UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI **INGEGNERIA**

Corso di Laurea triennale INGEGNERIA INFORMATICA E DELL'AUTOMAZIONE

CONFIGURAZIONE DI RETI IN AMBIENTI INDUSTRIALI

NETWORK CONFIGURATIONS IN INDUSTRIAL ENVIRONMENTS

Relatore:

Prof. **GAMBI ENNIO**

Correlatore:

Ing. **DE SANTIS ADELMO**

Tesi di Laurea di:

ACCATTOLI ELEONORA

A.A. **2019** / **2020**

INDICE

INTRODUZIONE

Per l'innegabile rilevanza che hanno le reti di telecomunicazione in questo sistema, tenendo in considerazione anche il periodo storico in cui ci troviamo, in questo lavoro è stato approfondito il tema delle configurazioni di reti.

In dettaglio, ho centrato la mia tesi sulla configurazione di una rete aziendale, mostrando come anche sedi dislocate fisicamente possano comunicare in modo efficiente ed affidabile.

Nello specifico, verranno "messe a disposizione" le configurazioni necessarie affinché si possa realizzare quanto detto, con l'utilizzo di differenti protocolli, atti ad incrementare la velocità, la ridondanza e la sicurezza nei collegamenti e nelle connessioni, nel caso in cui si verificassero guasti o malfunzionamenti.

Infine, essendo il sistema informativo in continua evoluzione, è stata predisposta e configurata la rete con una nuova versione del protocollo di rete IP, l'IPv6, i cui indirizzi offrono dei miglioramenti sia a livello di disponibilità di hosts allocabili sia a livello di sicurezza.

OBIETTIVI

L’obiettivo di questo progetto è quindi, la creazione e la configurazione di una rete aziendale, tale da permettere la comunicazione tra gli utenti che vi si collegheranno, anche se aventi versioni differenti dell’Internet Protocol.

eNSP

Figura 1 Logo eNSP

eNSP è una piattaforma grafica di simulazione reti sviluppata da Huawei.

Essa fornisce mediante GUI, un laboratorio virtuale, per configurare e testare i dispositivi Huawei e le future reti, consentendo di sperimentare le principali tecniche di routing e switching.

eNSP è anche utilizzato per risolvere eventuali problemi di rete in aziende così da realizzare reti ICT sempre più innovative ed affidabili.

Grazie all'Università Politecnica delle Marche in collaborazione con Huawei, è stato possibile utilizzare questa piattaforma.

Una volta installato, all'apertura verrà visualizzata una schermata di questo genere, dove sarà possibile inserire i dispositivi di cui si ha bisogno per costruire la topologia, quali routers, switches, end devices, collegamenti fisici ma anche firewall e WLAN.

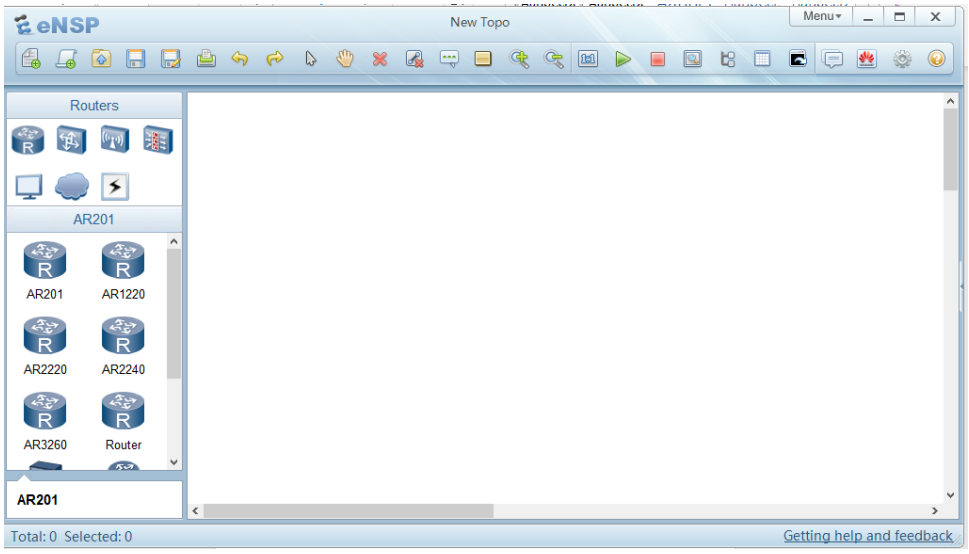


Figura 2 Schermata iniziale eNSP

Inoltre, per avere una visione completa dei programmi utilizzati, eNSP "lavora" in concomitanza con Virtualbox e Wireshark.

Figura 3 Logo VirtualBox

Virtualbox è un programma open source che permette la virtualizzazione per uso aziendale e domestico.

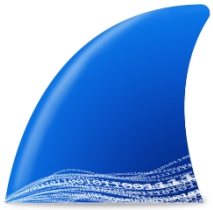


Figura 4 Logo WireShark

Wireshark invece è un software utilizzato per analizzare il traffico di rete. Partendo da un progetto eNSP, è possibile analizzare il traffico passante per un'interfaccia fisica, cliccando con il tasto destro del mouse, sopra il dispositivo di nostro interesse e selezionando tra le varie opzioni CaptureData e scegliendo l'interfaccia da analizzare.

Nel seguito verranno descritti gli elementi utilizzati per ottenere la configurazione finale.

TOPOLOGIA LOGICA E FISICA

La topologia di rete logica da realizzare è la seguente:

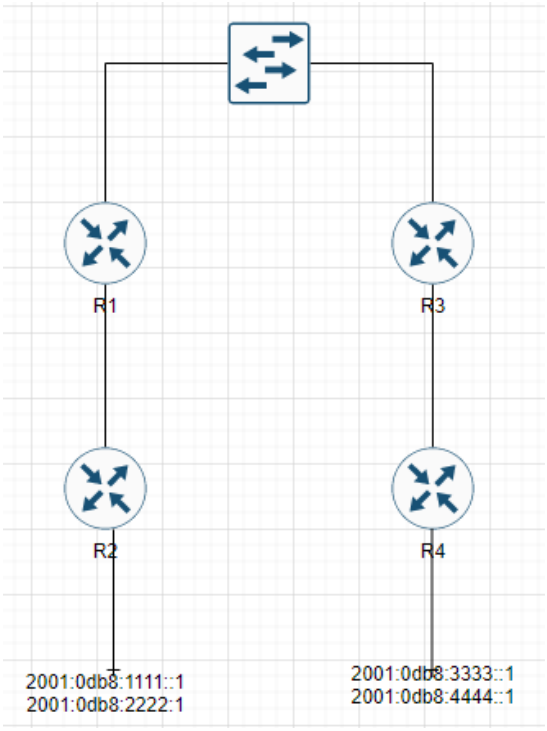


Figura 5 Topologia Logica

Deve essere creata basandosi sulla topologia fisica in figura sottostante:

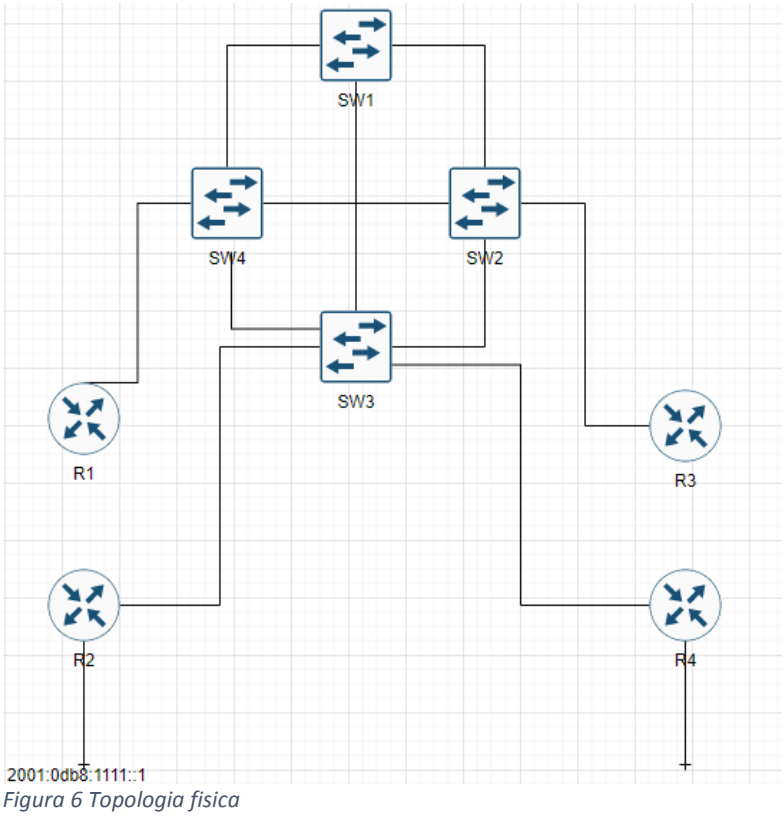


Figura 6 Topologia fisica

È stato richiesto di far comunicare i dispositivi della rete, anche se hanno versioni di protocollo di rete differenti – IPv4 e IPv6.

Sono state date delle direttive specifiche per la configurazione della rete, quali l'impostazione corretta degli switches con le relative VLAN, la configurazione di SW1 come primary root e SW3 come secondary root e l'implementazione di RSTP e LACP nel collegamento tra SW2 e SW4.

Infine, è stata richiesta la creazione di un tunnel GRE tra il router 2 e 4, nei quali fa capo la rete IPv6, per poi eseguire OSPFv3 su di essi.

DISPOSITIVI UTILIZZATI

Per realizzare la topologia, vengono utilizzati degli switches, dei routers e dei collegamenti Ethernet di tipo Gigabit.

SWITCH

Gli switches sono apparati di livello 2, che si occupano di commutare i frame. Permettono la comunicazione tra dispositivi della stessa LAN, facilitando le connessioni all'interno di aziende o il collegamento fra più filiali.

Ci sono principalmente tre modalità di funzionamento dello switch e sono:

- **Store and forward:** lo switch riceve completamente tutti i bit del frame e li immagazzina prima di inoltrarli, verificando l'FCS, riportando però un rallentamento nella trasmissione. Viene principalmente utilizzato per le connessioni che richiedono una maggior sicurezza.
- **Cut-through:** lo switch inoltra il frame appena possibile, rendendo il trasferimento più veloce, ma non controllando eventuali errori.
- **Fragment-free:** lo switch inoltra il frame dopo che ha ricevuto i primi 64 byte di esso, evitando quindi di inviare frame corrotti. Viene utilizzata soprattutto per le connessioni streaming.

La modalità di switching non può essere scelta dall'utente.

In tutti e tre i casi, lo switch, ogni qualvolta veda arrivare un frame, registrerà nella sua tabella dei MAC Address, gli indirizzi MAC dei dispositivi.

Figura 7 Switch S5700

In questo progetto sono stati utilizzati degli switches Huawei, modello S5700. Sono switches GE – GigabitEthernet progettati per

fornire accesso a larghezza di banda elevata e aggregazione multi-servizio Ethernet, permettendo una ampia capacità di commutazione, alta affidabilità e sicurezza. Supporta inoltre, l'autenticazione 802.1X, ARP e può fornire dinamicamente criteri per gli utenti quali VLAN, ACL etc.

Tra i tanti vantaggi, si può notare anche il supporto per IPv4-IPv6, che permette l'utilizzo di protocolli di routing come OSPFv3.

Per questi motivi e per il maggior numero di interfacce disponibili è stato scelto come dispositivo di livello 2.

ROUTER

Figura 8 Router AR1220

I routers sono apparati di livello 3, che permettono di instradare pacchetti tra hosts dislocati fisicamente.

I routers utilizzati sono gli AR1220 appartenenti alla serie AR1200, specializzati su piccola scala, con al massimo 50 utenti collegabili contemporaneamente. Offrono comunicazioni affidabili, scalabili e sicure grazie alle funzioni di protezione complete, rilevamento guasti e ai collegamenti di backup. Hanno larghezza di banda flessibile per traffico dati e voce ed interfacce sia via cavo e su fibra con velocità fino a 1 Gibt/s.

Sono stati scelti questi routers, perché uniscono tutte le funzioni di routing, switching, voce, sicurezza e WAN in un'unica soluzione, soddisfacente i requisiti diversificati delle aziende e semplificando le attività di gestione e manutenzione.

Alla ricezione di un frame, il router controllerà la correttezza dell'FCS ricevuto; se esatto, verificherà se il destination address ricevuto è associato ad un'interfaccia o se è un indirizzo di broadcast; in entrambi i casi, procederà con analizzare il

frame, effettuando il decapsulamento. Quindi verrà eliminato l'header e l'FCS e poi verrà inviato il campo data al livello 3, il cui tipo di L3 è definito all'interno del campo Type.

Per poter inoltrare il pacchetto, il router dovrà verificare la presenza dell'indirizzo di destinazione, all'interno della sua IP Routing-Table, una tabella contenente la "conoscenza" riguardo la raggiungibilità degli spazi di indirizzi associati ad esso. Per verificare la presenza dell'indirizzo di destinazione, il router effettuerà un confronto AND tra l'indirizzo contenuto nel campo "destination address" dell'header IP e quelli già presenti nella sua tabella. Verrà selezionato, utilizzando il longest match, l'indirizzo con più bit in comune e verrà inoltrato il pacchetto sull'interfaccia corrispondente all'indirizzo scelto. Per popolare la routing-table, è necessario conoscere l'IP di destinazione, il next hop e l'interfaccia di destinazione.

La popolazione delle tabelle di routing può avvenire in modo statico o dinamico. Nel primo caso è l'amministratore ad inserire le rotte per arrivare a destinazione. Nel secondo caso, invece, la rotta viene scelta mediante l'utilizzo di protocolli specifici, come OSPF.

Ad ogni interfaccia del router verrà assegnato un indirizzo IP. Un indirizzo IP è un codice numerico, tipicamente espresso in "dotted decimal notation" che consente di individuare la posizione di un nodo nella rete. Gli indirizzi IP possono essere assegnati in modo autonomo o in modo dinamico, nel primo caso, sarà l'amministratore a scegliere, in base alle esigenze, quale classe di indirizzi utilizzare e li assegnerà ai dispositivi. Nel secondo caso invece, sarà il DHCP – Dynamic Host Configuration Protocol ad assegnare gli indirizzi in automatico, in base alla disponibilità.

IPv4

Ogni indirizzo IP è formato da quattro numeri separati da punti e sono composti da due campi, il campo Network ed il campo Host, di grandezza variabile, in base alla classe di appartenenza, ma la cui somma è sempre pari a 32 bit.

Gli indirizzi IP sono raggruppabili in 5 classi:

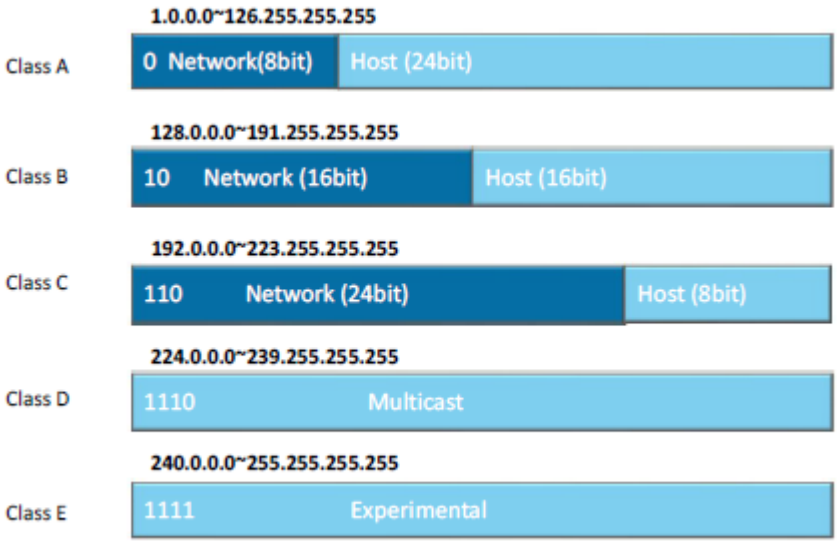


Figura 9 Classi di indirizzi

La classe degli indirizzi determina il numero di reti disponibili ed il numero di hosts collegabili con valore pari a 2^H-2, dove H indica i bit del campo Host.

La classe A viene impiegata nelle grandi aziende ed ha a disposizione 126 reti, con 16777214 hosts per rete; la classe B è impiegata nelle medie aziende, mettendo a disposizione 16384 reti con 65534 hots per rete; mentre la classe C è adoperata per ambienti piccoli quali casa, uffici, mette a disposizione 2097152 reti con 254 host collegabili per rete. Di tutti gli indirizzi utilizzabili, per ogni rete, il primo e l'ultimo di essi non sono assegnabili, in quanto riguardano rispettivamente il network address ed il broadcast address; il primo ha tutto il campo host a 0 e rappresenta lo spazio di indirizzi che si sta considerando,

mentre il secondo ha tutto il campo host a 1 ed è utilizzato per inviare pacchetti a tutti gli hosts appartenenti allo spazio.

Ad ogni indirizzo IP è sempre associata una subnet mask, ovvero una sequenza di bit posti al valore 1 in corrispondenza dei bit dedicati al campo Network, mentre i bit che corrispondono al campo Host sono posti a 0. La subnet mask permette di identificare la rete di appartenenza di un indirizzo, effettuando un AND tra l'indirizzo IP e la sua subnet.

Prendendo ad esempio un indirizzo di classe A, come 10.0.0.1, dalla schematizzazione sopra, si sa che gli indirizzi di questa classe hanno 8 bits per il campo network e 24 bits per il campo host, di conseguenza il suo network address sarà 10.0.0.0 mentre il suo broadcast address sarà 10.255.255.255. Gli indirizzi di questa classe avranno subnet mask pari a 255.0.0.0.

IPv6

Tutto ciò che è stato detto finora riguarda l'indirizzamento IPv4, ma con il proseguire degli anni, è stato studiato ed introdotto un nuovo protocollo di rete, IPv6, in grado di superare il limite del numero di indirizzi utilizzabili in IPv4.

Di fatti, a differenza dei precedenti, gli indirizzi IPv6 hanno lunghezza pari a 128 bit o 16 byte. Il numero di indirizzi disponibili è 10^{28} volte più grande del numero di indirizzi IPv4. Il formato è così suddiviso: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx e nel caso di presenza di più bit iniziali a 0 consecutivi, si possono omettere, sostituendoli con i "::". I primi 64 bit sono utilizzati per il routing ed indicano il prefisso della rete, mentre gli ultimi 64 bit sono definiti Interface ID, ovvero l'identificativo di un host.

Gli indirizzi IPv6 si possono distinguere in tre gruppi:

1. **Unicast:** specificano un'interfaccia singola, il pacchetto passerà da un host sorgente ad un host destinatario e si classificano in:
    a. **Global unicast:** paragonabili agli indirizzi IPv4 pubblici e sono gestiti a livello globale da IANA.
    b. **Unique local:** come gli indirizzi IPv4 privati
    c. **Link local:** indirizzi autoconfigurati, utilizzati nelle LAN.
2. **Multicast:** I pacchetti inviati ad un indirizzo multicast, vengono copiati e distribuiti ad ogni membro del gruppo.
    a. **Solicited Node Multicast:** utilizzati per rispondere ad eventuali richieste.
3. **Anycast:** specifica una serie di interfacce, che condividono tutte un singolo indirizzo. Un pacchetto inviato ad un indirizzo anycast è recapitato solo al membro più vicino del gruppo anycast.

UNICAST

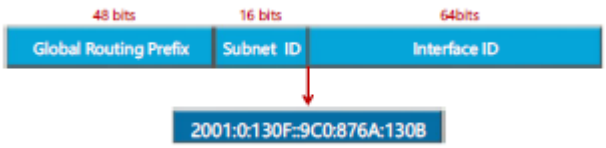


Figura 10 Formato indirzzi Unicast

Gli indirizzi Unicast sono formati da tre campi:

1. **Global Routing Prefix:** è assimilabile alla sezione Network di IPv4.
2. **Subnet ID:** corrisponde alla subnet di IPv4; cambiano però le dimensioni, in quanto si ha una dimensione fissa del campo Interface ID pari a 64 bits, rendendo disponibili 2^{64}-2 hosts e n bit per il subnetting, con n=128-64-bit campo network,

dove 128 è la lunghezza totale e 64 i bits fissi dell'Interface.

3. **Interface ID:** è l'identificativo dell'host.

UNIQUE LOCAL

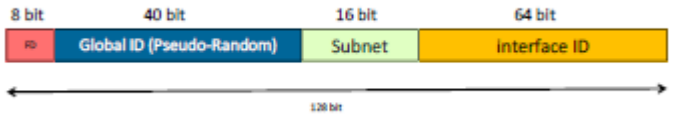


Figura 11 Formato indirizzi Unique Local

Gli indirizzi unique local sono privati e non sono registrati dallo IANA. Tutti gli indirizzi iniziano con FD seguiti poi da un global ID, pseudo-random.

