Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

Implementazione di OSPF in Architettura di Rete L3 Multivendor

OSPF Implementation in Multivendor L3 Network Architecture

Relatore:
Prof. Ennio Gambi

Tesi di Laurea di:
Antonio Smargiassi

Correlatore:
Ing. Adelmo De Santis

Anno Accademico 2023-2024

Abstract

This thesis, developed in the context of the Huawei HCIA-Datacom certification preparation course, describes the implementation of a heterogeneous network consisting of four routers from different vendors, in which the dynamic routing protocol OSPF is implemented.

The paper includes a description of the hardware used and theoretical recalls on the technologies and protocols employed. The complete configuration of the various devices is presented in detail, highlighting the differences between the various manufacturers' operating systems. Finally, simple methods are illustrated to verify the correct configuration and the achievement of the desired network operation.

The work demonstrates that, with the acquired knowledge, a student can build a multivendor network architecture, configure it to implement a dynamic routing protocol and verify the complete reachability of the network.

Sommario

Questa tesi, sviluppata nell'ambito del corso di preparazione alla certificazione Huawei HCIA-Datacom, descrive la realizzazione di una rete eterogenea composta da quattro router di fornitori diversi, in cui é implementato il protocollo di routing dinamico OSPF.

Il documento include una descrizione dell'hardware utilizzato e dei richiami teorici sulle tecnologie e protocolli impiegati. Viene presentata la configurazione completa dei vari dispositivi in maniera dettagliata, mettendo in evidenza le differenze tra i sistemi operativi dei diversi produttori. Infine, vengono illustrati metodi semplici per verificare la corretta configurazione e il raggiungimento del funzionamento desiderato della rete.

Il lavoro dimostra come, grazie alle conoscenze acquisite, uno studente possa realizzare un'architettura di rete multivendor, configurarla per implementare un protocollo di routing dinamico e verificare la completa raggiungibilitá della rete.

Indice

Elenco delle figure

Capitolo 1

Introduzione

1.1 Contesto

Questa tesi nasce nell'abito del corso di preparazione alla certificazione Huawei HCIA-Datacom[1] offerto dall'Universitá Politecnica delle Marche, che permette agli studenti di approfondire le tematiche del mondo networking e applicarle praticamente nelle esercitazioni nel Laboratorio di Information and Communication Technologies (ICT).

L'obiettivo di questo lavoro di tesi è di implementare una topologia di rete multivendor che consenta di ottenere la completa raggiungibilità di ogni nodo della rete implementando il protocollo di routing dinamico OSPF.

La topologia presentata in questa tesi comprende apparati di diversi produttori; in ambito aziendale è infatti naturale trovarsi ad operare in ambienti multivendor. Ciò può essere causato da restrizioni economiche o dalla volontá di mantenere una parte di rete preesistente. L'adozione di una strategia multivendor può essere dovuta alla necessità di sfruttare le caratteristiche e funzionalitá specifiche di diversi prodotti o da considerazioni di sicurezza, poiché l'utilizzo di dispositivi di diversi fornitori può ridurre il rischio di vulnerabilità comuni. Un ulteriore fattore é la disponibilitá di supporto tecnico, dalla qualitá del servizio post-vendita offerto e in generale della facilitá e comoditá di installazione e manutenzione degli apparati percepita al momento dell'acquisto.

Al giorno d'oggi per qualsiasi azienda, indipendentemente dal settore di appartenenza e dai servizi e prodotti offerti, la connessione interna e verso la rete globale sono diventate necessitá. Internet, con il suo insieme di protocolli, standard e tecnologie, è definibile una "tecnologia abilitante", ovvero un'innovazione la cui applicazione provoca un cambiamento notevole delle capacitá e possibilitá dei suoi utenti.

Uno degli elementi chiave del successo di Internet risiede nella sua standardizzazione a strati, che consente di passare dalla comunicazione di segnali elettrici su brevi distanze allo scambio di informazioni e servizi su scala globale. Quando si opera su un certo livello si può ignorare lo scopo e il funzionamento dei livelli inferiori e superiori, riducendo significativamente la complessitá e offrendo una notevole scalabilitá. Tipici modelli a strati usati per rappresentare le reti di connessione sono il modello ISO-OSI (Open System Interconnection) a 7 strati (fisico, collegamento dati,

rete, trasporto, sessione, presentazione, applicazione) e il modello equivalente TCP/IP (Transmission Control Protocol/Internet Protocol) a 5 strati (fisico, collegamento dati, rete, trasporto, applicazione). Il sistema descritto in questa tesi si basa esclusivamente sull'uso di router, dispositivi che operano al livello 3 , ovvero "rete", in entrambi i modelli menzionati. Il livello 3, noto anche in inglese come "network layer" o "internet layer", è responsabile del trasporto dei dati dalla rete di origine a quella di destinazione tramite un processo chiamato instradamento o "routing".

