione fuori banda. Un esempio della schermata principale di ZOC:



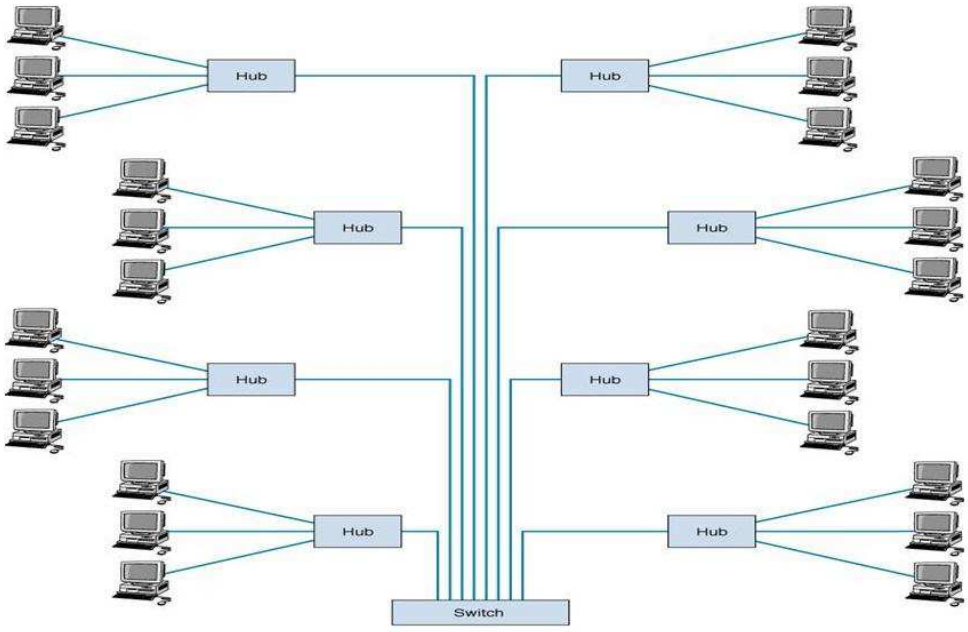
- Ostinato (v1.1): Ostinato[17] è un software che permette di creare pacchetti, leggere file .pcap (file che contengono dati dei pacchetti di rete) e generare traffico di rete. Durante il lavoro è stato utilizzato per la sua funzione di generatore di traffico di rete, poiché permette di generare traffico da un'interfaccia di rete verso un'altra, potendo giocare con i parametri dei pacchetti per eseguire vari test, si può inoltre decidere i protocolli utilizzati nella comunicazione, la grandezza del pacchetto, il contenuto degli header,ecc.. . Qui di seguito uno screen preso dal tirocinio, della schermata che permette di editare i parametri del flusso di dati che si intende creare:


Edit Stream [<unnamed>]
Protocol Selection
Protocol Data
Variable Fields
Stream Control
Packet View
Media Access Protocol
Ethernet II
Internet Protocol ver 4
Override Version
4
Override Header Length (x4)
5
DSCP
cs0
Not-ECT
Override Length
1500
Identification
04 D2
Fragment Offset (x8)
0
Don't Fragment
More Fragments
Time To Live (TTL)
127
Override Protocol
11
Override Checksum
08 9A
Mode
Count
Mask
Source
10 .10 .10 .149
Random Host
16
255.255.255.0
Destination
10 .10 .10 .230
Random Host
16
255.255.255.0
Options
User Datagram Protocol
Payload Data
Prev
Next
OK
Cancel

Capitolo 3

Topologia della rete

La topologia di rete utilizzata, ossia il modello geometrico utilizzato per rappresentare le relazioni di connettività tra gli elementi costituenti la rete stessa, è chiamato "collapsed backbone"[16], di cui in seguito riportiamo un esempio :



Tale tipologia riferisce ad un modello di rete in cui i nodi che costituiscono la dorsale (backbone) della rete vengono compressi in un unico dispositivo centrale, in questo caso costituito dai VSP7400, essi sono utilizzati in coppia per garantire un'alta affidabilità da parte della rete, ma di fatto essi vengono visti da essa come un unico dispositivo. Questo design di rete è largamente utilizzato ed adatto a reti aziendali di medio-grandi dimensioni, come quelle presenti in ospedali, scuole, altri enti pubblici e ambienti aziendali in generale, si adatta poco bene invece a reti più grandi ad esempio quelle

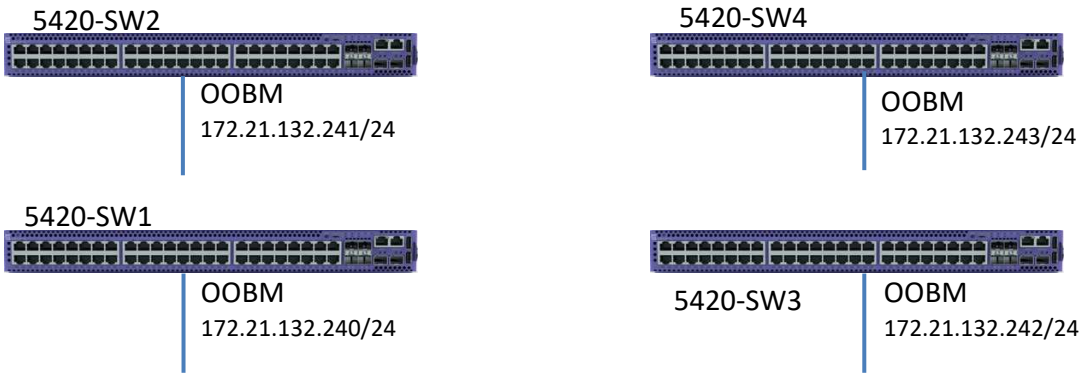
adibite ai servizi metropolitani, poiché i costi in termini di materiali e manutenzione potrebbero essere proibitivi.