LINK LOCAL

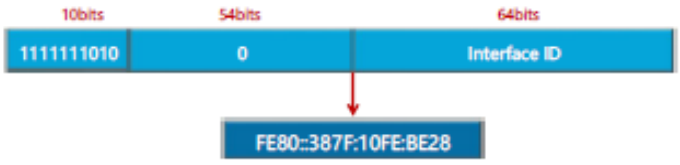
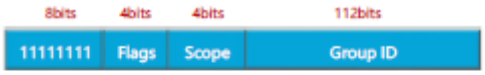


Figura 12 Formato indirizzi Link Local

Questa tipologia di indirizzi è la più utilizzata, vengono utilizzati per veicolare i protocolli di routing e le informazioni che non necessitano di un indirizzo con validità globale.

Hanno però un vincolo, ovvero i primi 10 bit, sono impostati al valore FE80 o 1111111010 e sono seguiti da 54 bits impostati a 0; questo perché essendo utilizzati nelle reti LAN, non prevedono l'utilizzo di sottoreti.

MULTICAST



Address Range	Description
FF02::1	All Nodes Addresses (Link Local)
FF02::2	All Routers Addresses (Link Local)

Figura 13 Formato indirizzi Multicast e address range del campo Scope.

Sono gli indirizzi sostitutivi degli indirizzi BROADCAST IPv4 e sono definiti su RFC4291.

Hanno i primi 8 bits standard, impostati tutti a 1, 4 bits del campo Flags utili ad identificare la presenza di indirizzi Well-Know o assegnati temporaneamente.

Il campo Scope, sempre di 4 bits, definisce un numero che identifica l'ambito dell'indirizzo multicast o meglio, il gruppo di dispositivi a cui si fa riferimento e può essere, o tutti i nodi, indicato con FF02::1 o tutti i routers, indicato con FF02::2.

Inoltre, ci sono alcuni indirizzi importanti utilizzati per il corretto funzionamento di IPv6 e sono riassunti nelle seguenti tabelle:

Address Range	Description
2000::/3	Current Global Unicast Range
2001:0DB8::/32	Reserved for Documentation
FE80::/10	Link Local Unicast Address Range
FF00::/8	Multicast Address Range
::/128	Unspecified Address
::1/128	Loopback Address

Figura 14 Indirizzi IPv6

Address Range	Description
2400::/12	APNIC (Asia)
2600::/12	ARIN (America)
2800::/12	LACNIC (Latin America and Caribbean)
2A00::/12	RIPE NCC (Europa)
2C00::/12	AfriNIC (Africa)
2001:0DB8::/32	Documentation

Figura 15 Indirizzi IPv6

A differenza di IPv4, IPv6 incorpora in sé stesso molte funzioni e protocolli utili per aumentare la sicurezza, la cifratura e l'affidabilità.

Tra di questi, troviamo lo SLAAC – State Less Address Auto-Configuration. utilizzato per evitare l'uso di server DHCP, così da permettere ad un nodo di configurarsi completamente in maniera automatica. Per fare ciò vengono scambiati dei messaggi:

- **Router advertisement:** è un messaggio inviato periodicamente da un router sulla rete o in risposta ad un messaggio di router solicitation. Contiene molte informazioni, tra le quali il modo in cui vengono gestiti gli indirizzi sulla rete.
- **Router solicitation:** è un messaggio inviato all'indirizzo multicast FF02::2, in modo che sia analizzato da tutti i router IPv6 presenti nello scope e che richiede loro di identificarsi.

Non fornisce però informazioni sull'Interface ID, la quale può essere compilata dall'amministratore o da EUI-64 a partire dal MAC address dell'interfaccia.

Per passare dal MAC address all'interface ID, è necessario aggiungere 16 bits, standard, ai 48 bits del MAC, così da arrivare ai 64 bits totali dell'Interface.

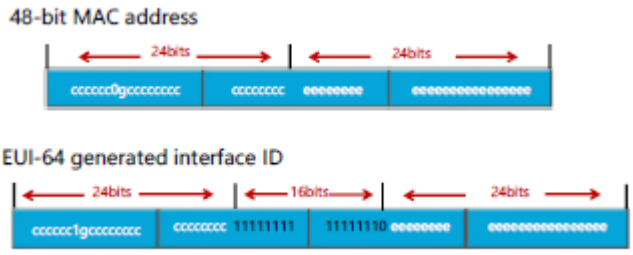


Figura 16 Passaggio da MAC address a Interface ID

I primi due byte del MAC address contengono una serie di informazioni importanti, in quanto contengono 2 bit utilizzati per definire il MAC address come broadcast, unicast etc.

Il 7 bit del MAC address viene negato, dopodiché viene diviso l'indirizzo in due parti uguali da 24 bits ciascuna e vengono aggiunti nel mezzo 16 bits – FFFE.

Un altro servizio aggiuntivo in IPv6 è il Neighbor Discovery Protocol, un protocollo utilizzato in sostituzione di ARP in IPv4. Esso definisce una coppia di messaggi:

1. **NS – Neighbor Solicitation:** chiede ad un host con un determinato indirizzo, di rispondere con il suo indirizzo fisico.
2. **NA – Neighbor Advertisement:** può essere utilizzato in risposta ad un NS o può essere di tipo unsolicited, inviato cioè a FF02::1.

INTERFACCE E COLLEGAMENTI

Le interfacce sono componenti fisici o logici che permettono ai dispositivi di comunicare tra loro. Interfacciare due dispositivi significa collegarli, seguendo degli standard che consentano lo scambio di dati.

Dal punto di vista fisico è caratterizzata dal mezzo trasmissivo e quindi dai cavi che vengono utilizzati. Nelle reti, l'interfaccia rappresenta la porta fisica di connessione in ingresso e uscita.

Ogni interfaccia di un dispositivo di rete sarà contraddistinta dalla tipologia e da tre numeri, come ad esempio GigabitEtherent0/0/1, dove il primo 0 sta ad indicare il numero del telaio, il secondo 0 sta ad indicare il numero dello slot e l'1 sta ad indicare il numero della porta associata all'interfaccia.

Nei routers che implementano IPv6, verranno anche aggiunte delle interfacce di Loopback, aventi lo scopo di testare il funzionamento del sistema.

In questo progetto, verrà assegnato alla loopback del router 2 l'indirizzo 2001:0db8:1111::1 e alla loopback del router 4 l'indirizzo 2001:0db8:3333::1.

Qui di seguito si possono vedere i collegamenti con le interfacce assegnate.

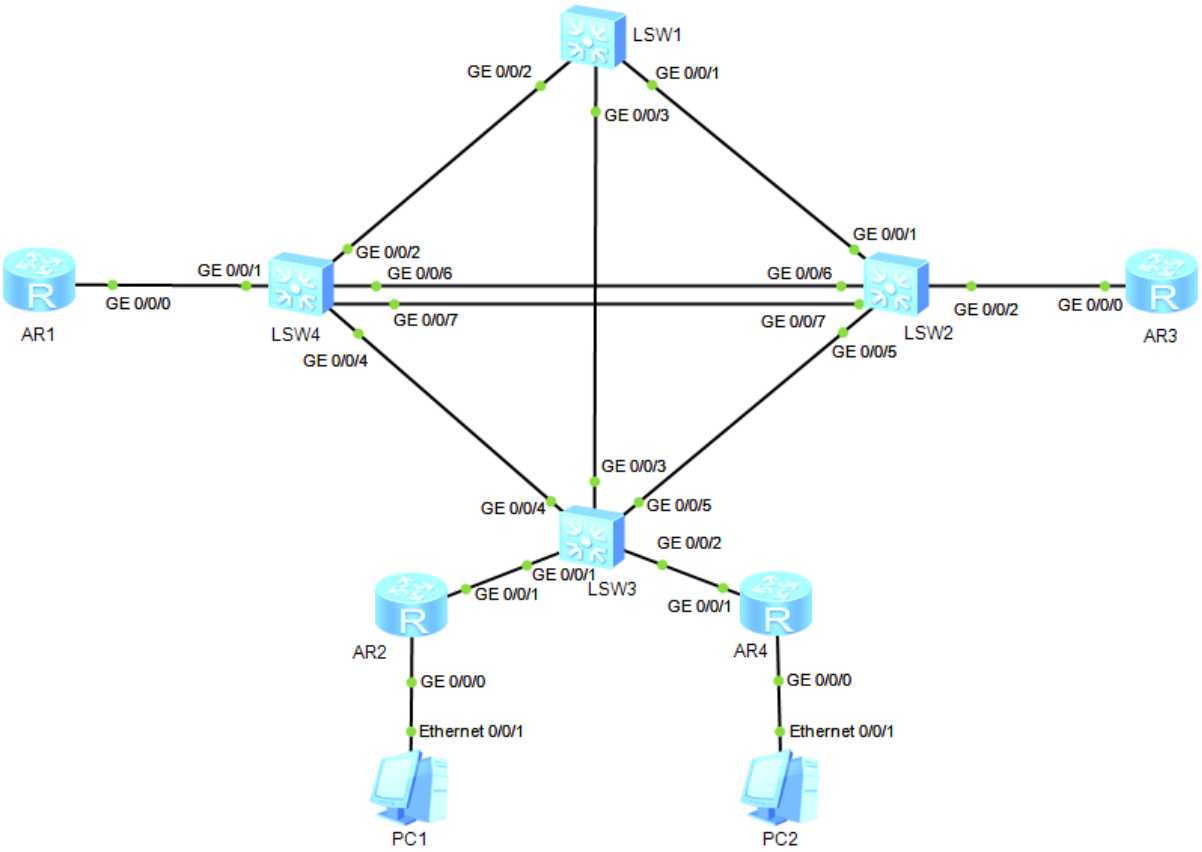


Figura 17 Topologia Fisica

MODELLO ISO/OSI

Ora, prima di entrare nel dettaglio del progetto, è bene partire dalle "origini".

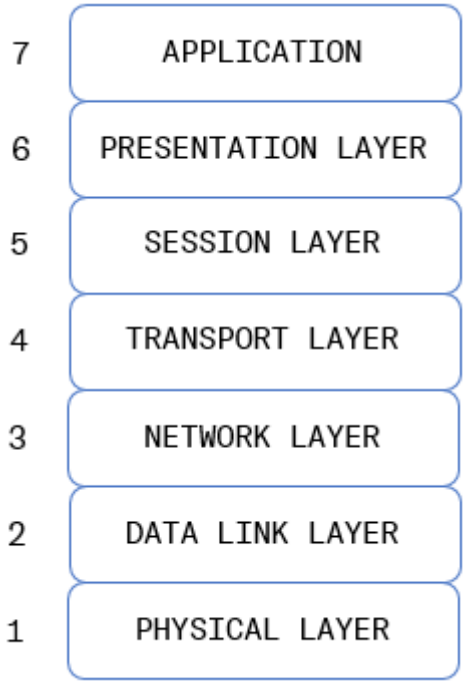


Figura 18 Modello ISO/OSI

Nel 1978 è stato definito il modello ISO/OSI, come standard per descrivere la struttura logica di una rete. È stato ideato per permettere una comunicazione comune indipendentemente da chi offre il servizio. Lo standard è composto da 7 livelli, organizzati come in figura e per far sì che la comunicazione avvenga correttamente, devono essere svolti, su ognuno di essi, tutte le loro specifiche funzioni.

I livelli si possono raggruppare in due grandi insiemi, quelli orientati al trasporto, dall'1 al 4 e quelli orientati all'applicazione, dal 5 al 7.

Si parte dal basso, dal livello fisico 1 che si occupa del bit flow, ovvero della trasmissione dei dati e della conversione dei bit di un pacchetto in un segnale fisico, adatto al mezzo trasmissivo che verrà utilizzato. La comunicazione con il mezzo viene definita attraverso dei protocolli e delle norme. In questo livello è quindi importante definire le regole per l'attivazione e disattivazione del collegamento fisico tra due punti, le caratteristiche dei cavi e le operazioni di multiplazione dei segnali.

Salendo di livello, si trova il data-link layer, che ha la funzione, innanzitutto, di frammentare la sequenza di bit ricevuta e di creare un frame, formato da 3 campi, header, data e trailer. Si occupa poi di individuare e risolvere eventuali errori e gestire

i vari meccanismi atti a correggerli. Gestisce inoltre, l'accesso multiplo al canale di comunicazione e ne regola le caratteristiche.

Ci sono principalmente due tipi di frame utilizzati:

1. Ethernet II – è riconoscibile dal campo type, perché assume valori maggiori/uguali a 1536 – 0x0600.

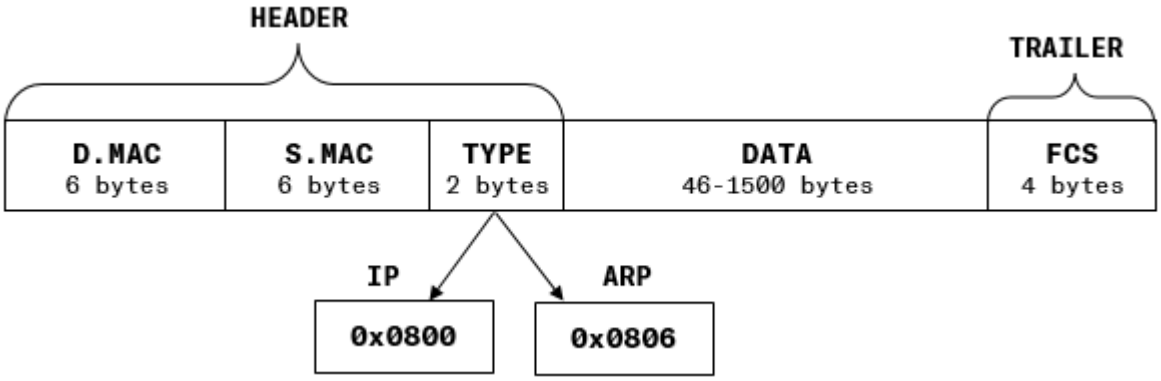


Figura 19 Frame Ethernet II

È formato da:

a. **HEADER:** intestazione del frame contenente:
   i. **D.MAC:** indirizzo MAC destinatario
   ii. **S.MAC:** indirizzo MAC sorgente
   iii. **TYPE:** tipologia di frame
      1. **IP:** con valore 0x0800
      2. **ARP:** con valore 0x0806
b. **DATA:** contenente le informazioni da trasmettere, di dimensioni variabili dai 46 ai 1500 bytes.
c. **TRAILER:** formato dall'FCS, di 4 bytes, per il controllo degli errori.

2. IEEE 802.3 – è riconoscibile dal campo length, in quanto assume valori minori a 1536. IEEE 802.3 consente di trasportare payload di tipo non Ethernet, come ad esempio STP.

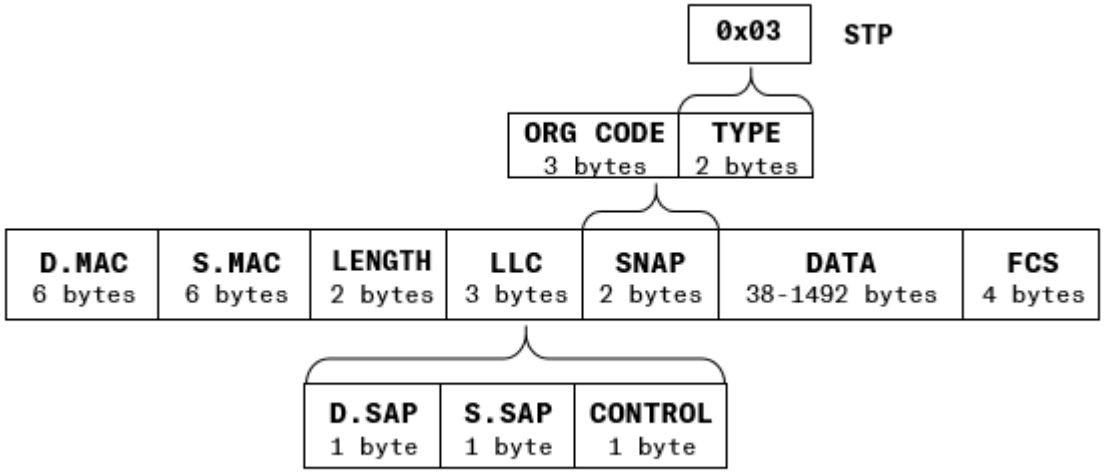


Figura 20 Frame IEEE 802.3

È formato dai seguenti campi:

a. **D.MAC:** indirizzo MAC destinatario
b. **S.MAC:** indirizzo MAC sorgente
c. **LENGTH:** lunghezza
d. **LLC – Logical Link Control**: utile per memorizzare le informazioni sul controllo del flusso dati.
    i. **D.SAP – Destination Service Access Point:** indica il punto di accesso per il servizio di destinazione; funge da puntatore ad un buffer di memoria.
    ii. **S.SAP – Source Service Access Point:** indica il punto di accesso per il servizio sorgente.
    iii. **CONTROL:** byte di controllo.
e. **SNAP – SubNetwork Access Protocol:** utile per definire molti protocolli.
    i. **ORG CODE:** Vendor Code.
    ii. **TYPE:** tipologia utilizzata, ad esempio STP con codice 0x03.
f. **DATA:** contiene i dati.
g. **FCS:** sequenza di controllo del frame.

Inoltre, i frames generati possono essere di tipo:

- **Unicast:** il frame inviato è destinato ad un solo host.
- **Broadcast:** il frame inviato è destinato a tutti gli host e si riconosce perché il D.MAC è costituito da tutti 1.
- **Multicast:** il frame è inviato a più destinatari.

A questo livello, l'host destinatario che riceve il frame, controlla l'FCS per verificare la presenza di eventuali errori, creatasi durante la trasmissione. L'FCS viene quindi nuovamente calcolato e confrontato con quello ricevuto; la coincidenza sta ad indicare la mancata presenza di errori, in caso contrario, verrà valutata la possibilità di correggerli. Se ciò non fosse possibile, il frame verrà scartato, senza però avvisare il mittente.

Proseguendo quindi, il frame viene poi inoltrato al livello di rete, il quale si occupa principalmente dell'indirizzamento logico ed instradamento dei pacchetti e della gestione della frammentazione. Per quanto riguarda il routing, viene identificato il percorso migliore per giungere a destinazione, utilizzando determinati protocolli.

La frammentazione interviene se il pacchetto L3 ha MTU – lunghezza – maggiore del payload del frame, che può variare dai 46 ai 1500 bytes. Solitamente viene utilizzato quando si deve trasmettere un pacchetto tra due LAN diverse, da una con MTU maggiore ad un con MTU minore.

Il campo Data al livello 3 viene incapsulato aggiungendo l'header IP, che varia il suo contenuto in base alla versione scelta.

Se IPv4, l'header ha dimensioni dai 20 ai 60 bytes e sarà così formato:

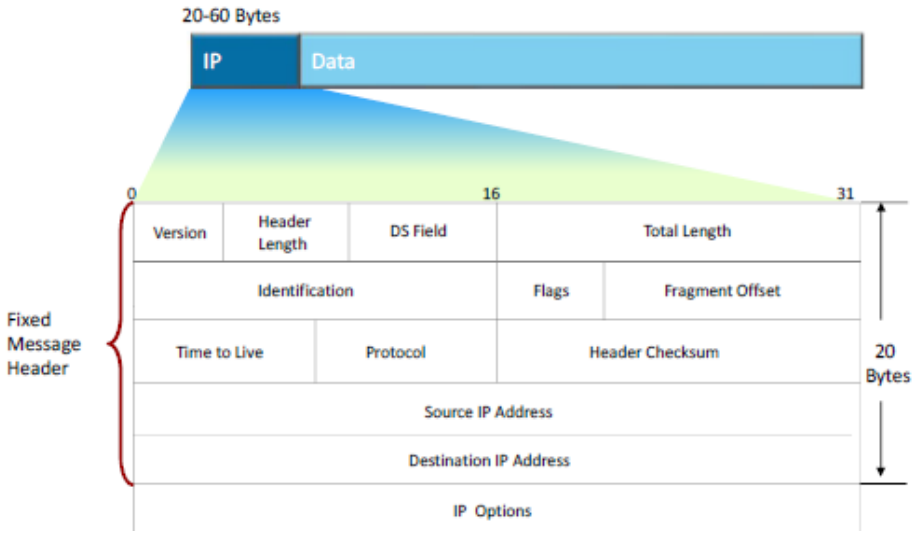


Figura 21 Header IP

- **Version** – 4 bit: indica la versione del protocollo in uso.
- **HLEN** – 4 bit: contiene i bit impostati ad un valore che indica la lunghezza dell'intestazione dei datagrammi, espressa in parole di 32 bit.
- **Differentiate Service** – 8 bit: si occupa della gestione della priorità dei dati.
- **Total length** – 16 bit: lunghezza complessiva del pacchetto, dati inclusi.
- **TTL – Time To Live** – 8 bit: corrisponde al tempo massimo di permanenza del pacchetto nella rete, il contatore viene decrementato ogni volta che passa per un router. Quando arriva a 0, viene generato un messaggio di errore di tipo ICMP e viene inviato al mittente.
- **Protocol** – 8 bit: indica a quale protocollo di livello superiore appartengono i dati contenuti nel pacchetto.
  Le principali sono:
  - 0x01: ICMP
  - 0x06: TCP

    - 0x11: UDP
    - 0x89: OSPF
    - 0x47: GRE
- **Header Checksum** – 16 bit: controllo errore sull'header.
- **Flags** – 3 bit: consente di gestire la frammentazione:
    - Bit 0: RESERVED – sempre a 0
    - Bit 1: DF – don't fragment
        - Se 0: si può frammentare
        - Se 1: non si può frammentare
    - Bit 2: MF – more fragments
        - Se 0: ultimo frammento
        - Se 1: frammento intermedio
- **Identification**: valore intero necessario all'host destinatario per identificare univocamente un pacchetto.
- **Source IP Address**: indirizzo IP sorgente.
- **Destination IP Address**: indirizzo IP destinatario.
- **IP Option**: contiene informazioni opzionali relative al trasferimento del pacchetto.