Un protocollo di livello 3 deve permettere il riconoscimento e l'indirizzamento dei vari dispositivi o interfacce di rete; il protocollo piú usato é indubbiamente il protocollo IP (Internet Protocol), nella sua versione 4 (indicato come IPv4), che usa indirizzi lunghi 32 bit. Gli indirizzi IPv4 sono stati definitivamente esauriti, portando alla nascita del protocollo IPv6 (con indirizzi di 128 bit); tuttavia per mantenere la compatibilitá con le reti e i dispositivi giá esistenti si usano abitualmente indirizzi privati IPv4 nelle reti domestiche e aziendali.

Ogni singolo dispositivo capace di comunicare tramite il protocollo IP possiede una tabella delle rotte (routing table) che contiene le informazioni per inoltrare i pacchetti IP verso la loro destinazione. Nelle routing table sono innanzitutto presenti i collegamenti diretti, ma si posssono aggiungere anche rotte statiche (static routing) dando manualmente indicazioni sulla raggiunbilitá delle reti non direttamente connesse. Le rotte statiche sono adatte a reti di piccole dimensioni e stabili, ma hanno degli svantaggi: in caso di cambiamenti nella topologia di rete devono essere corrette manualmente e in caso di reti di grandi dimensioni la configurazione diventa lunga e ripetitiva. Dunque i router hanno la possibilitá di aggiornare automaticamente le loro routing table sulla base di informazioni ricevute da altri router, realizzando cosí un routing dinamico.

Il routing dinamico necessita di protocolli per permettere ai router di scambiarsi informazioni sulle reti a loro connesse. Esempi di protocolli di routing dinamico sono OSPF, IS-IS e BGP.

1.2 Il progetto

La topologia di rete da realizzare è mostrata nella Figura 1.1, che contiene anche i nomi dei diversi apparati utilizzati e gli indirizzi di livello 3 (IPv4) scelti per le varie interfacce. Per ottenere la completa raggiungibilitá deve essere implementato nei quattro dispositivi il protocollo di routing dinamico OSPF. Si possono notare nei router, R1 e R2, le interfacce virtuali "Loopback", usate per simulare la presenza di ulteriori segmenti di rete e verificare la loro raggiungibilitá. Le reti usate sono tutte parte dello spazio di indirizzi privati 192.168.0.0/16 (192.168.0.0 – 192.168.255.255), diviso in sottoreti con lunghezza della parte di rete (netmask length) di 24 bit[1]. Il

[1]Gli indirizzi IPv4 sono espressi in "Dotted Decimal Notation", ovvero i 32 bit sono separati in quattro gruppi di 8 bit e il valore di ogni ottetto é espresso con notazione decimale. Il numero che segue "/" indica quanti bit appartengono alla parte di rete, che appunto identifica una rete.

valore decimale del terzo byte indica i nomi dei due router connessi (ad esempio la rete 192.168.13.0/24 collega il router 1 al router 3), mentre il quarto byte indica il router al quale appartiene l'interfaccia. Le interfacce Loopback hanno come terzo byte 11 o 22, a indicare che soltanto un router è effettivamente presente in tale rete. Fa eccezione a questo schema la rete che connette il router 4 al PC, in cui l'interfaccia del router ha indirizzo IP 192.168.1.1 (comunemente usato per i gateway e gli access point domestici) e il PC ottiene un indirizzo tramite il protocollo DHCP.

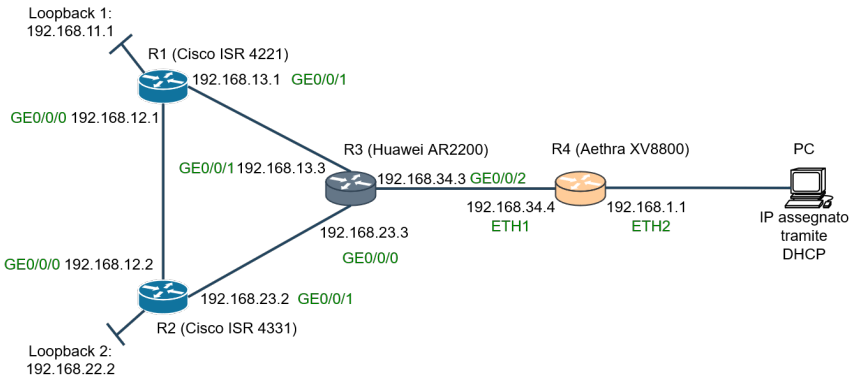


Figura 1.1: Topologia realizzata[2]