Capitolo 4

Configurazione delle macchine

4.1 Configurazione 5420M-48W-4YE

La prima fase del progetto è quella che riguarda appunto la configurazione delle macchine, ancor prima del loro cablaggio. Le prime ad essere state configurate sono gli switch della serie 5420M, esse sono state configurate partendo dalle impostazioni di fabbrica essendo nuove e mai utilizzate prima. La prima fase del lavoro inizia con la configurazione degli indirizzi dell'interfaccia OOBM (Out-of-Band Management), il cui vantaggio è quello di essere disponibile quando la rete non è raggiungibile, poiché se un dispositivo è spento, in standby, ibernato o risulta non accessibile tramite la rete LAN aziendale si può accedere ad esso tramite tale interfaccia. L'accesso a tale interfaccia avviene come menzionato nel capitolo precedente tramite una porta in rame 1000Base-T. Per fare ciò ci si collega allo switch tramite la porta seriale, siccome tale interfaccia non dispone ancora di un indirizzo, non può perciò essere raggiunta, ed utilizzando ZOC per connettersi al terminale dal quale verranno inviati tutti i comandi al dispositivo, il tipo di indirizzamento utilizzato è il seguente:



una volta connessi al terminale, vengono forniti i seguenti comandi alla macchina:

```
boot config flags ftpd
boot config flags sshd
boot config flags tftpd

prompt "5420M-SW1"  … "5420M-SW4"
password password-history 3

ssh
snmp-server user OrionNCM group "SnmpV3Grp" sha des

mgmt oob
ip address 172.21.132.241/24
ip route 0.0.0.0/0 next-hop 172.21.132.1 weight 300
enable
force-topology-ip
exit
mgmt vlan 4048
mac-offset 0
enable
exit

ntp server 172.21.190.155
ntp
```

chiaramente tali comandi verranno replicati su tutti e quattro gli switch. Andiamo ora ad analizzare i comandi più importanti. Come prima cosa si attivano alcuni flag (ftpd, sshd, tftpd) per poter poi abilitare alcuni servizi come l'FTP (File Transfer Protocol) per il trasferimento e download di file dal dispositivo (es: per scaricare le immagini degli aggiornamenti del software), l'SSH (Secure SHell) per l'accesso tramite OOBM ed infine il tftp (Trivial File Transfer Protocol), meno importante per i nostri scopi.

Accediamo ora alla sezione che ci permette di modificare i parametri della OOBM:

- mgmt oob: tale comando ci permette di accedere alla sezione contenente tutti i parametri della OOBM, per poterle così assegnare un indirizzo.

- ip address 172.21.132.241/24: con questo comando andiamo ad assegnare all'interfaccia OOBM dello switch in questione, l'indirizzo ip espresso in notazione CIDR (indirizzo/subnet), in questo caso l'indirizzo ip è 172.21.132.241 e la subnet è, 24 (equivalente a 255.255.255.0).

- ip route 0.0.0.0/0 next-hop 172.21.132.1 weight 300: serve a configurare il routing statico sullo switch, poiché in una prima configurazione senza ricorrere al routing dinamico, esso necessita di un'interfaccia di routing statico, passando attraverso all'host (router) con indirizzo 172.21.132.1/24.

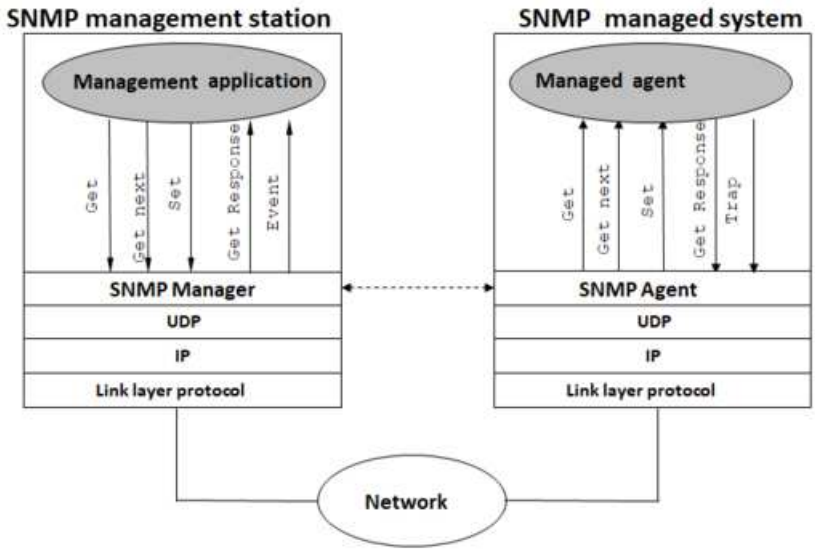
- mgmt vlan 4048: viene creata una VLAN per l'interfaccia OOBM e le viene assegnato il tag 4048.

Tra gli altri comandi indicati troviamo:

- ssh : serve ad abilitare effettivamente il protocollo SSH sullo switch in questione.

- snmp-server user OrionNCM group "SnmpV3Grp" sha des : serve a configurare il protocollo SNMP (Simple Network Management Protocol)[10], ossia un protocollo di rete operante a livello 7 del modello OSI, che consente di avere

una configurazione, gestione e supervisione semplificate, di apparecchi collegati ad una rete riguardo tutti gli aspetti legati ad azioni di management del network. Qui di seguito un'immagine che rappresenta la struttura di un sistema gestito tramite SNMP:

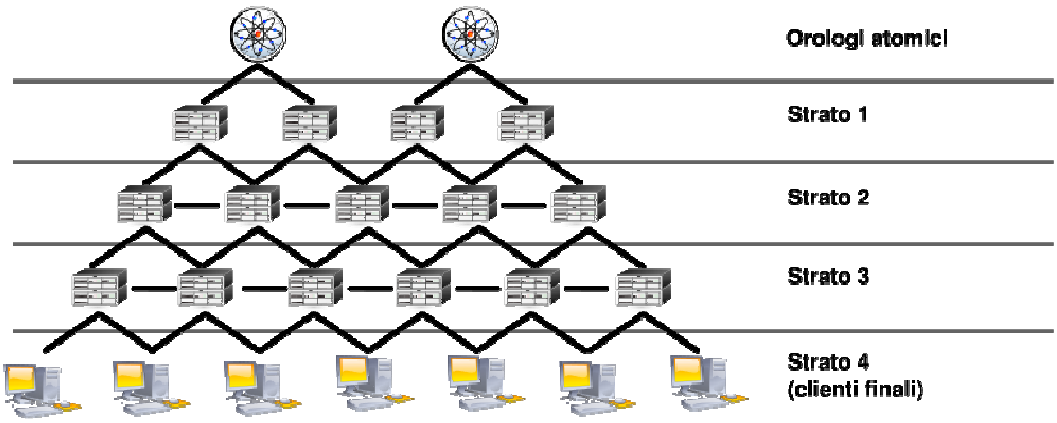


come si evince dall'immagine, l'architettura della gestione di un sistema tramite SNMP prevede tre elementi

1. il sistema di gestione, ossia il manager
2. l'agente di gestione che è presente nei dispositivi gestiti (ed eventuali subagent)
3. una collezione di managed object

Con il comando sopra indicato si crea il gruppo SnmpV3Grp e gli si aggiunge lo user OrionNCM.