Se invece è IPv6, l'header sarà così composto:

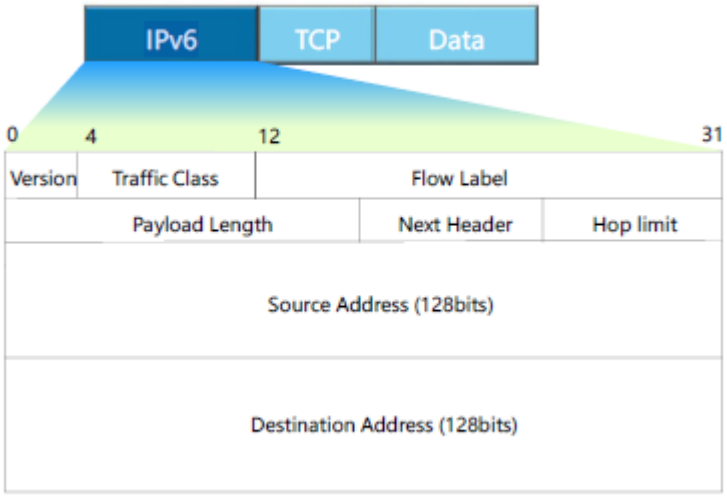


Figura 22 Header IPv6

- **Version:** versione utilizzata.
- **Traffic Class:** consente ad un nodo di indicare la priorità di un pacchetto in modo che ne possa essere ottimizzato l'inoltro da parte dei routers. Viene utilizzato dal mittente o da un router per identificare e distinguere le differenti priorità dei pacchetti IPv6.
- **Flow Label:** identifica uno stream continuo di pacchetti che possono essere raggruppati in base a delle caratteristiche comuni, quali origine/destinazione, appartenenza ad un processo o applicazione. Può essere utilizzata dal mittente per identificare delle sequenze di pacchetti per i quali richiede un trattamento speciale da parte del router, come ad esempio un servizio in real-time.
- **Payload Lenght:** lunghezza del payload.
- **Next Header:** identifica il tipo di header che segue l'header IPv6, che non è più di 20 byte, ma diviene modulare, ovvero si possono aggiungere dei campi in base alle esigenze di instradamento o protezione dell'informazione. Ha funzioni simili al campo Protocol di IPv4.
- **Hop limit:** campo il cui calore viene decrementato ogni qualvolta il pacchetto attraversa un router.
- **Source Address:** indirizzo del mittente.
- **Destination Addrress:** indirizzo del destinatario.

Una delle innovazioni apportate da IPv6 è l'extension header, un nuovo modo per comunicare fra peer. Vengono introdotti altri campi contenenti informazioni, estendendo appunto l'header, grazie all'utilizzo di puntatori. I campi che possono essere aggiunti sono i seguenti:

- **IPv6 Header**
- **Hop-by-Hop Option Header**
- **Destination Option Header**
- **Routing Header**

- **Fragment Header**
- **Authentication header**
- **Encapsulating Security Payload Header**
- **Destination Options header**
- **Upper-layer header**

Ognuno di questi campi, eccetto Hop-by-Hop, non viene processato dai nodi di transito, ma solo dal nodo di destinazione, il quale procede al decapsulamento delle informazioni.

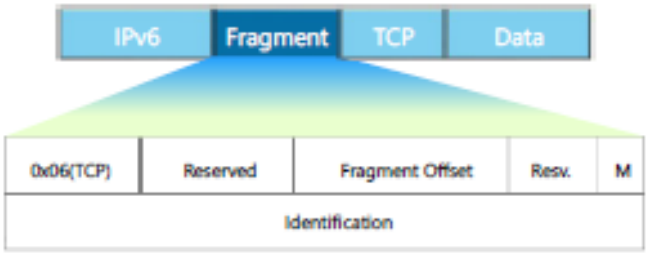


Figura 23 Fragment Header

Dal livello 3 si passa poi il pacchetto al livello 4, al livello di trasporto, il quale si occupa di stabilire e mantenere le connessioni tra nodi. Si tratta di un protocollo end-to-end. Permette la multiplazione dei dati scambiati tra due nodi. I principali protocolli sono TCP e UDP, il primo orientato alla connessione, mentre il secondo no. Anche in questo caso avviene l'incapsulamento prima di inoltrare di nuovo il pacchetto, detto datagramma.

Il modello ISO/OSI è stato molto importante per aver introdotto la stratificazione e l'interfacciamento tra i vari stati. Successivamente è stato studiato un nuovo modello, simile al precedente, ma più semplice, il modello TCP/IP.

TCP/IP

Il modello TCP/IP è divenuto lo standard per la comunicazione nelle reti. Si basa principalmente sull'utilizzo di due protocolli, TCP – Transmission Control Protocol ed IP- Internet Protocol. Ne fanno però parte anche altri protocolli aggiuntivi come, ad esempio UDP – User Datagram Protocol o ICMP – Internet Control Message Protocol. A differenza dell'ISO/OSI, si basa soltanto su 4 livelli.

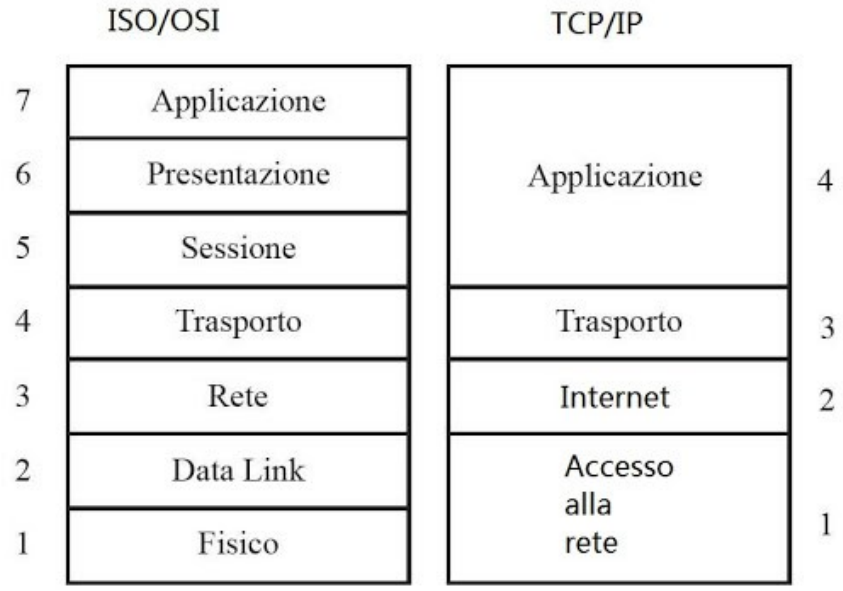


Figura 24 Modelli a confronto – ISO/OSI e TCO/IP

Il livello fisico TCP/IP è l'unione dei primi due livelli di ISO/OSI ed ha le stesse funzioni; di fatti comprende tutte le connessioni fisiche, i segnali ed i mezzi trasmessivi che permettono la creazione della topologia fisica della rete. A questo livello si può parlare di dominio di collisione, specialmente nelle topologie di rete a BUS.

Lo strato Internet corrisponde allo strato Network dell'OSI ed ha lo scopo di selezionare il miglior percorso attraverso la rete, per recapitare il messaggio al destinatario.

Lo strato di trasporto, anch'esso coincidente con il layer 4 dell'altro modello, crea una connessione logica tra sorgente e

destinazione indipendentemente dalla rete utilizzata, assemblando e segmentando i dati che riceve dal livello di applicazione e inviandoli al destinatario, un segmento per volta. Sono disponibili due tipologie di servizi, TCP e UDP, che verranno analizzati a breve.

Infine, all'ultimo livello del TCP/IP, si trova il livello di applicazione, il quale si occupa di implementare le applicazioni che permettono l'interazione con l'utente. Alcuni protocolli utilizzati sono:

- **FTP – File Transfer Protocol:** servizio TCP per il trasferimento dei file.
- **DNS – Domain Name System:** utile per tradurre i nomi di dominio.
- **Telnet:** è un "terminale virtuale", ovvero offre la possibilità di accedere da remoto ad un altro computer.

TCP

TCP o Transmission Control Protocol è un protocollo orientato alla connessione, ovvero prima di trasmettere informazioni, i nodi devono sincronizzarsi scambiando i numeri di sequenza che assegneranno ai loro datagrammi in un processo detto Three Way Handshake, spiegato successivamente.

TCP suddivide i dati dell'utente in segmenti di non più di 64KB e li incapsula in datagrammi IP. Quindi il pacchetto che si verrà a creare, avrà un header IP e un header TCP, entrambi di 20 bytes ed un campo data.

Il segmento TCP ha una sua struttura con i seguenti campi:

<table>
<tr><td colspan="3">Sorce Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="5">Sequence number</td></tr>
<tr><td colspan="5">Acknowledgment number</td></tr>
<tr><td>Data Offset</td><td>Reserved 4 bit</td><td>Flags</td><td colspan="2">Window</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

- **Source port:** porta sorgente.
- **Destination port:** porta destinazione.
- **Sequence number:** numero di sequenza del primo byte contenuto nel segmento ed è il valore che viene scambiato dai nodi nel processo di sincronizzazione.
- **Acknowledgment number:** se il bit ACK è a 1, è questo il numero di sequenza che ci si aspetta di ricevere.
- **Data offset:** indica dove iniziano i dati.
- **Flags – Control bit:** sono 8 flag necessari in varie situazioni, come per aprire o chiudere una connessione, per richiedere l'attenzione al campo ack etc.
- **Window:** indica la dimensione della finestra in ricezione, cioè quanti byte il destinatario può ricevere.
- **Checksum:** controllo d'errore sull'intestazione e sui dati, effettuato in blocchi di 16 bit.

CONNESSIONE E DISCONNESSIONE.

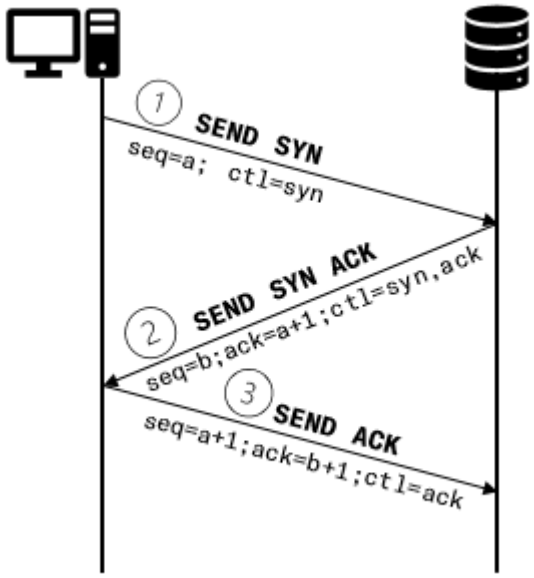


Figura 25 Three Way Handshake

Come accennato precedentemente, la connessione avviene utilizzando il Three Way Handshake tra client e server.

L'host invierà una richiesta SYN, di sincronizzazione, al server, contenente come informazioni il numero di sequenza; il server a sua volta risponderà inviando un SYN ACK, così da confermare anche la corretta ricezione della richiesta, con un suo numero di sequenza e con un ack di valore pari al numero di sequenza inviato dall'host, incrementato di 1.

Infine, il client risponderà, come conferma finale, con un ACK, con numero di sequenza pari all'ack ricevuto dal server e come ack, il valore della sequenza incrementato di 1.

In questo modo è da considerarsi conclusa la procedura di connessione ed il client può trasmettere i dati.

Sia il TCP che l'UDP, utilizzano delle porte come mezzo per gestire flussi di dati attraverso un'unica connessione fisica alla rete. Una porta è un valore numerico specificato su 2 byte, che identifica un determinato canale utilizzabile per la comunicazione, permettendo di instaurare più comunicazioni simultaneamente. In questo modo, la connessione che si va ad instaurare tra due nodi viene identificata univocamente da una coppia di dati <indirizzo IP:porta del mittente> e <indirizzo IP:porta destinatario>, dette socket.

Ci sono delle porte note e riservate, con numero inferiore a 1024, spesso utilizzate in applicazioni TCP. Alcune di esse sono:

- 21: FTP
- 23: Telnet
- 25: SMTP – e-mail
- 80: HTTP

Nel momento in cui il client vorrà cessare la connessione, dovrà inviare un ACK+FIN al server, il quale, accogliendo la richiesta, risponderà con un ACK di conferma. Però, prima che effettivamente si chiuda la connessione, dovrà intercorrere un lasso di tempo di alcuni minuti, affinché tutti i pacchetti rimasti in circolazione, possano essere recapitati a destinazione.

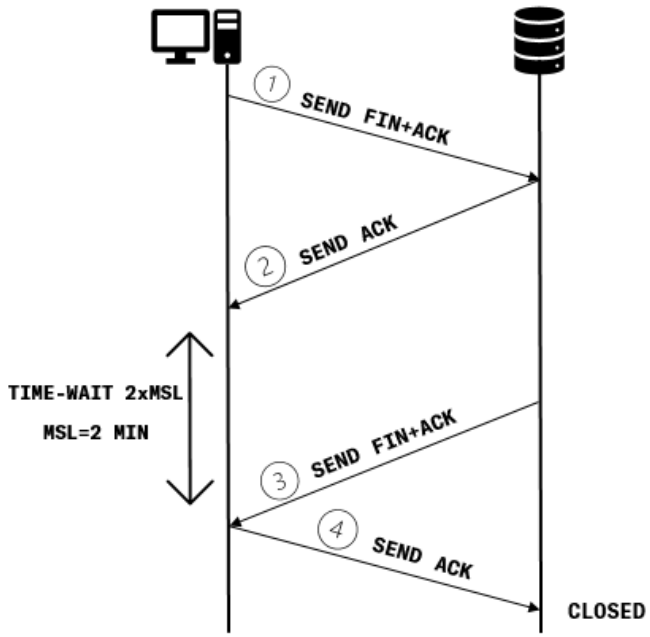


Figura 26 Chiusura connessione

Al termine, il server inoltrerà un FIN+ACK all'host, il quale inviando un ACK, chiuderà definitivamente la connessione.

UDP

L'UDP – User Datagram Protocol a differenza del precedente, non è orientato alla connessione e quindi non richiede una sincronizzazione tra i nodi; per questo risulta meno affidabile. Ogni datagramma UDP viene incapsulato in un datagramma IP, di conseguenza la dimensione del datagramma UDP non può superare la dimensione del datagramma IP.

L'UDP è costituito da un header di 8 bytes, contro i 20 bytes del TCP e dal campo data.

Il segmento UDP è così composto:

Source Port	Destination Port
Lenght	Checksum
Data – Messagge	

- **Source port:** identifica il numero di porta della sorgente.
- **Destination port:** identifica il numero di porta della destinazione.
- **Lenght:** contiene la lunghezza totale in bytes.
- **Checksum:** contiene il codice di controllo del datagramma.
- **Data:** contiene i dati del messaggio.

UDP viene impiegato dalle applicazioni aventi come requisito maggior velocità di trasferimento, tralasciando piccole perdite o errori durante il trasferimento. Di fatti uno dei principali utilizzi è ad esempio, nello streaming.

LAVORO SVOLTO

Avendo illustrato brevemente la base della comunicazione, è possibile procedere con l'analisi del progetto.

Per realizzare la topologia fisica, sono stati necessari quattro switches e quattro routers.

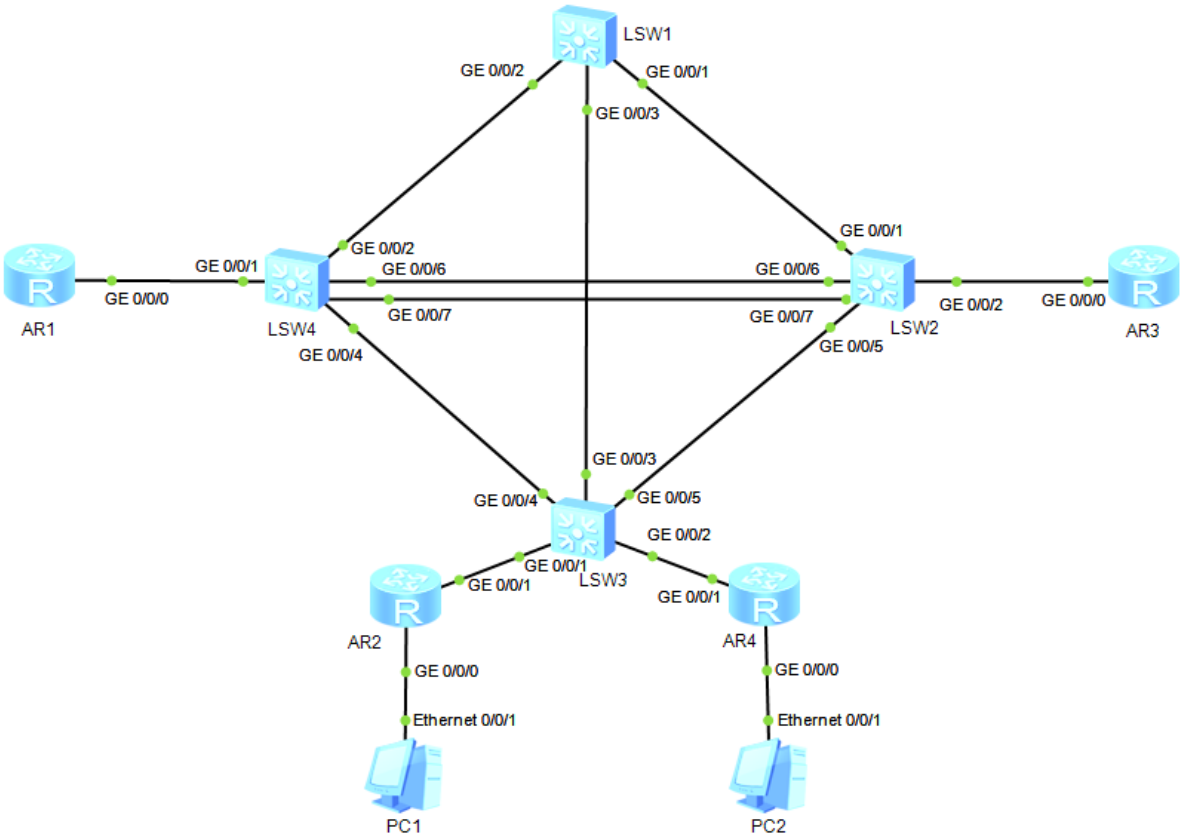


Figura 27 Topologia fisica

CONFIGURAZIONI

Entrando nel dettaglio della configurazione, per evitare che due nodi appartenenti allo stesso link, lavorino con velocità e/o duplex differenti, è stata disabilitata su tutti gli switches, l'auto-negoziazione. Quest'ultima, definita dallo standard IEEE 802.3u, ha il compito di far concordare i dispositivi sulle caratteristiche del link, in termini di velocità e duplex.

Entrambi gli switches, collegati allo stesso link, dovranno essere configurati allo stesso modo.

Ad esempio, lo SW1 e lo SW4 sono collegati da un link con interfaccia GigabitEthernet 0/0/2 ed attraverso questa serie di istruzioni è possibile disabilitare l'auto-negoziazione e stabilire le specifiche di connessione.

<Huawei> system-view *//consente di accedere alle configurazioni del dispositivo*
[Huawei] sysname S1 *//cambia il nome del dispositivo in S1, così da facilitarne la comprensione, per la configurazione e/o manutenzione.*
[S1] interface GigabitEthernet0/0/2 *//si entra nell'interfaccia GigabitEthernet 0/0/2, dove il 2 sta ad indicare il numero della porta dello switch.*
[S1-GigabitEthernet0/0/2]undo negotiation-auto *//si disabilita l'auto-negoziazione.*
[S1-GigabitEthernet0/0/2]speed 100 *//le velocità possibili sono 10/100/1000, in base poi a quali sono supportate dal dispositivo.*
[S1-GigabitEthernet0/0/2]duplex full *//si imposta in base alla velocità scelta; se 10 Mbps si sceglie HALF, altrimenti FULL. Half significa che sul link possono trasmettere uno alla volta in una sola direzione, mentre Full duplex indica la capacità di trasmettere contemporaneamente in entrambe le direzioni. Nel primo caso è necessaria la presenza di CSMA/CD, un meccanismo per la rilevazione di eventuali collisioni. L'host che vuole trasmettere, prima deve controllare se il canale è libero ed in caso affermativo potrà trasmettere. Se avvenissero delle collisioni, l'host dovrà terminare la trasmissione, ritentandola successivamente.*

Per un corretto funzionamento, anche nello switch 4, verranno impostate le stesse configurazioni.

```
<Huawei> system-view

[Huawei] sysname S4

[S4] interface GigabitEthernet0/0/2

[S4-GigabitEthernet0/0/2]undo negotiation-auto

[S4-GigabitEthernet0/0/2]speed 100

[S4-GigabitEthernet0/0/2]duplex full
```

Come si può vedere dalle schermate qui di seguito, viene eseguito lo stesso procedimento su tutti gli switches e su tutte le interfacce di essi.