1.3 Struttura della tesi

Dopo aver esposto una introduzione generale al tema della tesi e aver dato una descrizione del progetto da realizzare, é presente una breve presentazione dei dispositivi utilizzati. Ad essa segue una spiegazione dei concetti teorici rilevanti per il progetto, come OSPF, DHCP, ping e traceroute.

La parte piú importante contiene la procedura di configurazione dei router nel dettaglio, con sottosezioni dedicate a ciascun apparato.

A ció segue la descrizione delle verifiche effettuate per assicurarsi di aver raggiunto lo scopo del progetto, ovvero la completa raggiungibilità della rete tramite routing dinamico.

Al termine sono presenti alcune considerazioni su possibili espansioni del progetto e una sintesi dei risultati.

[2] disegno realizzato tramite diagrams.net

Capitolo 2

Dispositivi

2.1 Cisco ISR 4221

Un aspetto centrale di questa tesi è la compresenza di più produttori; in questo secondo capitolo sono descritti brevemente i disposti utilizzati. Il router Cisco ISR 4221[2] é un "branch router" prodotto dall'azienda americana *Cisco Systems, inc.* appartenente alla serie 4000. Possiede due porte Ethernet (standard RJ-45), 4 GB di RAM e 8 GB di flash memory.

La configurazione di questo dispositivo, come tutti gli altri, é stata effettuata tramite command line interface (CLI). Per accedere alla console si deve utilizzare un cavo seriale; nel caso particolare del laboratorio tale cavo é connesso ad un server MOXA che permette di accedere alla console del router tramite la connessione telnet ad una particolare porta TCP.

2.2 Cisco ISR 4331

Anche il router Cisco ISR 4331[3] é un "branch router" prodotto dalla *Cisco Systems, inc.* e appartenente alla serie 4000. Possiede 4 GB di RAM, 4 GB di memoria flash e tre porte WAN: una GE (GigabitEthernet, per connessioni in rame), una SFP (Small Form Factor Pluggable, ottica) e una GE/SFP.

A differenza del precedente, é stato configurato collegandosi direttamente alla porta di console tramite un adattatore USB/seriale, usando i classici parametri 9600-8-N-1 (9600 bit/s; 8 bit di dati; nessun bit di paritá; 1 bit di stop).

2.3 Huawei AR2220

Il router Huawei AR2220[4] é uno dei router presenti nel Laboratorio di Information and Communication Technologies (ICT) del Dipartimento di Ingegneria dell'Informazione dell'Universitá Politecnica delle Marche in cui possono esercitarsi gli studenti del corso di preparazione alla certificazione Huawei HCIA-Datacom. Prodotto dalla *Huawei Technologies Co., Ltd.*, possiede tre porte GigabitEthernet, 2 GB di RAM e 2 GB di flash memory.

Anche la console di questo router é connessa al server MOXA ed é accessibile tramite una connessione telnet.

2.4 Aethra XV8800

Il router Aethra XV8800[5] é una piattaforma universale CPE (Customer Premise Equipment) per piccole e medie imprese prodotta dall'azienda *Aethra Telecommunications*. Possiede 2 porte Ethernet/SFP, uno switch LAN a 8 porte e WiFi integrato.

Il suo processore x86 Intel Atom C3000 rende possibili la Network Functions Virtualization e il Software Defined Networking.

Il collegamento alla porta di console é possibile tramite un adattatore USB/seriale, mantenendo i parametri 8-N-1, ma con velocitá di trasmissione 115200 bit/s.

(a) Sottofigura 1. Cisco ISR 4221

(b) Sottofigura 2. Cisco ISR 4331

(c) Sottofigura 3. Huawei AR2220

(d) Sottofigura 4. Aethra XV8800

Figura 2.1: Router utilizzati

Capitolo 3

Richiami teorici

3.1 OSPF

OSPF[6] (Open Shortest Path First) é un protocollo di routing dinamico di tipo link-state. A differenza di un protocollo di tipo distance-vector, in cui i dispositivi si scambiano i contenuti delle loro routing table, in un protocollo di routing link-state i router condividono informazioni sui loro collegamenti. I router stabiliscono tra loro una relazione di vicinato e si scambiano LSA (Link State Advertisement) che contengono informazioni sullo stato delle interfacce a loro direttamente connesse.