- ntp server 172.21.190.155: configura il server per il protocollo NTP all'indirizzo indicato. Il protocollo NTP (Network Time Protocol)[11] è uno dei più vecchi protocolli client-server in uso, la sua funzione è quella di compensare alla scarsa qualità degli orologi hardware dei sistemi, sincronizzando gli orologi dei computer all'interno di una rete. Qui di seguito una figura rappresentante l'architettura del servizio NTP:



- ntp: abilita effettivamente il protocollo NTP sullo switch in questione.

La stessa configurazione viene replicata sugli switch ai lati della rete, ossia Switch EXOS-SW5 e Switch EXOS-SW6.

4.2 **Configurazione VSP7400-48Y-8C**

La configurazione dei VSP7400 avviene in maniera analoga a quanto riportato per i 5420M, per semplicità viene riportata la configurazione finale delle due macchine, dove in giallo sono indicate le differenze tra le due configurazioni:

# # CLI CONFIGURATION # prompt "VSP7400-SWA" password hash sha1	# # CLI CONFIGURATION # prompt "VSP7400-SWB" password hash sha1

```
#
# ISIS SPBM CONFIGURATION
#
router isis
spbm 1
spbm 1 nick-name 0.01.00
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
spbm 1 smlt-virtual-bmac 62:08:05:07:50:01
spbm 1 smlt-peer-system-id 6208.0507.4002
exit


#
# VLAN CONFIGURATION
#

vlan members remove 1 1/8,1/16,1/49,1/53
vlan create 100 type port-mstprstp 0
vlan i-sid 100 2000100
exit
vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
vlan create 4053 type port-mstprstp 1
vlan i-sid 4053 12004053
interface Vlan 4053
ip address 10.1.1.1 255.255.255.248 0
exit


#
# NLS CONFIGURATION
#
mgmt oob
ip address 172.21.133.245/24
ip route 0.0.0.0/0 next-hop 172.21.133.1 weight 300
enable
force-topology-ip
exit
```

```
#
# ISIS SPBM CONFIGURATION
#
router isis
spbm 1
spbm 1 nick-name 0.02.00
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
spbm 1 smlt-virtual-bmac 62:08:05:07:50:01
spbm 1 smlt-peer-system-id 6208.0507.4001
exit


#
# VLAN CONFIGURATION
#

vlan members remove 1 1/8,1/16,1/49,1/53
vlan create 100 type port-mstprstp 0
vlan i-sid 100 2000100
exit

vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
vlan create 4053 type port-mstprstp 1
vlan i-sid 4053 12004053
interface Vlan 4053
ip address 10.1.1.2 255.255.255.248 0
exit


#
# NLS CONFIGURATION
#
mgmt oob
ip address 172.21.133.246/24
ip route 0.0.0.0/0 next-hop 172.21.133.1 weight 300
enable
force-topology-ip
exit
```

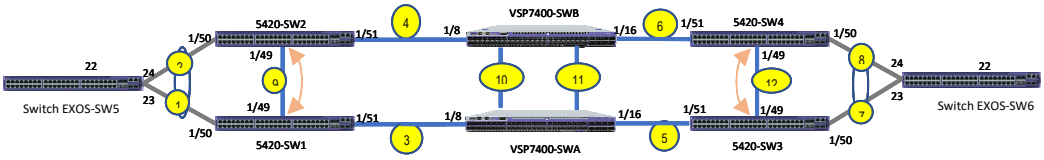
# # VIRTUAL IST CONFIGURATION # virtual-ist peer-ip 10.1.1.2 vlan 4053 # # ISIS CONFIGURATION # router isis sys-name "VSP7400-SWA" is-type l1 system-id 6208.0507.4001 manual-area 49.0000 exit router isis enable	# # VIRTUAL IST CONFIGURATION # virtual-ist peer-ip 10.1.1.1 vlan 4053 # # ISIS CONFIGURATION # router isis sys-name "VSP7400-SWB" is-type l1 system-id 6208.0507.4002 manual-area 49.0000 exit router isis enable

Come prima differenza troviamo nella sezione “CLI CONFIGURATION” troviamo prompt "VSP7400-SWA" e prompt "VSP7400-SWB" che indicano semplicemente il nome assegnato alla macchina che verrà visualizzato sulla riga di comando quando ci si connette tramite ZOC. Troviamo poi spbm 1 smlt-peer-system-id 6208.0507.4002 e spbm 1 smlt-peer-system-id 6208.0507.4001, indica il peer utilizzato nella configurazione del protocollo SMLT, ossia un numero da 12 cifre assegnato alla macchina, infatti se ci troviamo sul VSP7400A, va indicato come peer il system-id del VSP7400B, con il quale viene condiviso l’aggregazione dei collegamenti tramite SMLT. Successivamente possiamo vedere le differenza nell’assegnazione degli indirizzi IP sulle interfacce per la VLAN 4053, ossia ip address 10.1.1.1 255.255.255.248 0 e ip address 10.1.1.2 255.255.255.248 0 e sull’interfaccia OOB, ip address 172.21.133.245/24 e ip address 172.21.133.246/24. Nella sezione “VIRTUAL IST CONFIGURATION” troviamo virtual-ist peer-ip 10.1.1.2 vlan 4053 e virtual-ist peer-ip 10.1.1.1 vlan 4053 che indicano per ciascuna macchina il peer utilizzato per l’alta affidabilità, poiché le due macchine vengono viste a livello logico, come una sola, notiamo infatti che si indica come indirizzo IP quello dell’altra macchina con cui forma il collegamento. Infine abbiamo i nomi assegnati ai dispositivi, sys-name "VSP7400-

SWA" e sys-name "VSP7400-SWB" e i system-id menzionati prima, system-id 6208.0507.4001, system-id 6208.0507.4002.