LSW1

```
interface GigabitEthernet0/0/1
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
```

Figura 28 Interfacce Switch 1

LSW2

```
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp-static
 max active-linknumber 1
#
interface GigabitEthernet0/0/1
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 stp edged-port enable
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/6
 undo negotiation auto
 speed 100
 eth-trunk 1
#
interface GigabitEthernet0/0/7
 undo negotiation auto
 speed 100
 eth-trunk 1
#
```

Figura 29 Interfacce Switch 2

LSW3

```
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 21
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 43
#
interface GigabitEthernet0/0/3
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/4
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/5
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
```

Figura 30 Interfacce Switch 3

LSW4

```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 stp edged-port enable
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
 undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 100
#
interface GigabitEthernet0/0/7
 undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 100
#
```

Figura 31 Interfacce Switch 4

Per assicurare un funzionamento affidabile, vengono utilizzati collegamenti ridondanti tra i vari switches, così nel caso in cui un link cada, sarà attivato il link ridondante.

Ma ciò non esclude la possibilità di incombere in:

- **broadcast storms:** avviene quando uno switch invia un frame broadcast, chiedendo agli switches destinatari di inoltrarlo nuovamente, ottenendo a lungo andare, un collasso della rete, dato che i frame non hanno un TTL – Time To Live.
- **mac instability:** si verifica quando i frames vengono inoltrati su più collegamenti, generando dei loop, i quali sono la principale fonte di instabilità. In particolare, la tabella dei MAC address potrebbe essere sottoposta ad un continuo aggiornamento, dovuto all'arrivo di frames su porte differenti dello stesso switch.

STP

Per risolvere queste problematiche, è stato introdotto l'STP – Spanning Tree Protocol, un protocollo atto ad impedire che si verifichino dei loop, disattivando in modo logico i collegamenti ridondanti.

Gli switches con le relative porte avranno un ruolo ben definito. Prima di tutto, i dispositivi eleggeranno un bridge root, ovvero uno switch che sarà a capo della rete. Per "selezionarlo", gli switches dovranno comunicare tra loro scambiandosi dei BPDU – Bridge Protocol Data Unit, stringhe di dati trasportate all'interno di frame.

PID	PVI	BPDU TYPE	FLAGS	ROOT ID	RPC	BRIDGE ID	PORT ID	MESSAGGE AGE	MAX AGE	HELLO TIME	FWD DELAY

Il frame conterrà diverse informazioni, tra le quali:

- **PID – Port ID:** entra in gioco in presenza di connessioni doppie e/o ridondanti. È la combinazione della priorità della porta e del numero di porta, come ad esempio 80.1, dove 80 indica la priorità ed 1 il numero della porta. La priorità varia a multipli di 16. Se ci sono due porte con stessa priorità, diventerà porta ROOT quella con numero di porta inferiore.
- **BPDU TYPE:** indica la tipologia di BPDU utilizzata e può essere:
    1. **Configutation:** sono downstream, ovvero vanno dal bridge root verso gli altri switches.
    2. **TCN – Topology Change Notification:** sono upstream, quindi vanno dai nodi foglia al root. Viene emesso quando si deve cambiare la topologia.
- **RPC – Root Path Cost:** il costo per arrivare dal bridge root ad un nodo foglia.
- **Bridge ID:** la combinazione, propria di ogni switch, tra valore di priorità e MAC address del dispositivo.
- **Port ID:** tiene conto della porta di uscita del BPDU.
- **Message Age:** indica il numero di switches attraversati.
- **MAX Age:** indica il lasso di tempo da attendere prima di ritenere inattivo uno switch ed è pari a 20 secondi.
- **Hello Time:** è l'intervallo di tempo, solitamente di 2 secondi, per inviare nuovamente un BPDU, così da mostrare di essere attivi e funzionanti.
- **FWD Delay – Forward Delay:** è il tempo speso negli stati di Listening e Learning ed è pari a 15 secondi ciascuno, di default.

Quindi, inizialmente, tutti gli switches propagheranno un BPDU comunicando di essere loro il root bridge, dopodiché ciascun switch confronterà il proprio bridge ID con quello ricevuto e trasmetterà l'ID con priorità maggiore, ovvero quello con valore numerico

minore tra i due. Di default viene assegnato 32768 come priorità, ma per aumentarla, basterà configurare lo switch con un numero inferiore ad esso. Nel caso in cui ci sia parità di priorità, verranno confrontati i MAC address.

Una volta eletto il root bridge, ad ogni porta degli switches verrà assegnato un proprio ruolo e stato. Tra i ruoli ci sono:

1. **Designated:** le porte del root sono così definite consentono il traffico dal ROOT verso i segmenti ad esso collegati.
2. **Root:** sono le porte collegate alle porte designated.
3. **Alternate:** sono le porte che indicano un percorso alternativo verso il root. Sono utilizzate per rompere lo switching loop e possono solo ricevere BPDU da porte DESIGNATED.

In unione ad uno dei seguenti stati:

1. **Forwarding**
2. **Disabled**
3. **Blocking**
4. **Learning**
5. **Listening**

Come si può vedere dal grafo sottostante, inizialmente tutte le porte sono DISABLED, man mano che vengono attivate passano a BLOCKING. In questo stato, le porte non possono inoltrare frame, ma possono solo ricevere e processare i BPDU ed inoltre, non vengono neanche memorizzati i MAC address dei dispositivi.

Si può tornare in questo stato, anche quando, passato il MAX age, solitamente pari a 20 secondi, il root bridge non riceve più gli Hello BPDU, inoltrati di default ogni 2 secondi, arrecando così un cambiamento nella topologia della rete. Lo switch invierà un frame, il TCN - Topology Change Notification, a tutti gli altri membri dell’albero, comunicando di mettere in time-out i vecchi indirizzi MAC address.

A questo punto, sarà necessario un processo di rielezione del root bridge. Quindi per convergere il traffico, si passerà dallo stato BLOCKING agli stati LISTENING e LEARNING.

LISTENING consente di negoziare lo stato della porta, permettendo anche lo scambio dei BPDU, ma non consentendo lo scambio del traffico utente.

LEARNING consente di popolare la tabella dei MAC address, senza permettere lo scambio del traffico utente.

Lo switch, quindi, attenderà in totale 50 secondi; 20 secondi del MAX Age, 15 secondi del LISTENING e 15 secondi del LEARNING. Terminato questo periodo, la porta passerà a FORWARDING.

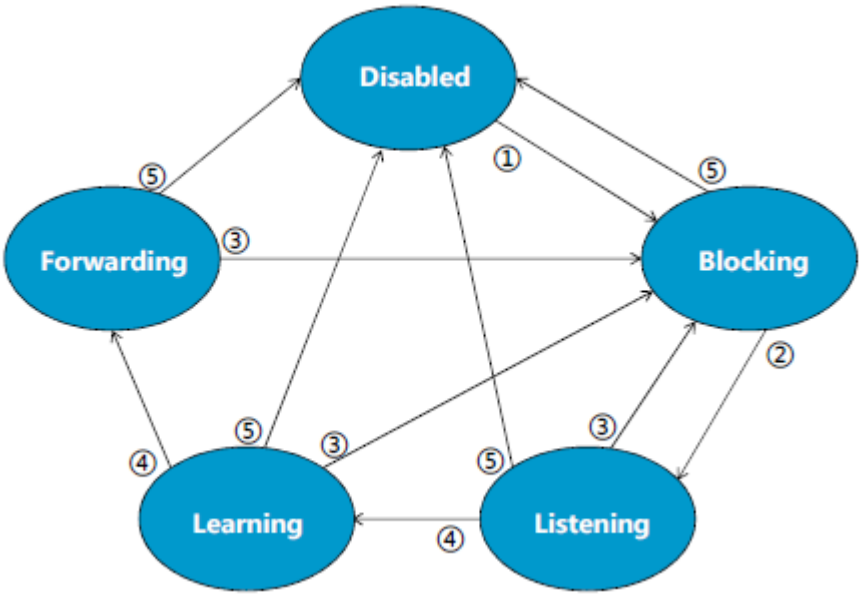


Figura 32 Diagramma a stati STP

Uno dei principali svantaggi dell'STP è appunto questa lentezza nella convergenza, per questo è stato introdotto, l'RSTP – Rapid Spanning Tree Protocol.

RSTP

RSTP è un protocollo di rete che garantisce una topologia senza loop; utilizza un processo di proposta e accordo che consente l'immediata negoziazione dei collegamenti da realizzare, riducendo così di molto i tempi di attesa.

Il funzionamento è simile a STP, viene eletto un root bridge, una root port su ogni switch ed una designated port in ogni segmento. Richiede una connessione veloce, possibilmente full-duplex, così da ottenere una riconfigurazione rapida in caso di necessità.

RSTP riduce il numero di stati di una porta a 3, unendo gli stati Disabled, Blocking e Listening di STP, in un unico, chiamato DISCARDING. Gli altri due stati restano invece invariati e sono LEARNING e FORWARDING.

Ad ogni stato della porta, corrisponderà un ruolo:

1. **Discarding**: riceve solo BPDU
2. **Alternate:** è una porta che consente un percorso alternativo verso il root-switch. Si attiva solo nel momento del bisogno e non effettua l'inoltro del traffico.
3. **Backup:** è la porta che fornisce un percorso di backup, ridondante, ma meno desiderabile. Solitamente, quando uno switch ha due porte in uno stesso segmento, quella a costo più alto, viene definita di backup. Questa porta lavora come la DISCARDING e si attiva, solo nel momento in cui cada l'altro link.
4. **Root:** porta nello stato di forwarding ed è eletta per ogni switch non-root che consente il percorso con il minor costo verso il root bridge.

5. **Designated:** porta nello stato di forwarding, viene eletta per ogni segmento della LAN, in base al bridge ID dello switch cui appartiene. Permette l'inoltro del traffico verso il root bridge.

Infine, si possono trovare anche le edge-port, cioè porte che collegano lo switch con i terminali; esse non ricevono configurazioni BPDU e non partecipano al calcolo RSTP.

RSTP è stato utilizzato anche in questo progetto, nei collegamenti tra gli switches. Qui di seguito, si possono vedere le configurazioni apportate agli switches.

<S4> system-view

[S4] stp mode rstp *//viene abilitato rstp*

[S4] int gigabitethernet 0/0/1

[S4-GigabitEthernet0/0/1] stp bdpu-protection *//si abilita la protezione bpdu nell'interfaccia*

Attraverso due comandi è possibile visualizzare la configurazione di RSTP in ogni switch.

Con "display stp brief" vengono elencate tutte le porte attive con RSTP, mostrando anche il loro ruolo, il loro stato e se hanno protezioni attive.

```
<S4>dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/4        ALTE  DISCARDING      NONE
   0    Eth-Trunk1                  ALTE  DISCARDING      NONE
```

Figura 33 Porte definite con RSTP

```
<S4>dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :32768.4c1f-cc53-0272
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0     .4c1f-ccba-05ee / 200000
CIST RegRoot/IRPC   :32768.4c1f-cc53-0272 / 0
CIST RootPortId     :128.3
BPDU-Protection     :Disabled
TC or TCN received  :63
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:3m:42s
Number of TC        :17
Last TC occurred    :GigabitEthernet0/0/2
----[Port2(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :32768.4c1f-cc53-0272 / 128.2
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :14
 TC or TCN received  :0
 BPDU Sent           :693
         TCN: 0, Config: 0, RST: 693, MST: 0
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
----[Port3(GigabitEthernet0/0/2)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :0.4c1f-ccba-05ee / 128.2
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
----[Port5(GigabitEthernet0/0/4)][DISCARDING]----
 Port Protocol       :Enabled
 Port Role           :Alternate Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :4096.4c1f-ccc8-3f8c / 128.4
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :3
 TC or TCN received  :19
 BPDU Sent           :4
         TCN: 0, Config: 0, RST: 4, MST: 0
 BPDU Received       :758
         TCN: 0, Config: 0, RST: 758, MST: 0
----[Port1(Eth-Trunk1)][DISCARDING]----
 Port Protocol       :Enabled
 Port Role           :Alternate Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=199999
 Designated Bridge/Port   :32768.4c1f-cc14-46fa / 128.1
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :3
 TC or TCN received  :25
 BPDU Sent           :4
         TCN: 0, Config: 0, RST: 4, MST: 0
 BPDU Received       :777
         TCN: 0, Config: 0, RST: 777, MST: 0
```

Figura 34 Configurazione globale

Invece con il comando "display stp", vengono visualizzate le informazioni in dettaglio, di tutte le porte, anche quelle non attive.

Infatti, dalla Figura 35, si può notare nella prima riga "Mode RSTP", ovvero la modalità di STP utilizzata, dopodiché vengono visualizzati ulteriori dettagli utili per capire come è stata organizzata la topologia.

Il CIST Bridge – Common Internal Spanning Tree fornisce il bridge ID del sistema che si sta analizzando.

Il CIST ROOT-ERPC o External Root Path Cost mostra il bridge ID del ROOT switch ed il costo per raggiungerlo. Se sul CIST Root viene visualizzato un valore differente dal CIST Bridge, significa che lo switch preso in considerazione non è il ROOT. Ovviamente come ulteriore conferma per capire se lo switch è il root è il costo associato, se 0, è lui il root.

Vengono inoltre mostrate altre informazioni come il bridge ID ed i tempi di configurazione, quali hello time, max age, fwr delay etc.

Anche per le altre porte, compreso l'Ethernet Trunk, definito successivamente, verranno visualizzate le configurazioni dettagliate.

Riguardo lo switch 2, la porta legata all'interfaccia GigabitEthernet0/0/1, viene eletta come root, che, come detto precedentemente, viene impostata su ogni switch non-root e rappresenta la porta, con il minor costo, per arrivare al bridge root.

```
<S2>dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/5        ALTE  DISCARDING      NONE
   0    Eth-Trunk1                  DESI  FORWARDING      NONE
```

Figura 35 Porte switch 2 RSTP

```
<S2>dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :32768.4c1f-cc14-46fa
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .4c1f-ccba-05ee / 200000
CIST RegRoot/IRPC   :32768.4c1f-cc14-46fa / 0
CIST RootPortId     :128.2
BPDU-Protection     :Disabled
TC or TCN received  :43
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:4m:22s
Number of TC        :17
Last TC occurred    :GigabitEthernet0/0/1
----[Port2(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :0.4c1f-ccba-05ee / 128.1
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :4
 TC or TCN received  :18
 BPDU Sent           :6
         TCN: 0, Config: 0, RST: 6, MST: 0
 BPDU Received       :583
         TCN: 0, Config: 0, RST: 583, MST: 0
----[Port3(GigabitEthernet0/0/2)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :32768.4c1f-cc14-46fa / 128.3
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :13
 TC or TCN received  :0
 BPDU Sent           :568
         TCN: 0, Config: 0, RST: 568, MST: 0
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
----[Port6(GigabitEthernet0/0/5)][DISCARDING]----
 Port Protocol       :Enabled
 Port Role           :Alternate Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :4096.4c1f-ccc8-3f8c / 128.5
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :4
 TC or TCN received  :24
 BPDU Sent           :5
         TCN: 0, Config: 0, RST: 5, MST: 0
 BPDU Received       :642
----[Port1(Eth-Trunk1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=199999
 Designated Bridge/Port   :32768.4c1f-cc14-46fa / 128.1
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :25
 TC or TCN received  :3
 BPDU Sent           :660
         TCN: 0, Config: 0, RST: 660, MST: 0
 BPDU Received       :4
         TCN: 0, Config: 0, RST: 4, MST: 0
```

Figura 36 Configurazione globale switch 2 RSTP

Viene eletto l'Ethernet-Trunk, come porta Alternate, infatti il suo stato è impostato a DISCARDING, quindi abilitata solo in caso di malfunzionamenti.

Lo switch 1 è stato impostato come primary root. Si può notare dal ruolo delle porte che sono tutte configurate come DESIGNATED ed hanno come stato FORWARDING.

```
[S1] stp root primary
```

Si può notare che tutte le porte dello switch sono impostate come DESIGNATED e almeno una di esse, è connessa ad una porta ROOT.

LSW1

```
<S1>dis stp bri
 MSTID   Port                        Role  STP State     Protection
   0     GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/3        DESI  FORWARDING      NONE
```

Figura 37 Configurazione porte switch 1 RSTP

Il valore mostrato nel CIST BRIDGE e nel CIST Root della Figura 45, coincidono; inoltre, il costo per arrivare al root è pari a 0; l'unione di queste tre "configurazioni" dimostrano che lo switch S1 è il root della topologia.

```
<S1>dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :0    .4c1f-ccba-05ee
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .4c1f-ccba-05ee / 0
CIST RegRoot/IRPC   :0    .4c1f-ccba-05ee / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
CIST Root Type      :Primary root
TC or TCN received  :15
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:0m:12s
Number of TC        :15
Last TC occurred    :GigabitEthernet0/0/3
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol      :Enabled
 Port Role          :Designated Port
 Port Priority      :128
 Port Cost(Dot1T )  :Config=auto / Active=20000
 Designated Bridge/Port   :0.4c1f-ccba-05ee / 128.1
 Port Edged         :Config=default / Active=disabled
 Point-to-point     :Config=auto / Active=true
 Transit Limit      :147 packets/hello-time
 Protection Type    :None
 Port STP Mode      :RSTP
 Port Protocol Type :Config=auto / Active=dot1s
 BPDU Encapsulation :Config=stp / Active=stp
 PortTimes          :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send     :5
 TC or TCN received :1
 BPDU Sent          :349
        TCN: 0, Config: 0, RST: 349, MST: 0
BPDU Received       :1
        TCN: 0, Config: 0, RST: 1, MST: 0
----[Port2(GigabitEthernet0/0/2)][FORWARDING]----
 Port Protocol      :Enabled
 Port Role          :Designated Port
 Port Priority      :128
 Port Cost(Dot1T )  :Config=auto / Active=20000
 Designated Bridge/Port   :0.4c1f-ccba-05ee / 128.2
 Port Edged         :Config=default / Active=disabled
 Point-to-point     :Config=auto / Active=true
 Transit Limit      :147 packets/hello-time
 Protection Type    :None
 Port STP Mode      :RSTP
 Port Protocol Type :Config=auto / Active=dot1s
 BPDU Encapsulation :Config=stp / Active=stp
 PortTimes          :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send     :4
 TC or TCN received :2
 BPDU Sent          :349
        TCN: 0, Config: 0, RST: 349, MST: 0
BPDU Received       :2
        TCN: 0, Config: 0, RST: 2, MST: 0
----[Port3(GigabitEthernet0/0/3)][FORWARDING]----
 Port Protocol      :Enabled
 Port Role          :Designated Port
 Port Priority      :128
 Port Cost(Dot1T )  :Config=auto / Active=20000
 Designated Bridge/Port   :0.4c1f-ccba-05ee / 128.3
 Port Edged         :Config=default / Active=disabled
 Point-to-point     :Config=auto / Active=true
 Transit Limit      :147 packets/hello-time
 Protection Type    :None
 Port STP Mode      :RSTP
 Port Protocol Type :Config=auto / Active=dot1s
 BPDU Encapsulation :Config=stp / Active=stp
 PortTimes          :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send     :2
 TC or TCN received :0
 BPDU Sent          :11
        TCN: 0, Config: 0, RST: 11, MST: 0
BPDU Received       :1
        TCN: 0, Config: 0, RST: 1, MST: 0
```

Figura 38 Configurazione globale switch 1 RSTP

Lo switch S3 è stato impostato come secondary root, nel caso in cui il primary root si guasti, con il seguente comando

[S3] stp root secondary

```
<S3>dis stp bri
 MSTID   Port                        Role  STP State     Protection
   0     GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/3        ROOT  FORWARDING      NONE
   0     GigabitEthernet0/0/4        DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/5        DESI  FORWARDING      NONE
```

Figura 39 Configurazione porte switch 3 RSTP

```
<S3>dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :4096 .4c1f-ccc8-3f8c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0     .4c1f-ccba-05ee / 200000
CIST RegRoot/IRPC   :4096 .4c1f-ccc8-3f8c / 0
CIST RootPortId     :128.3
BPDU-Protection     :Disabled
CIST Root Type      :Secondary root
TC or TCN received  :15
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:8m:33s
Number of TC        :12
Last TC occurred    :GigabitEthernet0/0/3
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :4096.4c1f-ccc8-3f8c / 128.1
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :8
 TC or TCN received  :0
 BPDU Sent           :342
         TCN: 0, Config: 0, RST: 342, MST: 0
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
----[Port4(GigabitEthernet0/0/4)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :4096.4c1f-ccc8-3f8c / 128.4
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :9
 TC or TCN received  :3
 BPDU Sent           :385
         TCN: 0, Config: 0, RST: 385, MST: 0
 BPDU Received       :3
         TCN: 0, Config: 0, RST: 3, MST: 0
----[Port5(GigabitEthernet0/0/5)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :4096.4c1f-ccc8-3f8c / 128.5
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :13
 TC or TCN received  :4
 BPDU Sent           :434
         TCN: 0, Config: 0, RST: 434, MST: 0
 BPDU Received       :4
         TCN: 0, Config: 0, RST: 4, MST: 0
----[Port2(GigabitEthernet0/0/2)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :4096.4c1f-ccc8-3f8c / 128.2
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :15
 TC or TCN received  :0
 BPDU Sent           :347
         TCN: 0, Config: 0, RST: 347, MST: 0
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
----[Port3(GigabitEthernet0/0/3)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=200000
 Designated Bridge/Port   :0.4c1f-ccba-05ee / 128.3
 Port Edged          :Config=default / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :147 packets/hello-time
 Protection Type     :None
 Port STP Mode       :RSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :6
 TC or TCN received  :8
 BPDU Sent           :128
         TCN: 0, Config: 0, RST: 128, MST: 0
 BPDU Received       :264
         TCN: 0, Config: 0, RST: 262, MST: 2
```

Figura 40 Configurazione globale switch 3 RSTP

La configurazione finale che si ottiene è la seguente:

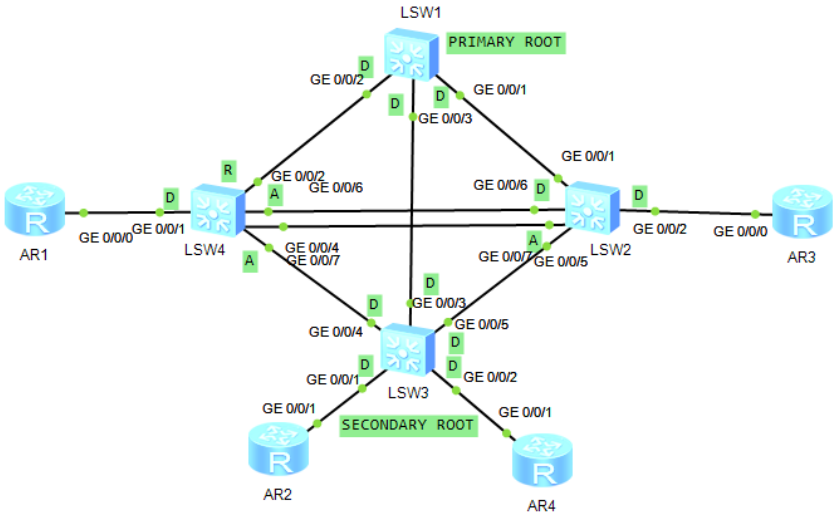


Figura 41 Topologia fisica con ruoli RSTP delle porte

LACP

Per terminare la configurazione a livello a 2, è necessario implementare il link aggregation, il quale prevede un meccanismo standard di negoziazione, che permette a due switches di utilizzare più cavi in parallelo, andando a creare così un trunk-link tra loro, in grado di incrementare la velocità e la ridondanza.