Ogni router mantiene un proprio LSDB (Link State Database), in cui vengono aggiunti i LSA ricevuti, dunque esso contiene la descrizione di tutte la interfacce della rete e dell'intera topologia. In seguito ogni router determina il percorso ottimale verso ogni spazio di indirizzi noto nella rete tramite il suo LSDB e l'algoritmo SPF (Shortest Path First), considerando anche una metrica basata sulla velocitá di ogni collegamento rispetto ad una banda di riferimento. Infine, ogni router genera le rotte basate sui percorsi ricavati dall'algoritmo SPF e le aggiunge nella sua routing table.

Di default il costo per interfacce che operano a 1 Gbit/s é 10; nei vari sistemi si puó cambiare la banda di riferimento, oppure la banda del collegamento oppure direttamente il costo. Non é importante in questo contesto poiché tutte le interfacce della rete considerata lavorano alla stessa velocitá.

Un dominio OSPF é una rete formata da disposivi OSPF contigui che usano gli stessi parametri. In caso di reti molto grandi, per ridurre le dimensioni dei LSDB e le risorse consumate dal processo OSPF, ogni rete puó essere divisa in gruppi logici chiamati "aree", ognuna con un suo identificativo, in cui tutti i LSDB sono sincronizzati. L'area 0 esiste sempre ed é definita "backbone", tutte le altre aree sono "non-backbone"; le seconde non possono essere direttamente collegate fra loro e il traffico tra una e l'altra deve attraversare l'area 0. Ai limiti delle aree le rotte sono riassunte (route summarization) per ridurre le dimensioni delle routing table. In questo esempio, visto il ridotto numero di router, appartengono tutti all'area 0.

In OSPF si puó stabilire il tipo di rete di ogni interfaccia; quando una interfaccia usa incapsulamento Ethernet, il tipo di rete predefinito é il Broadcast Multiple Access (BMA o broadcast). In una rete multi-access (come le reti BMA), viene eletto un DR (designated router) e una riserva (BDR, backup designated router); il DR ha

una conoscenza completa della topologia della rete e costituisce una singola sorgente di LSA, riducendo il numero di pacchetti scambiati nel broadcast. L'elezione del DR é basata sulla preferenza, che puó essere modificata manualmente per forzare il processo.

In caso di sue soli dispositivi in un collegamento, la banda usata non puó essere ulteriormente ridotta e dunque si puó saltare la fase di elezione del DR. In questa tesi ogni segmento di rete é di tipo Point-to-point (P2P) e perció le prioritá sono state lasciate al valore predefinito, ovvero 1.

OSPF é considerato un IGP (interior gateway protocol), usato per scambiare informazioni sulle rotte all'interno di un "autonomous system" (ad esempio dentro una rete aziendale), in contrasto con BGP (border gateway protocol) dove diversi autonomous systems si scambiano informazioni.
OSPF in questa tesi fá riferimento a OSPFv2 (RFC 2328), ideato per IPv4; esiste anche la versione OSPFv3 [7] (RFC 2740), dedicata a IPv6.

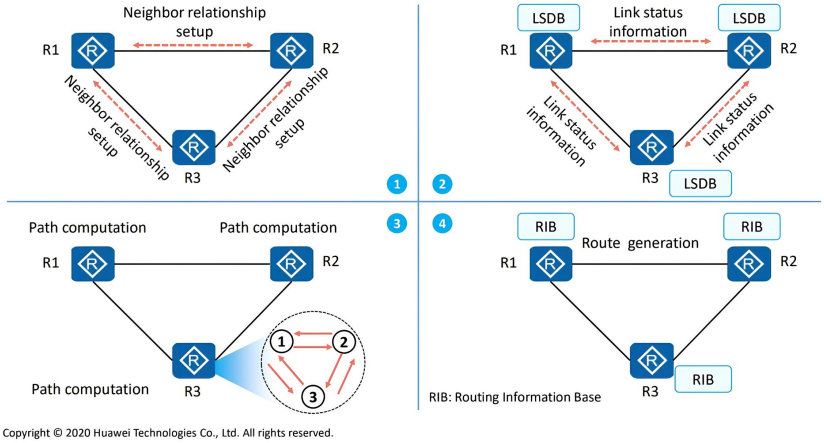


Figura 3.1: Schema di funzionamento del protocollo OSPF, tratto dalle slide del corso di preparazione alla certificazione Huawei HCIA-Datacom

3.2 DHCP

Il protocollo DHCP[8] (Dynamc Host Configuration Protocol) viene usato per permettere ai dispositivi di una rete locale di ricevere automaticamente ad ogni accesso un indirizzo IP adatto alla connessione. Uno (o piú) DHCP server gestiscono le assegnazioni dinamicamente. Nel lavoro svolto, un DHCP server é implementato sul router Aethra permettendo la connessione immediata di un PC alla rete realizzata.