4.3 **Collegamento dei dispositivi e attivazione SPBM e IS-IS**

In questa fase viene effettuato il collegamento degli switch per la creazione topologica del Fabric Connect e l'attivazione dei protocolli SPBM e IS-IS, due dei protocolli cardine del Fabric:



Il protocollo SPBM[12] rappresenta una delle due versioni del protocollo SPB (Shortest Path Bridging). Quest'ultimo è un protocollo basto sull'IS-IS, descritto fra breve, destinato a rimpiazzare l'STP (Spanning Tree Protocol), esso rappresenta una tecnologia che permette di semplificare la creazione e la configurazione delle reti informatiche in ambito carrier e aziendale soprattutto, fornendo la funzione di instradamento a più percorsi. A differenza del protocollo ST, permette di avere più instradamenti possibili a costo uguale, apportando molti benefici nelle reti a livello 2, consentendo di estenderle, accelerare i tempi di convergenza e aumentare la banda passante, distribuendo il traffico su tutti gli instradamenti possibili. L'SPBM si basa sul concetto di MAC-in-MAC[13], ossia una tecnica che consiste nell'incapsulare l'indirizzo MAC dell'utente finale in quello del fornitore di servizi.
L'IS-IS (Intermediate System to Intermediate System), su cui si basa l'SPB, è un protocollo che permette ai nodi all'interno di un dominio di routing di scambiarsi

informazioni e configurazioni di routing per facilitare le operazioni di instradamento e le relative funzioni. Esso è organizzato in due categorie di funzioni principali:

- funzioni indipendenti dalla sottorete: funzioni indipendenti dal tipo di sottorete che si sta utilizzando (determinano i cammini delle NPDU, ossia dei pacchetti e li gestiscono dinamicamente, provvedono a gestire le risorse utilizzate dagli Intermediate System).

- funzioni dipendenti dalla sottorete: sono funzioni dipendenti dalla sottorete utilizzata (cancellano e stabiliscono dinamicamente i link, inizializzano i data link, determinano le reti vicine,ecc…).

Qui di seguito i comandi per l'attivazione e configurazione dei due protocolli sugli switch 5420M:

```
spbm
spbm ethertype 0x8100
router isis
spbm 1
spbm 1 nick-name 0.10.00
spbm 1 b-vid 4051,4052 primary 4051
vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
router isis
system-id 6208.0507.4010
manual-area 49.0000
sys-name 5420M-SW1
spbm 1 smlt-peer-system-id
6208.0507.4011
vlan create 4053 type port 1
vlan i-sid 4053 12004053
interface vlan 4053
ip address 10.10.1.3/24
virtual-ist peer-ip 10.10.1.4 vlan 4053
router isis
spbm 1 smlt-virtual-bmac
62:08:05:07:50:02
router isis enable
interface gigabitethernet 1/49
isis
isis spbm 1
isis enable
no shutdown
exit
```

riprendiamo i comandi principali tra quelli indicati:

- spbm: abilita effettivamente il protocollo SPBM sulla macchina in questione.

- spbm 1: l'attivazione del protocollo SPBM necessita anche la creazione di un'istanza globale, che viene indicata con u numero compreso tra 1 e 100, in questo caso 1.

- spbm ethertype 0x8100: imposta l'ethertype al valora 0x8100, esso rappresenta un campo a due ottetti del frame ethernet che indica il protocollo incapsulato nel payload del pacchetto (0x8100 è il valore di default ed indica il protocollo 802.1Q).

- spbm 1 nick-name 0.10.00: associa all'istanza dell'spbm il nick-name dello switch, ossia 0.10.00.

- spbm 1 b-vid 4051,4052 primary 4051: associa all'istanza globale dell'SPBM, la VLAN di backbone, se ne possono appunto configurare al massimo 2 e bisogna indicare quella primaria, in questo caso la 4051.

- vlan create 4051 type spbm-bvlan: crea una vlan adibita alle comunicazioni necessarie per funzionare per il protocollo SPBM e le assegna il tag 4051.

- vlan create 4052 type spbm-bvlan: stessa cosa, cambia solo il tag.

- system-id 6208.0507.4010: imposta il parametro system-id al valore indicato, necessario all'attivazione del protocollo SMLT.

- spbm 1 smlt-peer-system-id 6208.0507.4011: associa il system-id del peer con il quale lo switch costituisce la coppia sulla quale viene attivato il protocollo SMLT, perciò sull'altro switch il comando sarà identico solo che il system-id sarà 6208.0507.4010.

Nota: il protocollo SMLT (Split MultiLink Trunk)[14] è una variante dell'MLT, ossia una tecnologia di aggregazione dei collegamenti che consente di raggruppare diversi collegamenti ethernet per fornire, come in questo caso, tolleranza gli errori. Esso viene utilizzato per fornire ulteriore ridondanza alla rete, distribuendo i collegamenti su più linee appunto.

- vlan create 4053 type port 1: crea la VLAN 4053 basata sulle porte e la associa all'ID 1.

- vlan i-sid 4053 12004053: associa la VLAN 4053 all'I-SID (Service Instance ID, esso è un valore che identifica univocamente una VSN del Fabric Connect). Nei comandi successivi si assegna un indirizzo all'interfaccia per la VLAN 4053.

- isis: tale comando applicato ad una porta dello switch, come indicato sopra abilita il protocollo IS-IS e ne crea un'interfaccia sulla porta indicata.

- isis spbm 1: abilita l'istanza dell'SPBM sull'interfaccia creata per l'ISIS (sempre applicato ad una porta dello switch).

Tale configurazione viene chiaramente replicata sugli altri switch variando alcuni parametri e comandi, ma la struttura è simile (inoltre gli switch di edge, ossia SW1 e SW6 sono dotati di EXOS invece che VOSS, quindi la sintassi sarà leggermente diversa per alcuni comandi).