Onde realizzare quanto detto ci si serve di due modalità, LACP o Manual Mode.

LACP – Link Aggregation Control Protocol, specificato nello standard IEEE 802.2ad, permette di raggruppare più porte fisiche in un singolo canale logico.

In questa topologia è stato richiesto di implementare LACP tra gli switches 2 e 4. Affinché ciò sia possibile, è necessario aggiungere un link tra i due switches.

In LACP ci sono due modalità di funzionamento, il manual mode o load balancing mode e lo static LACP mode.

Nel primo, le interfacce membro sono aggiunte manualmente al link aggregation group – LAG e tutti i link sono attivi per il

forwarding. Il bilanciamento avviene sulla base degli indirizzi MAC o IP della sorgente e destinazione, così da non dividere il frame. Questa modalità può essere utilizzata anche nelle aree di reti che necessitano di una connessione veloce.

Nello static LACP mode, invece, viene istaurato sempre un link di backup, nel caso in cui ci fosse un malfunzionamento. Per fare ciò, i dispositivi, che in questo caso sono lo switch 4 e lo switch 2, si scambiano dei pacchetti LACP per effettuare la negoziazione, di tipo MASTER/SLAVE, per determinare chi sarà il dispositivo atto a scegliere le interfacce da lasciare attive. Vengono assegnati quindi due ruoli, ACTOR, corrispondente al MASTER ed è colui che ha priorità maggiore ed il PARTNER o SLAVE, che è il restante dispositivo. Sono individuabili due priorità:

1. **Di sistema:** configurabile in “system-view” e determina quale dei dispositivi funge da actor.
2. **Di interfaccia:** si configura in “interface-view” e determina quale interfaccia sarà attiva.

Una volta terminata la negoziazione, l’ACTOR determinerà quali sono le interfacce attive e quali inattive. Per questo motivo LACP viene anche chiamato M:N, dove M sta ad indicare le interfacce attive che si occupano dell’inoltro dei dati con la modalità load balancing, mentre N rappresenta i link inattivi ridondanti.

È necessario a questo punto, creare un Ethernet Trunk con le seguenti istruzioni:

[S4] interface Eth-Trunk 1 *//definizione interfaccia logica*

[S4-Eth-Trunk1] mode lacp-static *//modalità utilizzata*

[S4-Eth-Trunk1]trunkport gigabitethernet 0/0/6 *//associazione interfacce fisiche*

[S4-Eth-Trunk1] trunkport gigabitethernet 0/0/7

[S4-Eth-Trunk1] max active-linknumber 1 *//soltanto uno dei due link è attivo*

[S4-Eth-Trunk1] bpdu enable *//abilitazione dei bpdu*

[S4-Eth-Trunk1] interface gigabitethernet 0/0/6

[S4-GigabitEthernet0/0/6] lacp priority 1 *//il traffico veicolerà solo qui, avendo impostato come priorità 1, che è molto alta.*

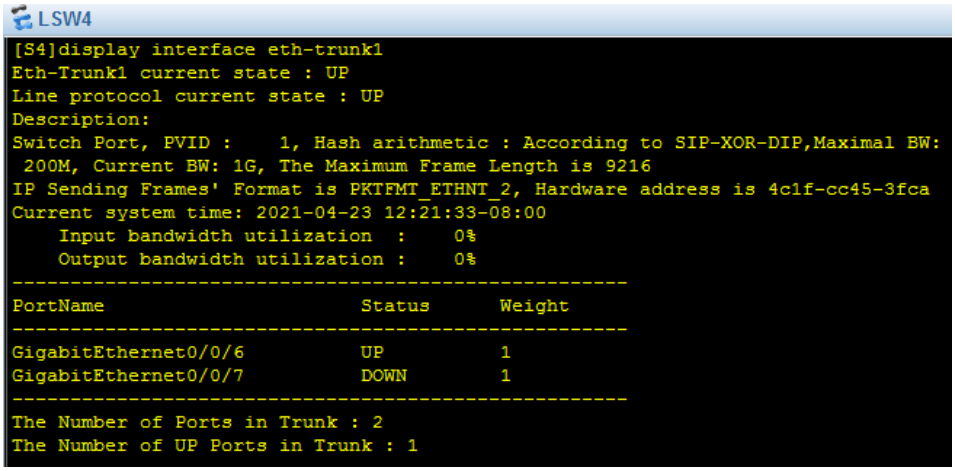


Figura 42 Interfaccia Ethernet-Trunk

Dalla Figura 52 si può notare l'avvenuta creazione dell'Ethernet-Trunk 1, con associate due interfacce fisiche GigabitEthernet 0/0/6 e 0/0/7, dove soltanto la 0/0/6 è UP, data l'istruzione che soltanto un link alla volta può essere attivo.

Per quanto riguarda la trasmissione dei frames, deve essere seguita una metrica, per far sì che essi vengano trasmessi in modo corretto ed ordinato, dato che Ethernet non prevede la numerazione dei frame prima che essi vengano trasmessi.

Il principio base è la creazione di un data flow, ovvero i dati che devono essere inviati, devono avere caratteristiche in comune e molto importante, devono avere stessa velocità e stesso duplex.

Bisognerà quindi scegliere una metrica da seguire tra le seguenti:

1. Stesso SOURCE MAC addresses
2. Stesso DESTINATION MAC addresses

3. Stesso SOURCE IP addresses
4. Stesso DESTINATION IP addresses
5. Stesso SOURCE e DESTINATION MAC addresses
6. Stesso SOURCE e DESTINATION IP addresses

In ogni caso i frames verranno trasmessi sullo stesso link fisico.

VLAN

Con l'introduzione delle VLAN - Virtual LAN è possibile separare hosts appartenenti allo stesso dominio di broadcast in LAN virtuali, permettendo così la connessione di dispositivi anche dislocati fisicamente in luoghi differenti.

L'utilizzo delle VLAN comporta diversi vantaggi, quali risparmio di tempo e denaro, dato che viene utilizzata la stessa struttura fisica di rete, aumento di sicurezza e prestazioni, visto che i frames non vengono propagati verso destinazioni non necessarie e gli hosts sono interessati solamente al traffico delle loro VLAN.

Ogni VLAN avrà un suo identificativo univoco, il VLAN ID che permette di riconoscere la VLAN e tutti i dispositivi che ne andranno a far parte.

Per assegnare le VLAN, esistono cinque modalità:

1. **Port based:** è basato sull'assegnazione delle VLAN in base al numero di porta dello switch. È quella utilizzata di default. Quindi sarà l'amministratore a configurare il PVID da associare ad ogni porta.
2. **MAC based:** le VLAN sono classificate basandosi sul MAC Address del NIC, Network Interface Cards. L'amministratore di rete configurerà il mapping tra i VLAN IDs ed i MAC addresses. In questo caso, nel momento in cui uno switch riceverà un frame untagged, esso cercherà nella MAC-VLAN table, un tag da aggiungere al frame in accordo con il MAC address del frame.

3. **IP subnet based:** si basa sull'indirizzo IP, ovvero, dopo aver ricevuto un frame non taggato, lo switch aggiungerà un tag VLAN con indirizzo IP all'header del pacchetto. Questo metodo è utilizzato nel VOIP.
4. **Protocol based:** i VLAN IDs sono allocati per pacchetti ricevuti nell'interfaccia in accordo con il protocollo utilizzato e con il formato dell'incapsulamento del pacchetto.
5. **Policy based:** è una combinazione di criteri per l'assegnazione dei tag VLAN, inclusi IP subnet, porte e MAC address, dove in ognuno di essi, dovrà avvenire il match, prima che venga assegnata la VLAN.

Ai fini del presente progetto, si considerano solo due possibili modi di funzionamento delle porte:

1. **ACCESS:** le porte access sono associate a link che collegano lo switch ai nodi foglia; essi utilizzano frame untagged, di tipo Ethernet, in quanto gli hosts non hanno sempre la necessità di distinguere il traffico; i dispositivi mittente e destinatario si trovano sulla stessa VLAN e perciò è necessario soltanto specificare l'indirizzo IP destinatario.

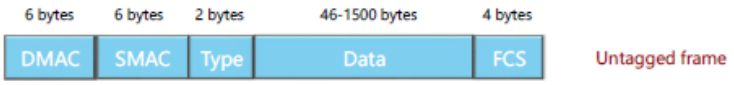


Figura 43 Frame Untagged

In questo caso, al momento della ricezione del frame, gli verrà aggiunto un tag con il default VLAN ID, così da poterlo poi inviare verso il trunk, ovvero verso altri switches.

Le porte access accettano anche frame tagged, ovvero frame Ethernet con aggiunto il campo TAG, contenente diverse informazioni, necessarie per l'inoltro del frame tra VLAN differenti. Il campo TAG conterrà le seguenti informazioni:

- **TPID:** Indica il tipo di frame, se taggato è 0x8100. Quindi ogni campo Tag inizierà con questo valore.
- **PCP – Priority Code Point:** necessario per classificare i frame.
- **DEI – Discard Eligibility Indicator:** indica se il frame può essere scartato, in caso di congestione.
- **VLAN ID:** 12 bit che identificano l'appartenenza del frame ad una VLAN e definito in 802.1Q.

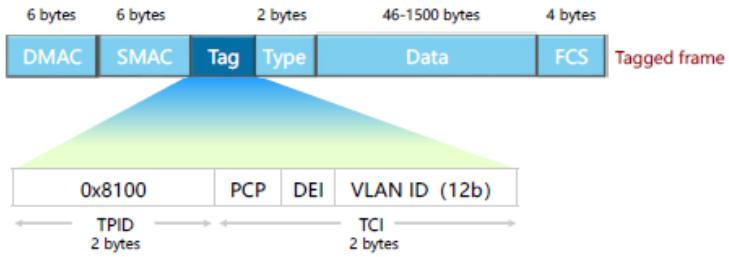


Figura 44 Frame Tagged

Questi frame vengono accettati se c'è una coincidenza tra il VLAN ID del frame e quello di default. In caso affermativo, viene tolto il tag e viene trasmesso il frame.

2. **TRUNK:** le porte trunk hanno associati link aventi il compito di collegare gli switches. Utilizzano frame di tipo tagged ed accettano in ricezione sia frame tagged che untagged.
   Se in ricezione, trovano un frame di tipo untagged, aggiungeranno un tag con il VLAN ID di default del frame e verrà trasmesso solo se quel VLAN ID è permesso alla porta. Se non è ammesso, il frame viene scartato. Se invece trovano un frame tagged, non aggiungono nessun tag, ma controllano se i due VLAN ID matchano; se matchano ed il VLAN ID è ammesso alla porta, viene tolto il tag e trasmesso il frame; se non matchano, viene controllato il permesso di passaggio alla porta; se può passare, viene comunque trasmesso il frame, se

non è ammesso il passaggio, viene scartato. In questo caso, è importante permettere il passaggio al trunk a tutte le VLAN, così da consentire la comunicazione.

Riportando ciò al progetto, sono state introdotte le VLAN, isolando le interfacce facenti parte di uno stesso switch, così da rendere più affidabile ed efficiente la topologia di rete. Per poter far comunicare tutte le VLAN, è stato necessario inserire dei routers; naturalmente gli hosts appartenenti alla stessa VLAN, potranno comunicare tra loro, senza ricorrere al router.

Per capire come organizzare le VLAN, si è partiti dalla topologia logica in Figura 56 e poi, una volta definita la configurazione, sono state "traslate" nella topologia fisica.

Sono state ideate quindi, tre VLAN:

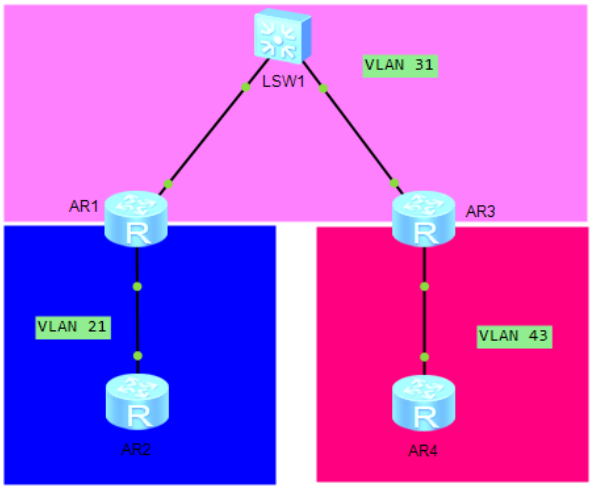


Figura 45 Suddivisione delle VLAN

1. VLAN 21:mette in comunicazione il router 2 con l' 1 e naturalmente tutto ciò che vi è collegato.
2. VLAN 31:unisce i routers 3 ed 1.
3. VLAN 43:unisce i routers 4 e 3.

È stata optata questa scelta, perché in questo modo riescono a comunicare tutti i dispositivi, anche se dislocati fisicamente, senza dar troppo carico alla rete.

Ora riportando la configurazione nella topologia fisica, si vanno ad evidenziare quali dispositivi e quali interfacce faranno parte di ogni VLAN.

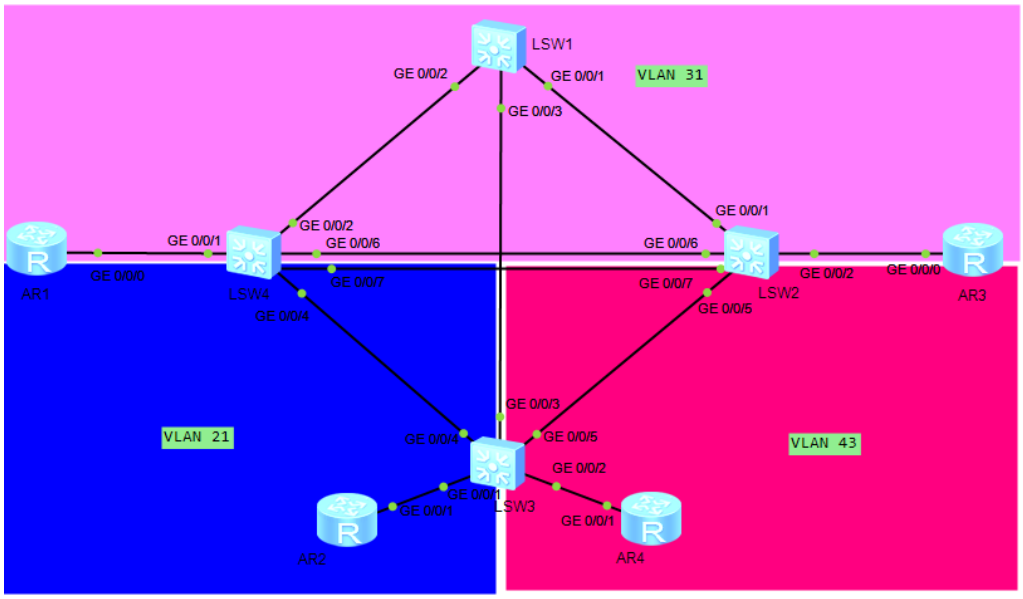


Figura 46 Suddivisione VLAN su topologia fisica

Le VLAN non riguarderanno solo dispositivi di livello 2, come gli switches, ma comprenderanno anche dispositivi di livello 3, ovvero i routers.

Su ogni switch verranno create le tre VLAN con il comando:

[S4] vlan batch 21 31 43

Dopodiché vengono associate le porte alle vlan.

[S4] interface gigabitethernet 0/0/1

[S4-GigabitEthernet0/0/1] port link-type trunk *//si definisce la porta come trunk*

[S4-GigabitEthernet0/0/1] port trunk allow-pass vlan all *//viene permesso il passaggio a tutte le VLAN*

Si eseguono le stesse istruzioni per tutte le altre interfacce dello switch, compreso l'Ethernet Trunk ed in ognuno di esse vengono definite le porte come trunk.

LSW4

```
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp-static
 max active-linknumber 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 stp edged-port enable
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
```

Figura 47 Configurazione porte interfacce e VLAN su switch 4

Qui di seguito si può notare la tabella riassuntiva delle VLAN configurate nello switch 4. Per ogni VLAN vengono elencate le porte Tagged e Untagged ed il loro stato UP o DOWN, rispettivamente indicate con U e D.

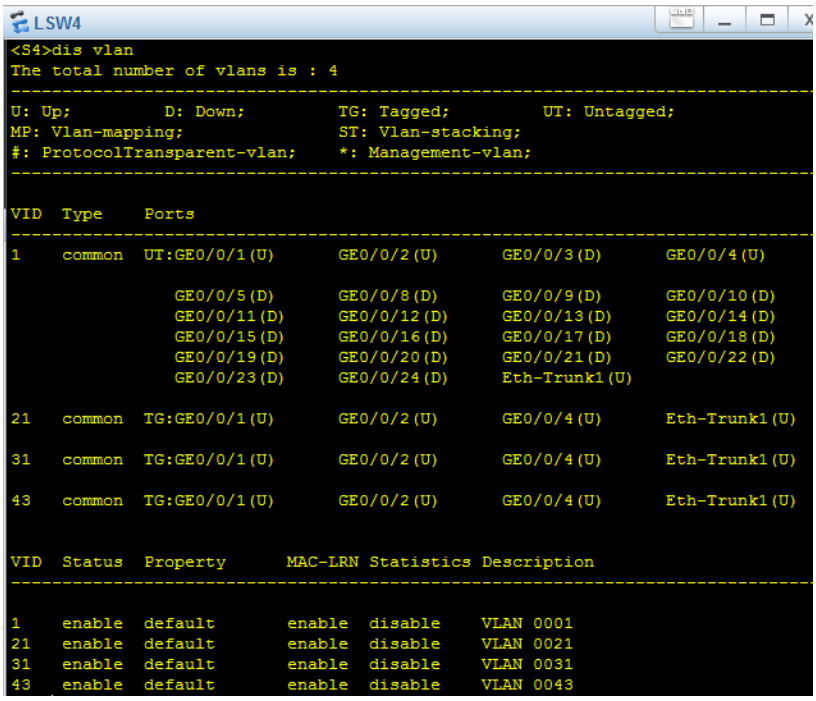


Figura 48 VLAN configurate su switch 4

Lo switch 1 ha tre interfacce, GigabitEthernet 0/0/1, 0/0/2 e 0/0/3, tutte di tipo trunk che lo collegano agli switches 4, 2 e 3.

```
interface GigabitEthernet0/0/1
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
```

Figura 49 Configurazione porte interfacce e VLAN switch 1

```
<S1>dis vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------

1    common  UT:GE0/0/1(U)      GE0/0/2(U)      GE0/0/3(U)      GE0/0/4(D)

                GE0/0/5(D)      GE0/0/6(D)      GE0/0/7(D)      GE0/0/8(D)
                GE0/0/9(D)      GE0/0/10(D)     GE0/0/11(D)     GE0/0/12(D)
                GE0/0/13(D)     GE0/0/14(D)     GE0/0/15(D)     GE0/0/16(D)
                GE0/0/17(D)     GE0/0/18(D)     GE0/0/19(D)     GE0/0/20(D)
                GE0/0/21(D)     GE0/0/22(D)     GE0/0/23(D)     GE0/0/24(D)

21   common  TG:GE0/0/1(U)      GE0/0/2(U)      GE0/0/3(U)

31   common  TG:GE0/0/1(U)      GE0/0/2(U)      GE0/0/3(U)

43   common  TG:GE0/0/1(U)      GE0/0/2(U)      GE0/0/3(U)


VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------

1    enable  default       enable  disable    VLAN 0001
21   enable  default       enable  disable    VLAN 0021
31   enable  default       enable  disable    VLAN 0031
43   enable  default       enable  disable    VLAN 0043
```

Figura 50 VLAN configurate su switch 1

Lo switch 2 ha anch'esso tutte le porte configurate come trunk.

LSW2

```
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp-static
 max active-linknumber 1
#
interface GigabitEthernet0/0/1
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 stp edged-port enable
#
```

Figura 51 Configurazione porte interfacce e VLAN su switch 2

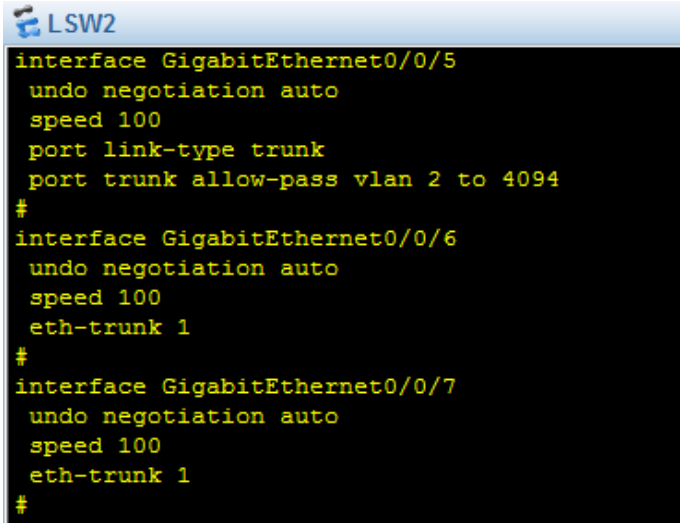


Figura 52 Configurazione porte interfacce e VLAN su switch 2

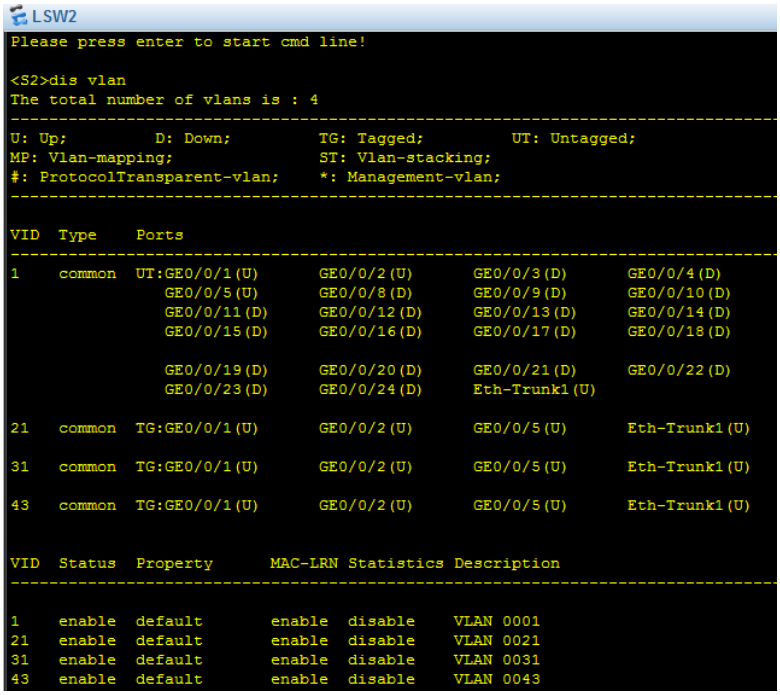


Figura 53 VLAN configurate su switch 2

Invece, nello switch S3, vengono configurate come ACCESS le porte associate alle interfacce GigabitEthernet 0/0/1 e 0/0/2 e gli vengono assegnate le VLAN cui appartengono, utilizzando le seguenti istruzioni:

```
[S3] interface gigabitethernet 0/0/1
[S3-GigabitEthernet0/0/1] port link-type access
```

[S3-GigabitEthernet0/0/1] port default vlan 21 *//associo alla porta la VLAN 21*

[S3] interface gigabitethernet 0/0/2

[S3-GigabitEthernet0/0/1] port link-type access

[S3-GigabitEthernet0/0/1] port default vlan 43

```
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 21
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 43
#
interface GigabitEthernet0/0/3
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/4
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/5
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
```

Figura 54 Configurazione porte interfacce e VLAN su switch 3

```
<S3>dis vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------

1    common  UT:GE0/0/3(U)      GE0/0/4(U)      GE0/0/5(U)      GE0/0/6(D)
               GE0/0/7(D)      GE0/0/8(D)      GE0/0/9(D)      GE0/0/10(D)
               GE0/0/11(D)     GE0/0/12(D)     GE0/0/13(D)     GE0/0/14(D)
               GE0/0/15(D)     GE0/0/16(D)     GE0/0/17(D)     GE0/0/18(D)
               GE0/0/19(D)     GE0/0/20(D)     GE0/0/21(D)     GE0/0/22(D)
               GE0/0/23(D)     GE0/0/24(D)

21   common  UT:GE0/0/1(U)

             TG:GE0/0/3(U)     GE0/0/4(U)      GE0/0/5(U)

31   common  TG:GE0/0/3(U)     GE0/0/4(U)      GE0/0/5(U)

43   common  UT:GE0/0/2(U)

             TG:GE0/0/3(U)     GE0/0/4(U)      GE0/0/5(U)


VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------

1    enable  default       enable  disable    VLAN 0001
21   enable  default       enable  disable    VLAN 0021
31   enable  default       enable  disable    VLAN 0031
43   enable  default       enable  disable    VLAN 0043
```

Figura 55 VLAN configurate su switch 3

Terminata la configurazione delle VLAN sugli switches, si procede con la configurazione dei routers; essi hanno però delle interfacce in comune su più VLAN, per questo sono state introdotte delle sub-interface, ovvero delle interfacce logiche, che permettono al router di processare frames taggati ed appartenenti a VLAN differenti.

Prima di iniziare, è bene riportare la topologia logica contenente gli indirizzi IP che dovranno poi essere assegnati alle interfacce.

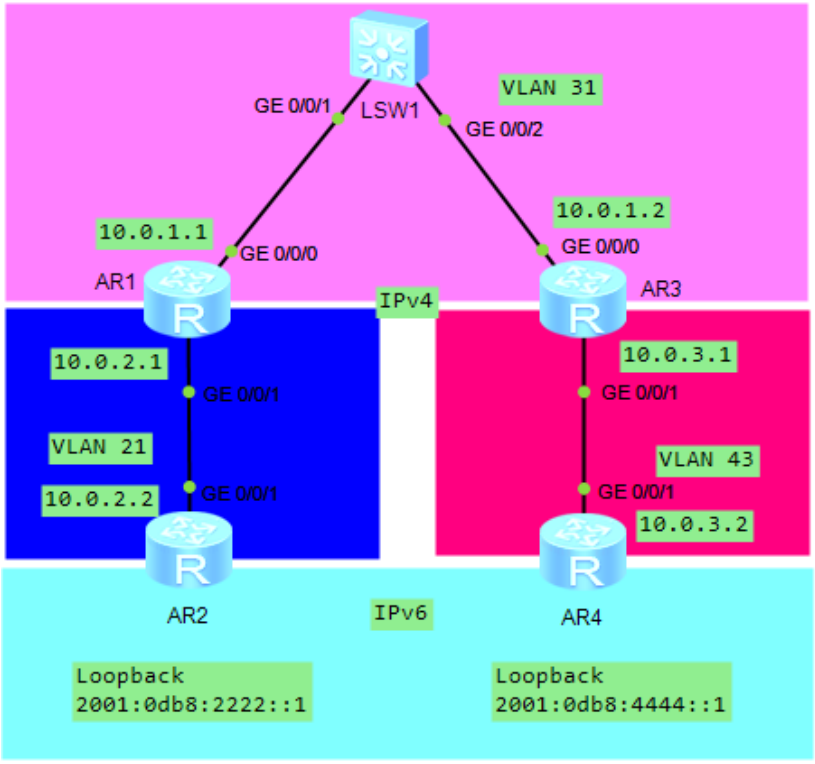


Figura 56 Topologia Logica con indirizzi IP da assegnare

Come indirizzi IP del mondo IPv4, sono stati scelti indirizzi di classe B e per ogni VLAN è stato associato uno spazio di indirizzi differente. Di fatti per la VLAN 21 è stato scelto come spazio di indirizzi il 10.0.2.0, per la VLAN 31, è stato scelto il 10.0.1.0, mentre per la VLAN 43 è stato impostato il 10.0.3.0.

Inoltre, essendo collegate ai routers R2 e R4, due interfacce di Loopback IPv6, ad essi sono stati assegnati rispettivamente gli indirizzi 2001:0db8:2222::1 e 2001:0db8:4444::1.

Ora, partendo dal router R1, sono state create due sotto-interfacce della GigabitEthernet0/0/0, nel seguente modo:

<R1> system-view

[R1] int gigabitethernet 0/0/0

[R1-GigabitEthernet0/0/0] int gigabitethernet 0/0/0.1 *//creazione sotto-interfaccia*

[R1-GigabitEthernet0/0/0.1] dot1q termination vid 31 *//associazione della sub-interface alla VLAN 31, quindi quando arriverà il pacchetto al router, all'interno del campo tag troverà questa associazione alla VLAN.*

[R1-GigabitEthernet0/0/0.1] ip address 10.0.1.1 255.255.255.0 *//associazione dell'indirizzo IP all'interfaccia*

[R1-GigabitEthernet0/0/0.1] arp broadcast enable *//abilitazione dell'arp, il protocollo utilizzato per conoscere l'indirizzo MAC, noto l'indirizzo IP*

[R1] int gigabitethernet 0/0/0

[R1-GigabitEthernet0/0/0] int gigabitethernet 0/0/0.2

[R1-GigabitEthernet0/0/0.2] dot1q termination vid 21

[R1-GigabitEthernet0/0/0.2] ip address 10.0.2.1 255.255.255.0

[R1-GigabitEthernet0/0/0.2] arp broadcast enable

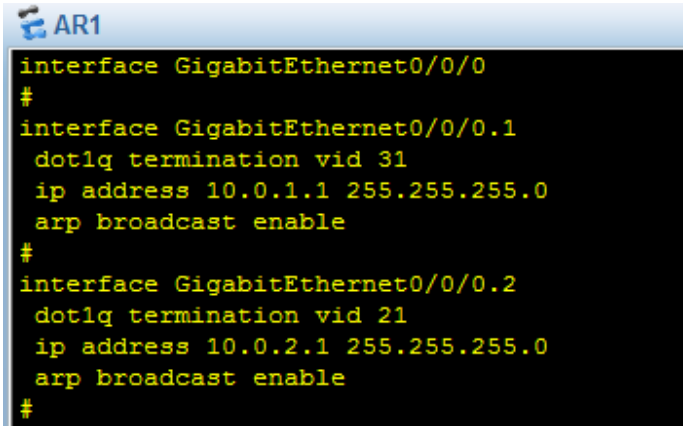


Figura 57 Creazione sub-interface sul router 1

Anche per il router 3 sono state configurate due subinterface, una collegata alla VLAN 31 ed una collegata alla VLAN 43.

```
[R3] int gigabitethernet 0/0/0

[R3-GigabitEthernet0/0/0] int gigabitethernet 0/0/0.1

[R3-GigabitEthernet0/0/0.1] dot1q termination vid 31

[R3-GigabitEthernet0/0/0.1] ip address 10.0.1.2 255.255.255.0

[R3-GigabitEthernet0/0/0.1] arp broadcast enable

[R3] int gigabitethernet 0/0/0

[R3-GigabitEthernet0/0/0] int gigabitethernet 0/0/0.2

[R3-GigabitEthernet0/0/0.2] dot1q termination vid 43

[R3-GigabitEthernet0/0/0.2] ip address 10.0.3.1 255.255.255.0

[R3-GigabitEthernet0/0/0.2] arp broadcast enable
```

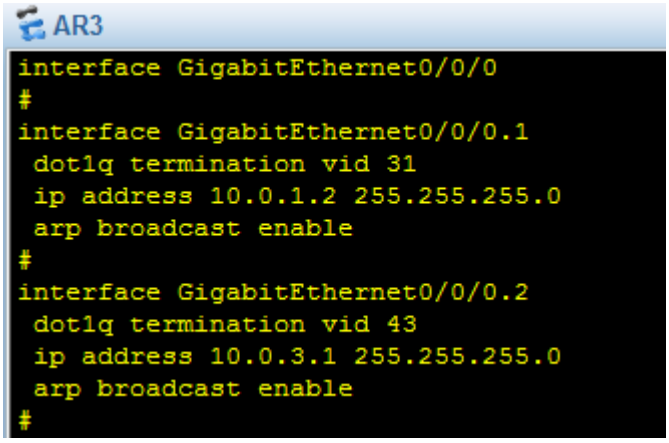


Figura 58 Creazione sub-interface su router 3

Invece, i routers 2 e 4 hanno un'interfaccia legata al mondo IPv4 e l'altra al mondo IPv6.

Il router 2 avrà l'interfaccia GigabitEthernet0/0/1 associata all'IPv4 con indirizzo 10.0.2.2 e la loopback IPv6 con indirizzo 2001:0db8:2222::1.

[R2] interface gigabitethernet0/0/1

[R2-GigabitEthernet0/0/1] ip address 10.0.2.2 255.255.255.0

[R2] ipv6 *//entra in IPv6 sul router R2*

[R2] interface loopback0 *//abilita IPv6 per l'interfaccia loopback0*

[R2-LoopBack0] ipv6 enable *//assegna un indirizzo IPv6 link-local all'interfaccia*

[R2-LoopBack0] ipv6 address 2001:0db8:2222::1 64

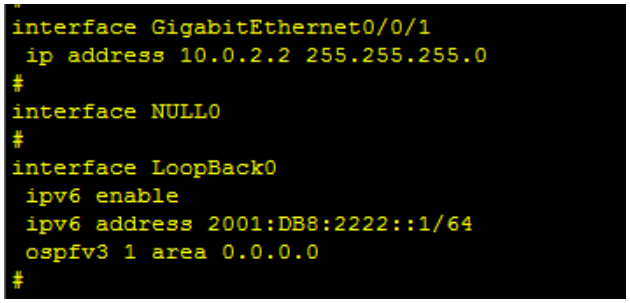


Figura 59 Abilitazione IPv6 e assegnazione indirizzi su router 2

Il router 4 invece, avrà l'interfaccia GigabitEthernet0/0/1 associata all'indirizzo IPv4 10.0.3.2 e la loopback associata all'indirizzo IPv6 2001:0db8:4444::1.

```
[R4] interface gigabitethernet0/0/1

[R4-GigabitEthernet0/0/1] ip address 10.0.3.2 255.255.255.0

[R4] ipv6

[R4] interface loopback0

[R4-LoopBack0] ipv6 enable

[R4-LoopBack0] ipv6 address 2001:0db8:4444::1 64
```

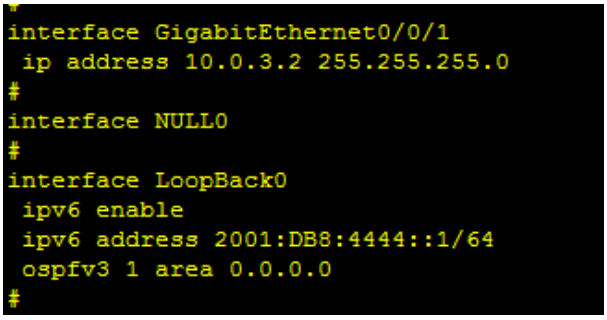


Figura 60 Abilitazione IPv6 e assegnazione indirizzi su router 4

OSPF

Per far sì che avvenga l'instradamento all'interno delle due reti, possono essere utilizzati due tipi di protocolli:

1. Protocolli che utilizzano il Distance Vector: il più noto è il RIPv2.
2. Protcolli che utilizzano il Link State: il più noto è OSPF.

In questo caso, sono stati scelti OSPF per IPv4 ed OSPFv3 per IPv6.

OSPF – Open Shortest Path First è un protocollo di routing basato sulla tecnologia link state, dove ogni nodo costruisce una propria mappa della connettività della rete e calcolerà in modo indipendente il next hop migliore verso una qualsiasi

destinazione, andando a popolare una sua tabella di routing, a differenza dei protocolli basati su distance vector che seguono una metrica unica, basata sul conteggio dei next hop, che possono essere al massimo 15.

Il funzionamento di OSPF può essere diviso in 3 fasi:

1. **Network Discovery:** un router che abbia un protocollo OSPF attivo, deve cercare i suoi routers vicini in modo tale da potergli chiedere eventuali informazioni sugli spazi di indirizzi.
2. **Topology Database Exchange:** i routers collaborano tra loro per scambiare informazioni sulla topologia. Si scambiano informazioni sul link, in modo che le informazioni possano essere inserite all'interno di un link state database.
3. **Route computation:** ogni router ha una sua visione sul percorso migliore da seguire. Quindi ogni router in modo indipendente, analizza le informazioni topologiche e sceglie la miglior rotta verso una destinazione secondo la sua prospettiva, a differenza del distance vector, che si basa su ciò che viene comunicato dai routers vicini.

I vantaggi di OSPF sono che può essere eseguito anche "sopra" altri protocolli come MPLS, che si occupa di instradare il traffico IP; minimizza l'overhead necessario allo scambio dati dei routers, quindi ci sarà più spazio per il traffico utente.

Altri punti di forza sono la rapidità nella convergenza nel caso in cui la topologia di rete vari, la scalabilità, ovvero la capacità di variare la dimensione della rete e metriche accurate, basate sulle velocità delle interfacce.

L'unico svantaggio è che richiede memoria e CPU per permettere la gestione del database.

FUNZIONAMENTO

OSPF definisce una gerarchia su due livelli che costituiscono i domini di instradamento e sono: il routing intra-area, per i routers interni ed il routing inter-area, per i routers di confine. Grazie a questa divisione, OSPF viene utilizzato specialmente nelle reti di grandi dimensioni, così da ridurre le tabelle di instradamento.

Come detto, vengono introdotte delle aree, cioè insiemi di routers aventi lo stesso database, accomunati dalle stesse informazioni. In ogni topologia si ha sempre l'AREA 0 o Transit Area, ovvero l'area addetta al transito veloce dei pacchetti IP.

Ogni nodo conosce solo il percorso più breve verso le varie destinazioni ed inoltra tali informazioni verso i routers di confine, che a loro volta informeranno i routers di altri sistemi autonomi, trasmettendo in ciascuna area, un riassunto delle informazioni raccolte nell'area attuale.

I routers si scambieranno dei pacchetti, detti LSA – Link State Advertisement, contenenti informazioni sullo stato dei link, che verranno poi inseriti all'interno del database, LSDB. Su di esso verrà poi fatto eseguire OSPF e attraverso il calcolo delle rotte, verranno scelte quelle con costo minore e verranno inserite nella tabella di routing.

L'elemento distintivo è il ROUTER ID, un valore di 32 bit, necessario per identificare il router in modo univoco all'interno di una rete.

OSPF può lavorare sia in una rete di tipo broadcast che point-to-point.

Al momento dell'accensione i due routers, seguiranno il seguente diagramma a stati per arrivare ad una delle due configurazioni, Neighbor o Adjacent. Con la relazione neighbor, i routers vicini

si scambiano solo una parte delle informazioni al momento del bisogno, mentre con Adjacent vengono scambiate tutte le informazioni presenti sul database.