L'ultima parte della configurazione riguarda l'attivazione del protocollo LAG LACP[15] sui due collegamenti verso gli switch di edge. I LAG (Link AGregation) sono dei collegamenti che consentono di aggregare più collegamenti in un unico collegamento fornendo alcuni vantaggi come l'aumento della larghezza di banda, miglior utilizzo delle risorse fisiche a disposizione,ecc.. . Esistono due tipi di LAG, quelli statici e quelli dinamici, quelli statici vengono configurati manualmente mentre quelli dinamici si basano sul protocollo LACP (Link Aggregation Control Protocol). Esso è definito dallo standard IEEE 802.3ad e abilita i dispositivi ad inviare tra loro informazioni che consentono la gestione del LAG, che viene comunque configurato manualmente una prima volta, ma successivamente fornisce alcuni vantaggi, ossia permette ad esempio di disabilitare automaticamente collegamenti membri del LAG quando inattivi.
Su entrambi i dispositivi configurati velocità, tipo di trasmissione, controllo di flusso, ecc.., devono essere impostati in maniera simmetrica sui dispositivi sui quali il LAG viene configurato. Qui di seguito la configurazione:

```
interface GigabitEthernet 1/50
default-vlan-id 100
no shutdown
lacp key 150 aggregation enable timeout-time short
lacp enable
no spanning-tree mstp  force-port-state enable
exit
```

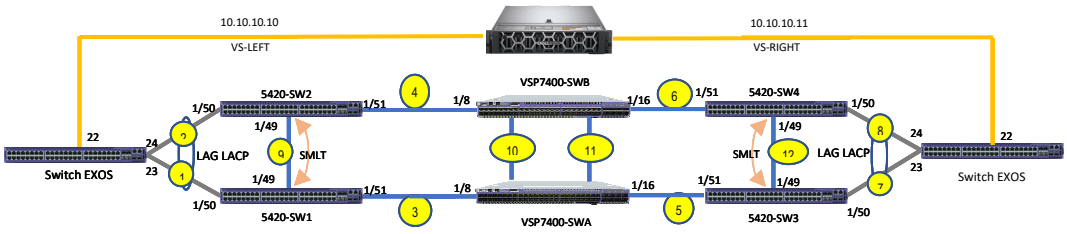
si entra nella porta in questione, ossia la 1/50 come si può anche vedere nell'immagine della rete e si definisce una chiave, ossia 150 per identificare il LAG, poiché si può ovviamente crearne più di uno sullo switch e poi lo si abilita.

Capitolo 5

Test

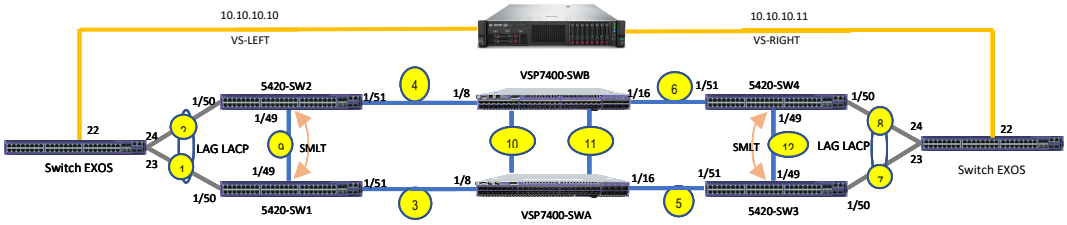
5.1 Test tramite ping

Una volta che le macchine sono state configurate, si è proceduto con i test di livello 2, demandando i test di livello 3 ad una fase di progetto successiva alla conclusione del tirocinio. A riprova che la configurazione delle macchine è stata eseguita correttamente, collegandoci ai due switch di edge SW5 e SW6 tramite due PC configurati con due indirizzi appartenenti alla stessa rete, si è verificata la comunicazione a livello 2, sfruttando il comando di ping. I PC utilizzati sono stati in realtà due macchine virtuali con Windows Server 2012, ospitate dall'ipervisore VMWare:

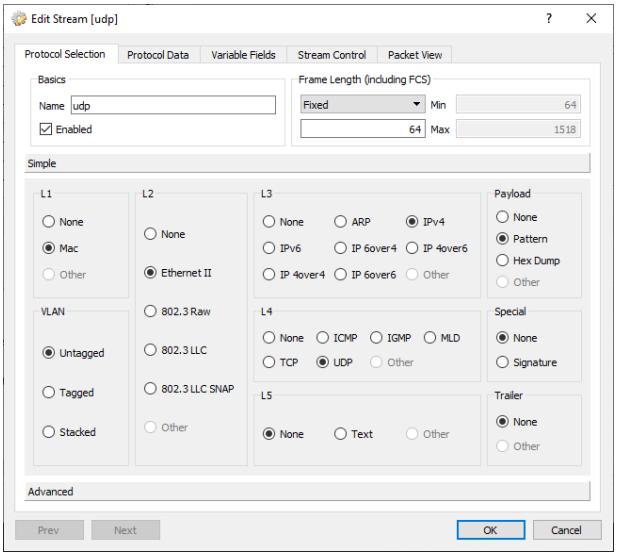


come si può notare dalla figura, le due macchine virtuali sono appunto state gestite dall'ipervisore VMWare, installato su un server Dell PowerEdge. VS-LEFT e VS-RIGHT indicano due schede di rete virtuali, attestate a due virtual switch diversi, a conferma che la configurazione è stata eseguita in maniera corretta, pingando dall'interfaccia VS-LEFT, ossia da 10.10.10.10/24, verso l'interfaccia VS-RIGHT si è ottenuta risposta da 10.10.10.11/24 e viceversa.