I routers si troveranno inizialmente nello stato di down, per poi iniziare un processo di “scoperta” dei vicini, inviando degli Hello Packets. Si entra così nell’Init. Ogni router determina il costo dei propri rami uscenti e nel momento in cui riceve una risposta sottoforma di Hello Packet, contenente il router ID del router che ha risposto, gli inoltrerà un Hello Packets con le sue informazioni. In questo modo il primo router capisce che è stato visto e quindi stabilisce una connessione 2-Way e verrà creata una relazione di vicinanza. Ogni nodo continua comunque a monitorare i costi dei link, effettuando il ricalcolo sulla base dell’algoritmo di Dijkstra ed in caso noti qualche variazione, la invierà ai routers. Se la comunicazione tra vicini diventa inattiva ed è stato già effettuato un tentativo per ristabilire la comunicazione, mediante l’invio periodico di Hello Packet, allora si passerà allo stato Attempt.

I routers come DR e BDR, rispettivamente Designated Router e Backup Designated Router, andranno a costituire, nelle reti broadcast, una relazione di stato adiacente con i routers vicini, andandosi a scambiare informazioni sullo stato dei link, in modo ordinato, così da formare il database.

Ciò richiede che i routers passino per lo stato ExStart, dove è richiesto di stabilire una relazione di tipo master-slave tra i routers e scambino un numero di sequenza utile per capire quanti dati sono stati trasferiti.

I vicini possono identificare percorsi di cui non sono a conoscenza o di cui non sono in possesso di informazioni aggiornate e pertanto possono richiedere dettagli aggiuntivi per queste rotte, come parte dello stato di caricamento.

Con lo stato ExChange, i due routers scambiano i pacchetti di tipo DD – Database Description e vengono numerati, cosicché possano verificare la corretta ricezione.

Il router analizza allora le informazioni ricevute e nel caso di lacune, le richiede al vicino, utilizzando pacchetti LSR – Link State Request, ai quali fanno seguito dei pacchetti LSU – Link State Update. Il router carica allora nel database le informazioni mancanti e così dallo stato loading si passa allo stato full. A questo punto, le informazioni che vengono scambiate sono riguardo la raggiungibilità degli spazi di indirizzi. Ciò serve per avere un database coerente. Una volta scambiate tali informazioni, si avrà una visione generale della rete e attraverso OSPF si potranno prendere decisioni riguardanti l'instradamento.

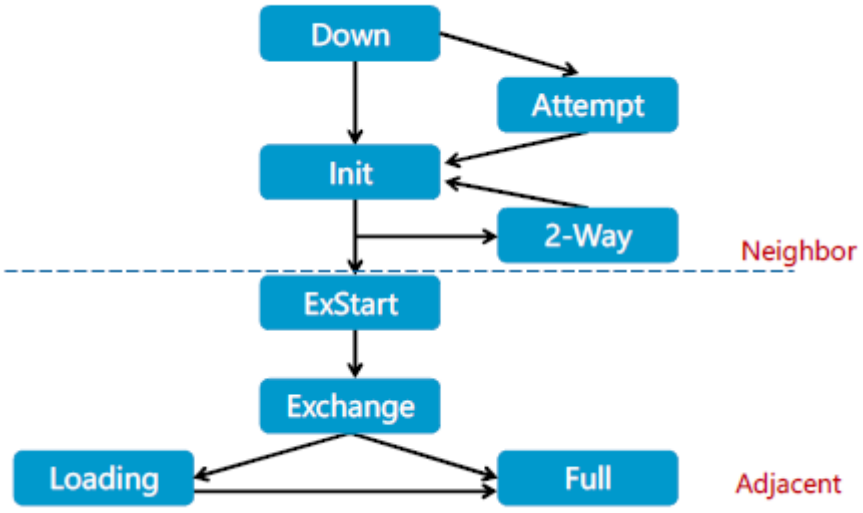


Figura 61 Diagramma a stati per stabilire relazioni tra routers

Gli Hello packet che vengno inviati sono formati nel seguente modo:

Hello Interval	Option	Router Priority
Router Dead Interval		
Designated Router		
Backup Designated Router		
Neighbor		

- **Hello interval:** è un timer che indica ogni quanto vengono inviati quei pacchetti, solitamente è 10 sec per le reti broadcast e 30 per le reti peer-to-peer.
- **Router priority:** priorità del router.
- **Router Dead Interval:** è 4xHelloTime, quindi 40 secondi per broadcast e 120 per le peer-to-peer.

La metrica utilizzata da OSPF è basata sulla larghezza di banda delle interfacce. Per determinare il costo della metrica, si deve eseguire il seguente calcolo: 10^8/larghezza di banda. Il termine al numeratore deve essere omogeneo con i routers che partecipano alla topologia, altrimenti potrebbero assegnare valori differenti di costo ai link.

Il costo è assegnabile anche dall'amministratore.

Riportando ciò alla topologia studiata, prima di tutto sono stati assegnati i router ID ai routers, dopodiché viene creata un'unica area, l'area 0, dato che non si tratta di una rete molto grande e vi si sono state associate le rispettive reti.

OSPF dovrà essere attivato su tutti i routers, in quanto "appartengono" al mondo IPv4.

Come per gli indirizzi IP si aveva la subnet mask, in questo caso viene introdotta la Wildcard Mask. Essa viene utilizzata per confrontare indirizzi e/o maschere. I bit con valore 0 indicano che deve esserci corrispondenza, mentre i bit a 1 vengono ignorati.

```
[R1]router-id 1.1.1.1
[R1] ospf 1 router-id 1.1.1.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0] network 10.0.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 10.0.2.0 0.0.0.255

[R3]router-id 3.3.3.3
[R3] ospf 1 router-id 3.3.3.3
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0] network 10.0.1.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0] network 10.0.3.0 0.0.0.255

[R2]router-id 2.2.2.2
[R2] ospf 1 router-id 2.2.2.2
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0] network 10.0.2.0 0.0.0.255

[R4]router-id 4.4.4.4
[R4] ospf 1 router-id 4.4.4.4
[R4-ospf-1]area 0
[R4-ospf-1-area-0.0.0.0] network 10.0.3.0 0.0.0.255
```

Con il comando “display ip routing-table” si può vedere come è stata popolata la tabella per l’instradamento dei pacchetti.

Infatti per ogni destinazione, viene visualizzato il protocollo utilizzato, con il costo per arrivare a quella destinazione, il next hop e l'interfaccia.

Ad esempio per arrivare all'indirizzo 10.0.3.0, viene utilizzato OSPF come protocollo di instradamento e si passa per l'indirizzo 10.0.1.2, con un costo pari a 2.

AR1

```
<R1>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/24  Direct  0    0           D   10.0.1.1        GigabitEthernet
0/0/0.1
        10.0.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.1
      10.0.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.1
        10.0.2.0/24  Direct  0    0           D   10.0.2.1        GigabitEthernet
0/0/0.2
        10.0.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.2
      10.0.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.2
        10.0.3.0/24  OSPF    10   2           D   10.0.1.2        GigabitEthernet
0/0/0.1
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 62 Routing-table router 1

Invece, per visualizzare i vicini del router 1, si utilizza il comando "display ospf peer". Il peer collegato a R1 è il router avente ID 3.3.3.3 ed indirizzo 10.0.1.2 ed hanno stabilito una full adiacency.

Il router con indirizzo 10.0.1.2 è stato eletto DR, mentre il 10.0.1.1 è stato eletto come BDR.

```
<R1>dis ospf peer

      OSPF Process 1 with Router ID 1.1.1.1
            Neighbors

 Area 0.0.0.0 interface 10.0.1.1(GigabitEthernet0/0/0.1)'s neighbors
 Router ID: 3.3.3.3          Address: 10.0.1.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.1.2  BDR: 10.0.1.1  MTU: 0
   Dead timer due in 38  sec
   Retrans timer interval: 5
   Neighbor is up for 00:33:07
   Authentication Sequence: [ 0 ]

            Neighbors

 Area 0.0.0.0 interface 10.0.2.1(GigabitEthernet0/0/0.2)'s neighbors
 Router ID: 2.2.2.2          Address: 10.0.2.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.2.2  BDR: 10.0.2.1  MTU: 0
   Dead timer due in 25  sec
   Retrans timer interval: 5
   Neighbor is up for 00:32:37
   Authentication Sequence: [ 0 ]
```

Figura 63 Vicini OSPF del router 1

Invece con il comando “display ospf 1 brief” vengono mostrate tutte la aree configurate con le principali informazioni delle interfacce collegate.

```
<R1>dis ospf 1 bri

      OSPF Process 1 with Router ID 1.1.1.1
            OSPF Protocol Information

 RouterID: 1.1.1.1          Border Router:
 Multi-VPN-Instance is not enabled
 Global DS-TE Mode: Non-Standard IETF Mode
 Graceful-restart capability: disabled
 Helper support capability   : not configured
 Applications Supported: MPLS Traffic-Engineering
 Spf-schedule-interval: max 10000ms, start 500ms, hold 1000ms
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Route Preference: 10
 ASE Route Preference: 150
 SPF Computation Count: 15
 RFC 1583 Compatible
 Retransmission limitation is disabled
 Area Count: 1   Nssa Area Count: 0
 ExChange/Loading Neighbors: 0
 Process total up interface count: 2
 Process valid up interface count: 2

 Area: 0.0.0.0          (MPLS TE not enabled)
 Authtype: None   Area flag: Normal
 SPF scheduled Count: 15
 ExChange/Loading Neighbors: 0
 Router ID conflict state: Normal
 Area interface up count: 2

 Interface: 10.0.1.1 (GigabitEthernet0/0/0.1)
 Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 10.0.1.2
 Backup Designated Router: 10.0.1.1
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1

 Interface: 10.0.2.1 (GigabitEthernet0/0/0.2)
 Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 10.0.2.2
 Backup Designated Router: 10.0.2.1
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

Figura 64 Aree configurate con OSPF

Con “display ospf 1 lsdb” viene visualizzato invece, il database del router R1.

```
<R1>dis ospf 1 lsdb

      OSPF Process 1 with Router ID 1.1.1.1
            Link State Database

                  Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    4.4.4.4         4.4.4.4            275  36    8000000A       1
 Router    2.2.2.2         2.2.2.2            278  36    8000000A       1
 Router    1.1.1.1         1.1.1.1            281  48    8000000F       1
 Router    3.3.3.3         3.3.3.3            280  48    80000011       1
 Network   10.0.3.2        4.4.4.4            275  32    80000005       0
 Network   10.0.2.2        2.2.2.2            278  32    80000005       0
 Network   10.0.1.2        3.3.3.3            302  32    80000005       0
```

Figura 65 Database OSPF router 1

Vengono visualizzate le tabelle di instradamento con le configurazioni di ogni router.

```
<R2>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/24  OSPF    10   2           D   10.0.2.1        GigabitEthernet
0/0/1
        10.0.2.0/24  Direct  0    0           D   10.0.2.2        GigabitEthernet
0/0/1
        10.0.2.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
      10.0.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
        10.0.3.0/24  OSPF    10   3           D   10.0.2.1        GigabitEthernet
0/0/1
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 66 Routing-table router 2

```
<R2>dis ospf 1 lsdb

      OSPF Process 1 with Router ID 2.2.2.2
            Link State Database

                  Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    4.4.4.4         4.4.4.4            445  36    8000000A       1
 Router    2.2.2.2         2.2.2.2            447  36    8000000A       1
 Router    1.1.1.1         1.1.1.1            452  48    8000000F       1
 Router    3.3.3.3         3.3.3.3            450  48    80000011       1
 Network   10.0.3.2        4.4.4.4            445  32    80000005       0
 Network   10.0.2.2        2.2.2.2            447  32    80000005       0
 Network   10.0.1.2        3.3.3.3            472  32    80000005       0
```

Figura 67 Database OSPF router 2

```
<R3>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/24  Direct  0    0           D   10.0.1.2        GigabitEthernet
0/0/0.1
        10.0.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.1
      10.0.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.1
        10.0.2.0/24  OSPF    10   2           D   10.0.1.1        GigabitEthernet
0/0/0.1
        10.0.3.0/24  Direct  0    0           D   10.0.3.1        GigabitEthernet
0/0/0.2
        10.0.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.2
      10.0.3.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0.2
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 68 Routing-table router 3

```
<R3>dis ospf 1 lsdb

       OSPF Process 1 with Router ID 3.3.3.3
             Link State Database

                   Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    4.4.4.4         4.4.4.4            556  36    8000000A       1
 Router    2.2.2.2         2.2.2.2            561  36    8000000A       1
 Router    1.1.1.1         1.1.1.1            564  48    8000000F       1
 Router    3.3.3.3         3.3.3.3            561  48    80000011       1
 Network   10.0.3.2        4.4.4.4            556  32    80000005       0
 Network   10.0.2.2        2.2.2.2            561  32    80000005       0
 Network   10.0.1.2        3.3.3.3            583  32    80000005       0
```

Figura 70 Database OSPF router 3

```
<R4>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/24  OSPF    10   2           D   10.0.3.1        GigabitEthernet
0/0/1
        10.0.2.0/24  OSPF    10   3           D   10.0.3.1        GigabitEthernet
0/0/1
        10.0.3.0/24  Direct  0    0           D   10.0.3.2        GigabitEthernet
0/0/1
        10.0.3.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
      10.0.3.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Figura 69 Routing-table router 4

```
<R4>dis ospf 1 lsdb

      OSPF Process 1 with Router ID 4.4.4.4
            Link State Database

                  Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    4.4.4.4         4.4.4.4            770  36    8000000A       1
 Router    2.2.2.2         2.2.2.2            777  36    8000000A       1
 Router    1.1.1.1         1.1.1.1            780  48    8000000F       1
 Router    3.3.3.3         3.3.3.3            777  48    80000011       1
 Network   10.0.3.2        4.4.4.4            770  32    80000005       0
 Network   10.0.2.2        2.2.2.2            777  32    80000005       0
 Network   10.0.1.2        3.3.3.3            799  32    80000005       0
```

Figura 71 Database OSPF router 4

OSPFv3

Sui routers 2 e 4 verrà abilitato anche OSPFv3, una versione di OSPF che supporta gli indirizzi IPv6. Quando vengono attivati i dispositivi e OSPF, si scambieranno degli Hello Packets attraverso i link-local FF02::5, indirizzo riservato a tutti i routers OSPF o FF02::6, indirizzo per tutti i DR. Anche in OSPFv3 il router ID ha un ruolo importante per l'identificazione e viene espresso in dot-dot, che riportato al router in oggetto R2, è 2.2.2.2. A differenza degli Hello Packet di OSPF, quelli di OSPFv3 non hanno più indicazioni riguardo gli indirizzi ma si riferiscono solo all'interface ID.

Per concludere il lavoro e quindi far comunicare le interfacce di Loopback ed i due mondi, è necessario introdurre un tunnel, il tunnel GRE tra il router 2 e 4.

TUNNEL GRE

Il tunnel GRE – Generic Routing Encapsulation viene introdotto per superare le limitazioni di IPSec, uno standard avente come obiettivo di garantire delle comunicazioni sicure fra due end-point, ma permettono il passaggio soltanto a pacchetti IP.

Con il tunnel GRE è possibile trasmettere qualsiasi formattazione ed eseguire protocolli che IPSec avrebbe bloccato. Con GRE aumenta la versatilità, a discapito della sicurezza, in quanto non è cifrato. Per questo molte volte vengono utilizzati insieme.

Con l'aggiunta del tunnel GRE è possibile far girare OSPFv3 anche nella parte di rete IPv6, permettendo così la comunicazione tra tutti i dispositivi della topologia.

Il GRE incapsula pacchetti di dati con un header che viene aggiunto all'interno di un pacchetto IP; il nuovo pacchetto sarà così formato:

Figura 72 Incapsulamento Gre

Nell'header IP il campo protocol è istanziato con valore 47, che indica appunto il GRE.

L'header di GRE invece, è abbastanza complesso, contiene diverse informazioni tra le quali l'autenticazione. Quando il bit di K dell'header è settato a 1, si può valorizzare il campo Key, configurando l'autenticazione.

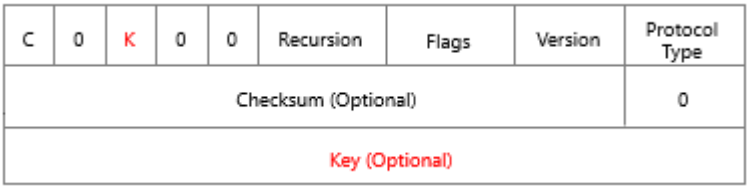


Figura 73 Header Gre

Un'altra funzione del GRE è il Keepalive, un sistema che consente di monitorare lo stato del tunnel. I messaggi di keepalive vengono inviati per verificare l'attività del tunnel. Se in un lasso di tempo, non vengono ricevuti questi messaggi, si considera il tunnel inattivo.

Nei routers 2 e 4, dopo aver configurato il GRE, viene abilitato OSPFv3 anche su di esso.

```
[R2] interface tunnel 0/0/1
[R2] tunnel-protocol gre
[R2] ipv6 enable
[R2] ipv6 address 2001:0db8:5555::1 64
[R2] source 10.0.2.2
```

```
[R2] destination 10.0.3.2
```

```
[R4] interface tunnel 0/0/1
[R4] tunnel-protocol gre
[R4] ipv6 enable
[R4] ipv6 address 2001:0db8:5555::2 64
[R4] source 10.0.3.2
[R4] destination 10.0.2.2
```

```
[R2]dis interface Tunnel0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.2.2 (GigabitEthernet0/0/1), destination 10.0.3.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2021-05-01 21:01:58-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Figura 74 Interfaccia Tunnel GRE su router 2

```
[R4]dis int Tunnel0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.3.2 (GigabitEthernet0/0/1), destination 10.0.2.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2021-05-01 21:05:39-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Figura 75 Interfaccia Tunnel GRE su router 4

Per far sì che OSPFv3 lavori correttamente, esso deve essere abilitato su ogni interfaccia.

```
[R2] ipv6
[R2] ospfv3
[R2-ospfv3-1]router-id 2.2.2.2
[R2] interface gigabitethernet 0/0/0
[R2-GigabitEthernet0/0/0] ospfv3 1 area 0
[R2] interface loopback0
[R2-LoopBack0] ospfv3 1 area 0
[R4] interface Tunnel 0/0/1
[R4-Tunnel0/0/1] ospfv3 1 area 0
```

//una volta configurato il tunnel, viene abilitato OSPFv3 anche sul tunnel GRE.