5.2 **Test tramite il tool “Ostinato”**

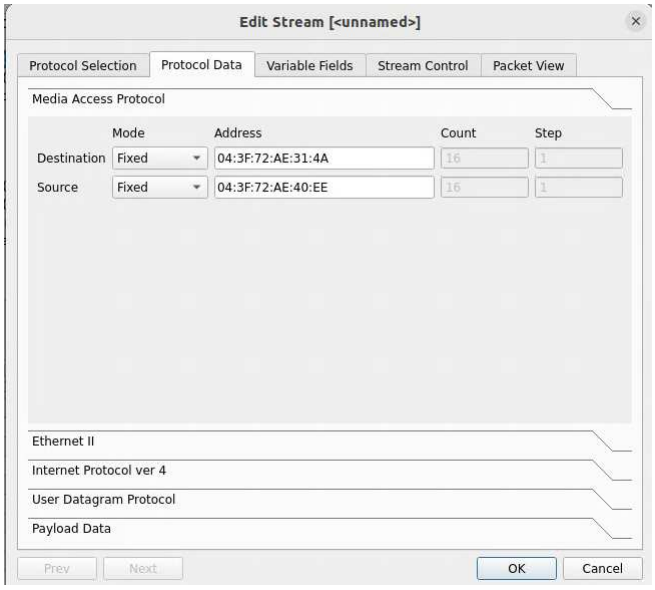


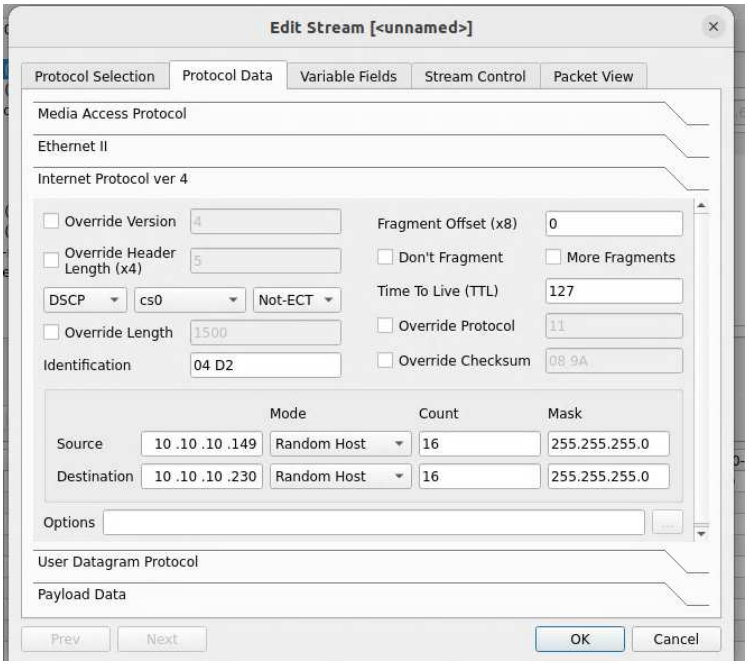
Con lo strumento Ostinato è possibile creare traffico di rete da un’interfaccia verso un’altra, potendo scegliere la struttura e la dimensione dei pacchetti generati ottenendo così una grande varietà di configurazioni disponibili. Ostinato viene installato su un HPE ProLiant dotato di Ubuntu v22.04. L’idea è di sostituire il server Dell PowerStation con la macchina sopra menzionata e generare traffico da un’interfaccia (VS-LEFT) verso l’altra (VS-RIGHT) e viceversa. In un primo momento si invia traffico da una interfaccia verso l’altra e si verifica che il numero di pacchetti persi assuma un valore tollerabile per una buona efficienza e un buon funzionamento della rete. In un secondo momento, si genera nuovamente traffico, disabilitando alcuni dei collegamenti numerati in figura, al fine di verificare la robustezza della rete, ossia se in presenza di situazioni anomale come il down momentaneo di alcuni collegamenti, la rete riesca comunque a garantire un corretto funzionamento e dei bassi tempi di assestamento. Il software supporta varie opzioni, ad esempio quella di selezionare i protocolli da utilizzare nella comunicazione, come nell’esempio illustrato qui di seguito:



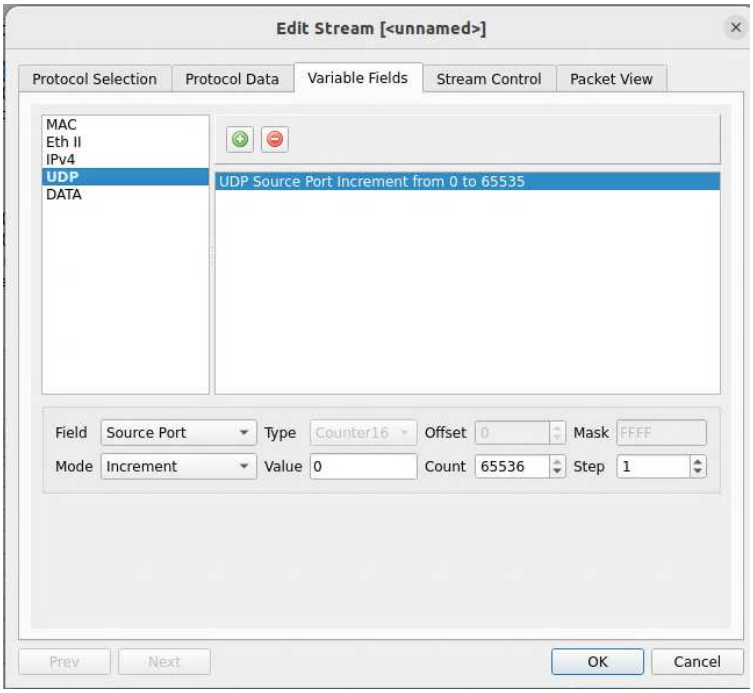
Si tratta di una schermata di Ostinato che mostra la selezione dei protocolli per i test svolti.

Successivamente nella sezione “Protocol Data” possiamo modificare a piacimento i dati relativi ai protocolli:





Nella sezione “Variable Fields” invece possiamo inserire dei valori incrementali per alcuni valori, come il numero delle porte:



I test intensivi di affidabilità eseguiti inviando pacchetti da un'interfaccia verso l'altra in realtà hanno evidenziato che su 8 milioni di frame da 512 byte l'uno, inviati da un'interfaccia verso l'altra e viceversa si è contabilizzata una perdita compresa tra gli 8000 e i 40.000 pacchetti, corrispondente un tasso di perdita contenuto tra lo 0.1 e lo 0.5 per mille, ritenuto tollerabile dai tecnici.
Anche inviando un treno più ridotto di frame si è misurato comunque un tasso di perdita simile, sempre inferiore o uguale allo 0.5%. Esperimenti eseguiti con un treno di 1 milione di frame inviato, sempre della stessa dimensione, si sono contati in diversi esperimenti un numero di frame persi compreso tra 0 e 5.000.