```
[R2]dis ipv6 routing-table
Routing Table : Public
      Destinations : 7  Routes : 7

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 2001:DB8:2222::              PrefixLength : 64
 NextHop      : 2001:DB8:2222::1             Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : LoopBack0                    Flags        : D

 Destination  : 2001:DB8:2222::1             PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : LoopBack0                    Flags        : D

 Destination  : 2001:DB8:4444::1             PrefixLength : 128
 NextHop      : FE80::A00:302                Preference   : 10
 Cost         : 1562                         Protocol     : OSPFv3
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : Tunnel0/0/1                  Flags        : D

 Destination  : 2001:DB8:5555::              PrefixLength : 64
 NextHop      : 2001:DB8:5555::1             Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : Tunnel0/0/1                  Flags        : D

 Destination  : 2001:DB8:5555::1             PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : Tunnel0/0/1                  Flags        : D
```

Figura 76 IPv6 routing-table router 2 con OSPFv3

```
[R2]dis ipv6 routing-table protocol ospfv3
Public Routing Table : OSPFv3
Summary Count : 3

OSPFv3 Routing Table's Status : < Active >
Summary Count : 1

 Destination  : 2001:DB8:4444::1               PrefixLength : 128
 NextHop      : FE80::A00:302                  Preference   : 10
 Cost         : 1562                           Protocol     : OSPFv3
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Tunnel0/0/1                    Flags        : D

OSPFv3 Routing Table's Status : < Inactive >
Summary Count : 2

 Destination  : 2001:DB8:2222::1               PrefixLength : 128
 NextHop      : ::                             Preference   : 10
 Cost         : 0                              Protocol     : OSPFv3
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : LoopBack0                      Flags        :

 Destination  : 2001:DB8:5555::                PrefixLength : 64
 NextHop      : ::                             Preference   : 10
 Cost         : 1562                           Protocol     : OSPFv3
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Tunnel0/0/1                    Flags        :

 Destination  : FE80::                         PrefixLength : 10
 NextHop      : ::                             Preference   : 0
 Cost         : 0                              Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : NULL0                          Flags        : D
```

Figura 77 IPv6 routing-table router 2 con OSPFv3

```
[R4] ipv6

[R4] ospfv3

[R4-ospfv3-1]router-id 4.4.4.4

[R4] interface gigabitethernet 0/0/0

[R4-GigabitEthernet0/0/0] ospfv3 1 area 0

[R4] interface loopback0

[R4-LoopBack0] ospfv3 1 area 0

[R4] interface Tunnel 0/0/1

[R4-Tunnel0/0/1] ospfv3 1 area 0
```

```
<R4>dis ipv6 routing-table
Routing Table : Public
      Destinations : 7  Routes : 7

 Destination  : ::1                              PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : InLoopBack0                      Flags        : D

 Destination  : 2001:DB8:2222::1                 PrefixLength : 128
 NextHop      : FE80::A00:202                    Preference   : 10
 Cost         : 1562                             Protocol     : OSPFv3
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : Tunnel0/0/1                      Flags        : D

 Destination  : 2001:DB8:4444::                  PrefixLength : 64
 NextHop      : 2001:DB8:4444::1                 Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : LoopBack0                        Flags        : D

 Destination  : 2001:DB8:4444::1                 PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : LoopBack0                        Flags        : D

 Destination  : 2001:DB8:5555::                  PrefixLength : 64
 NextHop      : 2001:DB8:5555::2                 Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : Tunnel0/0/1                      Flags        : D

 Destination  : 2001:DB8:5555::2                 PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : Tunnel0/0/1                      Flags        : D

 Destination  : FE80::                           PrefixLength : 10
 NextHop      : ::                               Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : NULL0                            Flags        : D
```

Figura 79 IPv6 routing-table con OSPFv3 router 4

```
<R4>dis ipv6 routing-table protocol ospfv3
Public Routing Table : OSPFv3
Summary Count : 3

OSPFv3 Routing Table's Status : < Active >
Summary Count : 1

 Destination  : 2001:DB8:2222::1                PrefixLength : 128
 NextHop      : FE80::A00:202                   Preference   : 10
 Cost         : 1562                            Protocol     : OSPFv3
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

OSPFv3 Routing Table's Status : < Inactive >
Summary Count : 2

 Destination  : 2001:DB8:4444::1                PrefixLength : 128
 NextHop      : ::                              Preference   : 10
 Cost         : 0                               Protocol     : OSPFv3
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : LoopBack0                       Flags        :

 Destination  : 2001:DB8:5555::                 PrefixLength : 64
 NextHop      : ::                              Preference   : 10
 Cost         : 1562                            Protocol     : OSPFv3
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        :
```

Figura 78 IPv6 routing-table con OSPFv3 router 4

La tabella di indirizzamento che si otterrà per i due routers saranno le seguenti:

AR4

```
Routing Table : Public
      Destinations : 7  Routes : 7

 Destination  : ::1                             PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : InLoopBack0                     Flags        : D

 Destination  : 2001:DB8:2222::1                PrefixLength : 128
 NextHop      : FE80::A00:202                   Preference   : 10
 Cost         : 1562                            Protocol     : OSPFv3
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

 Destination  : 2001:DB8:4444::                 PrefixLength : 64
 NextHop      : 2001:DB8:4444::1                Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : LoopBack0                       Flags        : D

 Destination  : 2001:DB8:4444::1                PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : LoopBack0                       Flags        : D

 Destination  : 2001:DB8:5555::                 PrefixLength : 64
 NextHop      : 2001:DB8:5555::2                Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

 Destination  : 2001:DB8:5555::2                PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

 Destination  : FE80::                          PrefixLength : 10
 NextHop      : ::                              Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : NULL0                           Flags        : D
```

Figura 80 Tabella di indirizzamento router 4

AR2

```
Routing Table : Public
      Destinations : 7  Routes : 7

 Destination  : ::1                             PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : InLoopBack0                     Flags        : D

 Destination  : 2001:DB8:2222::                 PrefixLength : 64
 NextHop      : 2001:DB8:2222::1                Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : LoopBack0                       Flags        : D

 Destination  : 2001:DB8:2222::1                PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : LoopBack0                       Flags        : D

 Destination  : 2001:DB8:4444::1                PrefixLength : 128
 NextHop      : FE80::A00:302                   Preference   : 10
 Cost         : 1562                            Protocol     : OSPFv3
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

 Destination  : 2001:DB8:5555::                 PrefixLength : 64
 NextHop      : 2001:DB8:5555::1                Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

 Destination  : 2001:DB8:5555::1                PrefixLength : 128
 NextHop      : ::1                             Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : Tunnel0/0/1                     Flags        : D

 Destination  : FE80::                          PrefixLength : 10
 NextHop      : ::                              Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : NULL0                           Flags        : D
```

Figura 81 Tabella indirizzamento router 2

CONCLUSIONI

In questo progetto di tesi si è dimostrato come, utilizzando opportunamente le VLAN, sia possibile realizzare una topologia logica che risponde a delle precise esigenze di connettività e che prescinde dal modo in cui, fisicamente, sono collegati gli apparati. Questo approccio può essere anche "dinamico" ed è alla base delle tecnologie emergenti SDN.

Utilizzando OSPF, un protocollo di routing dinamico, gli spazi di indirizzi IPv4 associati ai routers sono stati resi mutuamente raggiungibili. Le reti aziendali, con indirizzamento IPv6, sono state collegate tra loro sfruttando GRE ed il protocollo OSPFv3.

Qui di seguito viene visualizzato l'effettivo funzionamento della topologia realizzata, effettuando dei ping tra i routers.

```
<R1>ping 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=255 time=100 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=255 time=120 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=255 time=90 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=255 time=90 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 80/96/120 ms

    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=100 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=90 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=90 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=100 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 70/90/100 ms

<R1>ping 10.0.3.1
  PING 10.0.3.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.1: bytes=56 Sequence=1 ttl=255 time=60 ms
    Reply from 10.0.3.1: bytes=56 Sequence=2 ttl=255 time=110 ms
    Reply from 10.0.3.1: bytes=56 Sequence=3 ttl=255 time=70 ms
    Reply from 10.0.3.1: bytes=56 Sequence=4 ttl=255 time=90 ms
    Reply from 10.0.3.1: bytes=56 Sequence=5 ttl=255 time=80 ms

  --- 10.0.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/82/110 ms

<R2>ping 10.0.3.2
  PING 10.0.3.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.2: bytes=56 Sequence=1 ttl=253 time=310 ms
    Reply from 10.0.3.2: bytes=56 Sequence=2 ttl=253 time=250 ms
    Reply from 10.0.3.2: bytes=56 Sequence=3 ttl=253 time=290 ms
    Reply from 10.0.3.2: bytes=56 Sequence=4 ttl=253 time=270 ms
    Reply from 10.0.3.2: bytes=56 Sequence=5 ttl=253 time=290 ms

  --- 10.0.3.2 ping statistics ---
    5 packet(s) transmitted
```

Figura 82 Ping da router 1

```
<R2>ping 10.0.2.1
  PING 10.0.2.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.1: bytes=56 Sequence=1 ttl=255 time=100 ms
    Reply from 10.0.2.1: bytes=56 Sequence=2 ttl=255 time=90 ms
    Reply from 10.0.2.1: bytes=56 Sequence=3 ttl=255 time=100 ms
    Reply from 10.0.2.1: bytes=56 Sequence=4 ttl=255 time=120 ms
    Reply from 10.0.2.1: bytes=56 Sequence=5 ttl=255 time=110 ms

  --- 10.0.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 90/104/120 ms
<R2>ping 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=254 time=200 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=254 time=170 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=254 time=160 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=254 time=160 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=254 time=180 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 160/174/200 ms

<R2>ping 10.0.3.1
  PING 10.0.3.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.1: bytes=56 Sequence=1 ttl=254 time=180 ms
    Reply from 10.0.3.1: bytes=56 Sequence=2 ttl=254 time=160 ms
    Reply from 10.0.3.1: bytes=56 Sequence=3 ttl=254 time=170 ms
    Reply from 10.0.3.1: bytes=56 Sequence=4 ttl=254 time=170 ms
    Reply from 10.0.3.1: bytes=56 Sequence=5 ttl=254 time=180 ms

  --- 10.0.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 160/172/180 ms

<R2>ping 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=255 time=110 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=255 time=80 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=255 time=90 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=255 time=100 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 80/92/110 ms
<R2>ping ipv6 2001:0db8:4444::1
  PING 2001:0db8:4444::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001:DB8:4444::1
    bytes=56 Sequence=1 hop limit=64  time = 350 ms
    Reply from 2001:DB8:4444::1
    bytes=56 Sequence=2 hop limit=64  time = 250 ms
    Reply from 2001:DB8:4444::1
    bytes=56 Sequence=3 hop limit=64  time = 250 ms
    Reply from 2001:DB8:4444::1
    bytes=56 Sequence=4 hop limit=64  time = 280 ms
    Reply from 2001:DB8:4444::1
    bytes=56 Sequence=5 hop limit=64  time = 260 ms

  --- 2001:0db8:4444::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 250/278/350 ms

<R2>ping 10.0.3.2
  PING 10.0.3.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.2: bytes=56 Sequence=1 ttl=253 time=310 ms
    Reply from 10.0.3.2: bytes=56 Sequence=2 ttl=253 time=250 ms
    Reply from 10.0.3.2: bytes=56 Sequence=3 ttl=253 time=290 ms
    Reply from 10.0.3.2: bytes=56 Sequence=4 ttl=253 time=270 ms
    Reply from 10.0.3.2: bytes=56 Sequence=5 ttl=253 time=290 ms

  --- 10.0.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 250/282/310 ms
```

Figura 84 Ping da router 2

```
<R3>ping 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=255 time=100 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=255 time=80 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=255 time=80 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=255 time=70 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=255 time=100 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 70/86/100 ms

<R3>ping 10.0.2.1
  PING 10.0.2.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.1: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 10.0.2.1: bytes=56 Sequence=2 ttl=255 time=100 ms
    Reply from 10.0.2.1: bytes=56 Sequence=3 ttl=255 time=80 ms
    Reply from 10.0.2.1: bytes=56 Sequence=4 ttl=255 time=110 ms
    Reply from 10.0.2.1: bytes=56 Sequence=5 ttl=255 time=90 ms

  --- 10.0.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 80/92/110 ms

<R3>ping 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=254 time=160 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=254 time=200 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=254 time=180 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=254 time=160 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=254 time=170 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 160/174/200 ms
<R3>ping 10.0.3.2
  PING 10.0.3.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.2: bytes=56 Sequence=1 ttl=255 time=100 ms
    Reply from 10.0.3.2: bytes=56 Sequence=2 ttl=255 time=100 ms
    Reply from 10.0.3.2: bytes=56 Sequence=3 ttl=255 time=100 ms
    Reply from 10.0.3.2: bytes=56 Sequence=4 ttl=255 time=90 ms
    Reply from 10.0.3.2: bytes=56 Sequence=5 ttl=255 time=110 ms

  --- 10.0.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 90/100/110 ms
```

Figura 86 Ping da router 3

```
<R4>ping ipv6 2001:0db8:2222::1
  PING 2001:0db8:2222::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=1 hop limit=64  time = 290 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=2 hop limit=64  time = 240 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=3 hop limit=64  time = 240 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=4 hop limit=64  time = 260 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=5 hop limit=64  time = 250 ms

  --- 2001:0db8:2222::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 240/256/290 ms
```

Figura 85 Ping da router 4

```
<R4>ping 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=200 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=160 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=170 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=160 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=170 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 160/172/200 ms

<R4>ping 10.0.2.1
  PING 10.0.2.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.1: bytes=56 Sequence=1 ttl=254 time=180 ms
    Reply from 10.0.2.1: bytes=56 Sequence=2 ttl=254 time=160 ms
    Reply from 10.0.2.1: bytes=56 Sequence=3 ttl=254 time=160 ms
    Reply from 10.0.2.1: bytes=56 Sequence=4 ttl=254 time=180 ms
    Reply from 10.0.2.1: bytes=56 Sequence=5 ttl=254 time=180 ms

  --- 10.0.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 160/172/180 ms

<R4>ping 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=253 time=270 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=253 time=250 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=253 time=270 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=253 time=250 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=253 time=260 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 250/260/270 ms

<R4>ping 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=253 time=220 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=253 time=220 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=253 time=220 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=253 time=230 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=253 time=220 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 220/222/230 ms

<R4>ping ipv6 2001:0db8:2222::1
  PING 2001:0db8:2222::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=1 hop limit=64  time = 220 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=2 hop limit=64  time = 220 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=3 hop limit=64  time = 210 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=4 hop limit=64  time = 200 ms
    Reply from 2001:DB8:2222::1
    bytes=56 Sequence=5 hop limit=64  time = 210 ms

  --- 2001:0db8:2222::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 200/212/220 ms
```

Figura 87 Ping da router 4

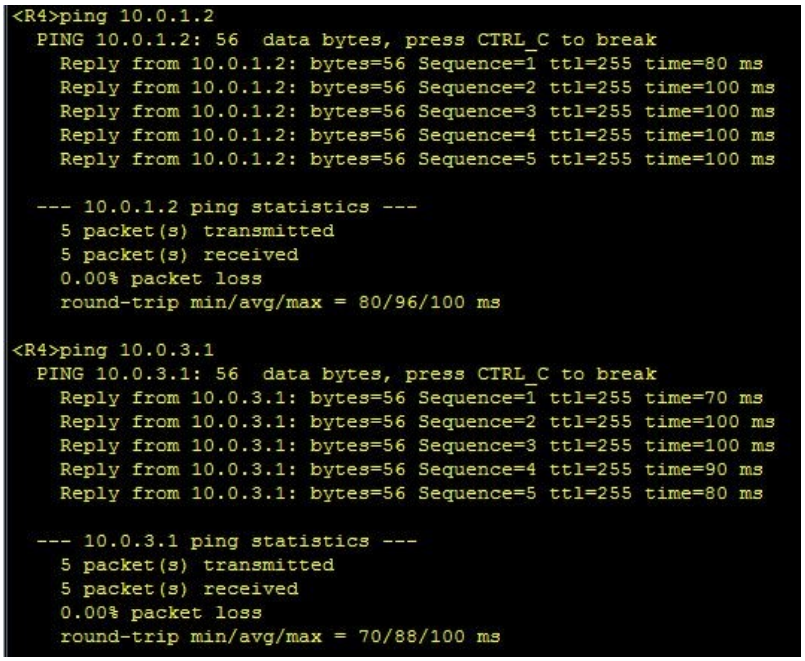


Figura 88 Ping da router 4

Qui di seguito sono state inserite le configurazioni finali di tutti i dispositivi.

```
sysname R4
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
ipv6
#
router id 4.4.4.4
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
```

```
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
ospfv3 1
 router-id 4.4.4.4
#
firewall zone Local
 priority 15
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
 ip address 10.0.3.2 255.255.255.0
#
interface NULL0
#
interface LoopBack0
 ipv6 enable
 ipv6 address 2001:DB8:4444::1/64
 ospfv3 1 area 0.0.0.0
#
interface Tunnel0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:5555::2/64
 ospfv3 1 area 0.0.0.0
 tunnel-protocol gre
 source 10.0.3.2
 destination 10.0.2.2
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
```

```
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return


sysname R2
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
ipv6
#
router id 2.2.2.2
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
ospfv3 1
 router-id 2.2.2.2
#
firewall zone Local
 priority 15
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
```

```
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
 ip address 10.0.2.2 255.255.255.0
#
interface NULL0
#
interface LoopBack0
 ipv6 enable
 ipv6 address 2001:DB8:2222::1/64
 ospfv3 1 area 0.0.0.0
#
interface Tunnel0/0/1
 ipv6 enable
 ipv6 address 2001:DB8:5555::1/64
 ospfv3 1 area 0.0.0.0
 tunnel-protocol gre
 source 10.0.2.2
 destination 10.0.3.2
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
Return


sysname R3
```

```
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
router id 3.3.3.3
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/0.1
 dot1q termination vid 31
```

```
 ip address 10.0.1.2 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/0.2
 dot1q termination vid 43
 ip address 10.0.3.1 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/1
#
interface NULL0
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.3.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
Return
```

```
sysname R1
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
router id 1.1.1.1
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
```

```
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/0.1
 dot1q termination vid 31
 ip address 10.0.1.1 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/0.2
 dot1q termination vid 21
 ip address 10.0.2.1 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/1
#
interface NULL0
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.2.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
```

```
wlan ac
#
return


sysname S4
#
vlan batch 21 31 43
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface Eth-Trunk1
 mode lacp-static
 max active-linknumber 1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
```

```
#
interface GigabitEthernet0/0/4
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
 undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 1
#
interface GigabitEthernet0/0/7
 undo negotiation auto
 speed 100
 eth-trunk 1
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
```

```
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
return


sysname S3
#
vlan batch 21 31 43
#
stp mode rstp
stp instance 0 root secondary
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 21
#
interface GigabitEthernet0/0/2
 port link-type access
```

```
 port default vlan 43
#
interface GigabitEthernet0/0/3
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/4
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/5
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
```

```
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
port-group def
#
return


sysname S2
#
vlan batch 21 31 43
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface Eth-Trunk1
```

```
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp-static
 max active-linknumber 1
#
interface GigabitEthernet0/0/1
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/6
 undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 1
#
interface GigabitEthernet0/0/7
 undo negotiation auto
 speed 100
 eth-trunk 1
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
```

```
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
Return
```

```
sysname S1
May  3 2021 16:10:26-08:00 S1 %%01PHY/1/PHY(l)[57]:
GigabitEthernet0/0/1: cha
nge status to up
#
vlan batch 21 31 43
#
stp mode rstp
stp instance 0 root primary
<S1>dis curr conf
#
sysname S1
#
vlan batch 21 31 43
#
stp mode rstp
stp instance 0 root primary
#
cluster enable
ntdp enable
ndp enable
```

```
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
 undo negotiation auto
 speed 100
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
```

```
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
return
```

BIBLIOGRAFIA

Dispense Huawei HCIA Routing & Switching

“Sistemi e Reti 1” L. Lo Russo, E. Bianchi , Hoepli

“Sistemi e Reti 2” L. Lo Russo, E. Bianchi , Hoepli

https://www.ionos.it/digitalguide/server/know-how/nozioni-di-base-sulla-vlan/

https://e.huawei.com/it/products/enterprise-networking/routers/ar-g3/ar12001

https://www.google.com/url?sa=i&url=http%3A%2F%2Fwww.highteck.net%2FIT%2FApplication%2FFunzionalita_e_protocolli_del_livello_Application.html&psig=AOvVaw1Z_4eYs75DWsOfhB3tutRJ&ust=1618645552504000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCOjqi-CigvACFQAAAAAdAAAAABAV

https://www.ilsoftware.it/articoli.asp?tag=Cavi-ethernet-differenze-e-caratteristiche_11964

https://www.ionos.it/digitalguide/server/know-how/il-modello-isoosi-per-gli-standard-e-i-protocolli/

https://lh3.googleusercontent.com/proxy/LN2UZ9qum3dJ759G1dede1sV3XVxj7AlE0u5PAJGJaUmxLHT2G4TIKCvRZVzDmXMcc-dTHBmIKP50qB21HL4X0KWNdeFMTIomgpybgBxNZjaovh4PymfHr4T

https://www.certificationkits.com/cisco-certification/cisco-ccna-640-802-exam-certification-guide/cisco-ccna-spanning-tree-protocol-stp-part-i/

https://support.huawei.com/enterprise/en/info-finder/switches/s5700-pid-6691579/

https://www.cavel.it/it/supporto-tecnico/scegli-il-cavo-adatto/scelta-del-cavo-lan-rete-ethernet

https://www.ibm.com/docs/it/i/7.1?topic=concepts-ipv6-address-types#ipv6addrtypes

https://upload.wikimedia.org/wikipedia/commons/d/d5/Virtualbox_logo.png

https://www.codexsprawl.com/wp-content/uploads/2016/02/caaumno1.png

https://www.juniper.net/documentation/us/en/software/junos/interfaces-ethernet-switches/topics/topic-map/switches-interface-gre.html#id-understanding-generic-routing-encapsulation

https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

https://www.netsetup.it/networking/54-rstp-rapid-spanning-tree-protocol

https://www.ionos.it/digitalguide/server/know-how/frame-ethernet/

https://www.cisco.com/c/it_it/solutions/small-business/resource-center/networking/network-switch-how.html#~switch-non-gestiti

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-1sg/ip6-route-ospfv3.html

https://www.ionos.it/digitalguide/server/know-how/presentazione-dei-protocolli-tcpip/

https://www.ionos.it/digitalguide/server/know-how/nozioni-di-base-sulla-vlan/

RINGRAZIAMENTI

In questo mio percorso di tesi, mi sento di ringraziare diverse persone, che sono state fondamentali per me.

In primis, il Professor Ennio Gambi, che si è subito attivato per potermi assegnare un argomento più vicino alle mie preferenze.

Al secondo posto, vorrei ringraziare l'Ingegnere Adelmo De Santis, che ha giocato un ruolo importante per lo svolgimento del progetto, fornendomi sostegno, chiarimenti e aiutandomi nei momenti in cui "non funzionava più nulla".

Dopodiché, vorrei ringraziare la mia famiglia, i miei amici e Flavio che mi sono stati sempre vicini, donandomi sostegno, aiuto, conforto, gioia e risate in questo percorso universitario.

In particolare, un grazie va a mio padre, Fabio, a cui dedico questa prima laurea, come sua rivincita.

Un grazie a mia madre, Romina, che con le sgridate, mi ha sempre invogliato a fare di meglio.

Un grazie a mia sorella Gloria, che ad ogni esame si presentava con un cornetto portafortuna, sostenendomi.

Un grazie al mio ragazzo Flavio, che con la sua simpatia e la sua dolcezza mi ha aiutato a portare a termine il mio progetto.

Un grazie alle mie migliori amiche, Valentina e Martina, che mi hanno accompagnato in tutto il percorso, aiutandomi a gestire le ansie, i momenti di sconforto ma anche le gioie che mi ha portato questo percorso.

Un ringraziamento speciale va alla mia Professoressa, Paola, una combattente che porto nel cuore!

Infine, ringrazio anche tutte le altre persone, parenti ed amici, che gioiscono con me, per questo traguardo raggiunto!