Più interessanti risultano invece i test eseguiti disabilitando alcuni dei collegamenti numerati in figura mentre si genera traffico da un'interfaccia all'altra e viceversa, in quanto la rete si trova a dover gestire una situazione anomala e ci si aspetta che ci riesca e anche in tempi abbastanza brevi.
Questi test vengono eseguiti sugli switch SW1, SW2, SW3, SW4, SW5 e SW6 disabilitando e riabilitando i collegamenti tra le coppie di switch (1/49) e quelli interni, ossia quelli uscenti dalle interfacce 1/51. Nelle tabelle che vengono riportate, i flussi di traffico si leggono in diagonale, in quanto il valore presente nella prima colonna e seconda riga indica i pacchetti ricevuti dall'interfaccia VS-LEFT, il valore presente nella terza riga e seconda colonna invece rappresenta i pacchetti inviati da VS-RIGHT a VS-LEFT, un discorso analogo vale per il flusso di dati opposto, qui di seguito riportiamo i risultati per ogni test:

- SW1:

Run 1 (shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.970.772	29.983.970
30.000.000	30.000.001
0	0

Run 2 (no shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.984.421	29.989.982
30.000.000	30.000.000

Run 3 (shutdown Gigabit Ethernet 1/49)

Port 0-1	Port 0-2
29.988.567	29.988.616
30.000.002	30.000.002

Run 4 (no shutdown Gigabit Ethernet 1/49)

Port 0-1	Port 0-2
30.000.007	30.000.006
30.000.000	30.000.000

- SW2:

Run 1 (shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.980.760	29.982.180
30.000.000	30.000.000

Run 2 (no shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.993.264	29.988.407
30.000.000	30.000.000

- SW3:

Run 1 (shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.980.516	29.981.601
30.000.000	30.000.000

Run 2 (no shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.998.617	29.995.606
30.000.000	30.000.000

Run 3 (shutdown Gigabit Ethernet 1/49)

Port 0-1	Port 0-2
30.000.006	30.000.006
30.000.000	30.000.000

Run 4 (no shutdown Gigabit Ethernet 1/49)

Port 0-1	Port 0-2
30.000.006	30.000.006
30.000.000	30.000.000

- SW4:

Run 1 (shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.986.080	29.990.530
30.000.000	30.000.000

Run 2 (no shutdown Gigabit Ethernet 1/51)

Port 0-1	Port 0-2
29.987.608	29.984.723
30.000.000	30.000.000

- SW5:

Run 1 (shutdown GigabitEthernet 1/50)

Port 0-1	Port 0-2
29.997.699	29.975.342
30.000.000	30.000.000

Run 2 (no shutdown GigabitEthernet 1/50)

Port 0-1	Port 0-2
29.922.319	29.931.467
30.000.000	30.000.000

Run 3(shutdown GigabitEthernet 1/51)

Port 0-1	Port 0-2
29.984.580	29.830.473
30.000.002	30.000.002

Run 4 (no shutdown GigabitEthernet 1/51)

Port 0-1	Port 0-2
29.913.951	29.907.966
30.000.000	30.000.000

- SW6:

Run 1(shutdown GigabitEthernet 1/50)

Port 0-1	Port 0-2
29.979.729	29.997.219
30.000.000	30.000.000

Run 2(no shutdown GigabitEthernet 1/50)

Port 0-1	Port 0-2
29.916.556	29.899.941
30.000.000	30.000.000

Run 3(shutdown GigabitEthernet 1/51)

Port 0-1	Port 0-2
29.915.517	29.997.151
30.000.000	30.000.000

Run 4(no shutdown GigabitEthernet 1/51)

Port 0-1	Port 0-2
29.937.548	29.931.253
30.000.000	30.000.000

Capitolo 6

Risultati e conclusioni

6.1 Risultati ottenuti

I test effettuati tramite il comando *ping* sono andati a buon fine, in quanto inviando richieste "Echo" dall'indirizzo 10.10.10.10/24 a 10.10.10.11/24 e viceversa si ottengono le rispettive"Echo Response". Sono stati effettuati più test con treni di richieste Echo, e sono stati poi replicati scollegando i collegamenti ai lati verso le due macchine virtuali: il risultato è quello aspettato, ossia si ottiene risposta fino a quando non si disabilitano i collegamenti. Questo significa che la connettività ha rispecchiato le configurazioni attese in merito alla comunicazione a livello 2. I test eseguiti con Ostinato hanno dato anch'essi risultati coerenti con quanto ci si aspettava, ossia anche con grandi quantità di dati trasmesse ad alta velocità, in situazioni di normale funzionamento, si ha in ricezione praticamente il 100% dei dati trasmessi (si perde un numero di pacchetti compreso tra lo 0,1% e 0,5% del totale). Si avrà sempre una minima perdita dovuta all'occasionale overflow dei buffer, trattandosi di test intensivi a saturazione di banda.
Invece i test eseguiti disabilitando alcuni collegamenti, hanno i risultati riportati a fine del precedente capitolo, vengono inviati 30.000.000 di pacchetti e in ricezione, si ha una perdita compresa tra un minimo di circa 0 e 170.000 pacchetti, ossia compreso tra lo 0% e il 5,7% del totale. Il valore 170.000 si presenta un'unica volta nei test, potrebbe essere quindi un dato limitato al caso, poiché nel resto dei test non si supera il valore di 100.000 pacchetti persi. Qui di seguito vengono riportate due tabelle contenenti i risultati ottenuti tramite Ostinato e indicati nel precedente capitolo:

SW1	IN	OUT	PERSI
Run 1	29970772	30000000	29228
Run 2	29984421	30000000	15579
Run 3	29988567	30000000	11433
Run 4	30000000	30000000	0
SW2	IN	OUT	PERSI
Run 1	29980760	30000000	19240
Run 2	29993264	30000000	6736
SW3	IN	OUT	PERSI
Run 1	29980516	30000000	19484
Run 2	29998617	30000000	1383
Run 3	30000000	30000000	0
Run 4	30000000	30000000	0
SW4	IN	OUT	PERSI
Run 1	29986080	30000000	13920
Run 2	29987608	30000000	12392
SW5	IN	OUT	PERSI
Run 1	29997699	30000000	2301
Run 2	29922319	30000000	77681
Run 3	29984580	30000000	15420
Run 4	29913951	30000000	86049
SW6	IN	OUT	PERSI
Run 1	29979729	30000000	20271
Run 2	29916556	30000000	83444
Run 3	29915517	30000000	84483
Run 4	29937548	30000000	62452
VSP7400B	IN	OUT	PERSI
Run 1	29659838	30000000	340162
Run 2	30000000	30000000	0

SW1	IN	OUT	PERSI
Run 1	29983970	30000000	16030
Run 2	29989982	30000000	10018
Run 3	29988616	30000000	11384
Run 4	30000000	30000000	0
SW2	IN	OUT	PERSI
Run 1	29982180	30000000	17820
Run 2	29988407	30000000	11593
SW3	IN	OUT	PERSI
Run 1	29981601	30000000	18399
Run 2	29995606	30000000	4394
Run 3	30000000	30000000	0
Run 4	30000000	30000000	0
SW4	IN	OUT	PERSI
Run 1	29990530	30000000	9470
Run 2	29984723	30000000	15277
SW5	IN	OUT	PERSI
Run 1	29975342	30000000	24658
Run 2	29931467	30000000	68533
Run 3	29830473	30000000	169527
Run 4	29907966	30000000	92034
SW6	IN	OUT	PERSI
Run 1	29997219	30000000	2781
Run 2	29899941	30000000	100059
Run 3	29997151	30000000	2849
Run 4	29931253	30000000	68747
VSP7400B	IN	OUT	PERSI
Run 1	30000000	30000000	0
Run 2	30000000	30000000	0

La tabella di sinistra rappresenta il flusso di dati con origine l'interfaccia VS-LEFT e destinazione VS-RIGHT e viceversa per quella di destra. Ogni run associata alla macchina rappresenta una rilevazione del traffico dati effettuata su una porta, attivandola o disattivandola, ripetendo questa procedura per ciascuno dei due flussi e in maniera tale da testare tutti i collegamenti, in totale 11, infatti per ogni flusso abbiamo 22 run. Come si può vedere dalle tabelle non sono stati effettuati test sul VSP7400A poiché avremmo ottenuto dati ridondanti siccome i collegamenti ad esso associati vengono inglobati dai test effettuati su SW1 e SW3.

6.2 **Obiettivi raggiunti e conclusioni**

Gli obiettivi prefissati sono stati raggiunti, anche se successivamente ai test di livello 2 eseguiti sulla rete, andrebbe implementato e configurato sui dispositivi, mentre il routing di livello 3, non è rientrato nell'ambito del progetto.

La rete è stata messa in funzione secondo le specifiche fornite e si è arrivati ad ottenere una corretta configurazione del Fabric Connect avendo così una comunicazione base di livello 2, i test effettuati, hanno inoltre dimostrato la robustezza e l'affidabilità dei collegamenti e degli algoritmi di bilanciamento del traffico, che tramite i test di carico, effettuati con il tool Ostinato, hanno dato prova della solidità fisica e strutturale della rete in questione. Ciò conferma quindi la validità della tecnologia Fabric Connect come soluzione alle reti aziendali che necessitano di una rete affidabile, veloce e relativamente semplice da configurare o modificare.

Bibliografia

[1] *Fabric Connect e Fabric Attach:*
https://www.extremenetworks.com/

[2] *LLDP:*
https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

[3] *Switch di edge:*
https://it.theastrologypage.com/edge-switch

[4] *EXOS:*
https://en.wikipedia.org/wiki/ExtremeXOS

[5] *Switch di core:*
https://www.fibermall.com/blog/aggregation-switch.htm

[6] *Specifiche Switch Extreme Networks:*
https://www.extremenetworks.com/

[7] *Fibre e connettori SPF:*
https://www.blackbox.it/it-it/page/45246/Informazioni/Risorse-Tecnologiche/Spiegazioni-Black-Box/lan/SFP-e-QSFP-Che-differenza-c-e

[8] *Specifiche HPE ProLiant DL560 Gen10:*
https://buy.hpe.com/it/it/servers/proliant-dl-servers/proliant-dl500-servers/proliant-dl560-server/server-hpe-proliant-dl560-gen10/p/1010026837

[9] *Specifiche Dell PowerEdge R740xd:*
https://www.dell.com/it-it/shop/enterprise-products/server-2ru-r740xd-intel/spd/poweredge-r740xd

[10] *SNMP:*
https://it.wikipedia.org/wiki/Simple_Network_Management_Protocol

[11] *NTP:*
https://it.wikipedia.org/wiki/Network_Time_Protocol

[12] *SPBM:*
https://it.wikipedia.org/wiki/IEEE_802.1aq

http://blog.reissromoli.com/2017/07/il-livello-2-ne-abbiamo-realmente.html

[13] *MAC-IN-MAC:*
https://www.h3c.com/EN/aspx/WebCommon/SystemError.aspx?aspxerrorpath=/en/Support/Resource_Center/HK/Switches/H3C_S9500E/H3C_S9500E_Series_Switches/Technical_Documents/Configure___Deploy/Configuration_Guides/H3C_S9500E_CG-Release1728-6W170/04/201211/761546_294551_0.htm#:~:text=MAC%2Din%2DMAC%20is%20a,for%20Ethernet%20and%20secures%20services.

[14] *SMLT:*
https://it.wikipedia.org/wiki/SMLT

[15] *LAG LLACP:*
https://www.dell.com/support/kbdoc/it-it/000121681/come-creare-e-gestire-l-aggregazione-dei-collegamenti-lag-su-uno-switch-dell-networking-serie-x

[16] *Collapsed backbone:*
https://slideplayer.com/slide/5802281/

[17] *Ostinato:*
https://ostinato.org/