3.3 Ping

Il comando Ping (Packet internet groper) utilizza il protocollo ICMP[9] (Internet Control Message Protocol) di controllo e diagnostica per i dispositivi di rete.

In particolare, tramite l'invio di messaggi "echo request" e la ricezione di messaggi "echo reply" viene testata la raggiungibilitá di un dispositivo o una interfaccia di rete di livello 3, identificata tramite il suo indirizzo IP, e viene misurato il tempo di andata e ritorno.

3.4 Traceroute

Il comando Traceroute (o Tracert) sfrutta i messaggi di errore ICMP[9] per determinare il percorso verso una destinazione con un certo indirizzo IP. Vengono inviati tre datagrammi UDP sulla porta 33434 con il TTL (Time To Live, un contatore nell'header IP che viene ridotto di una unità ad ogni passaggio attraverso un router) posto a uno. Quando il pacchetto raggiunge il primo router, il TTL viene decrementato a zero e questo invia un messaggio ICMP "Time to Live exceeded in Transit", che permette di conoscere il primo nodo attraversato.

La sorgente continua a inviare pacchetti incrementando di una unitá il TTL, ricavando ad ogni passaggio un ulteriore router per cui transitano i dati e il suo indirizzo. Il processo termina quando il pacchetto arriva alla destinazione ed essa risponde con un messaggio ICMP "Destination Unreachable".

Nei sistemi Windows, al posto di usare il protocollo UDP di livello 4, Traceroute é interamente realizzato tramite richieste ICMP.

Capitolo 4

Svolgimento del progetto

4.1 Configurazione router 1

Prima di iniziare la configurazione, ogni router é stato riavviato ripristinando la configurazione di default e ripartendo dal boot iniziale. Per fare ció sui sistemi Cisco[10] si usa la combinazione `erase startup-config` e `reload`. Sul router Huawei si adopera `reset saved-configuration` e `reboot`, mentre sul router Aethra si usa il solo comando `restart` con il parametro `restore-default-conf`

Come giá detto si accede alla console del router 1 tramite una connessione telnet verso il server MOXA del laboratorio. Al primo avvio, terminata la sequenza di boot, il prompt chiede se si vuole entrare nel dialogo di configurazione iniziale; in questo caso, l'opzione deve essere ovviamente rifiutata essendo interessati a fare una configurazione manuale. Per prima cosa é stata impostata una password per la modalitá enable. A tal fine, si usano i comandi `enable` per passare dalla user mode (indicata dal simbolo `>` nella console) alla enable mode (indicata da `#`) e `configure terminal` per passare da essa alla configuration mode (indicata da `(config)#`). In quest'ultima si usa il comando `enable secret <password>`.

Come seconda cosa si esegue il comando `no ip domain-lookup`; ció perché per impostazione predefinita, quando si immette un comando in user o enable mode e non viene riconosciuto, i router Cisco lo considerano il nome di un dispositivo che l'utente tenta di raggiungere tramite telnet. Dunque, il router avvia una chiamata DNS (Domain Name System) per risolvere il comando non riconosciuto in un indirizzo IP, che deve scadere senza risposta prima che la console torni disponibile; il comando usato disabilita questa funzione di default.

Con il comando `hostname R1` viene cambiato il nome del router in R1, per tenerne traccia fra i vari dispositivi, infatti il prompt passa da `Router(config)#` a `R1(config)#`.

La configurazione vera e propria inizia con la creazione dell'interfaccia virtuale Loopback 1, con il comando `interface Loopback 1`, che modifica il prompt in `R1(config-if)#`. Ad essa viene assegnato l'indirizzo IP corretto con `ip address 192.168.11.1 255.255.255.0`. Nei router Cisco la netmask va scritta per esteso in Dotted Decimal Notation, non é possibile specificare solo la sua lunghezza in bit.

Per le interfacce fisiche la configurazione é analoga, con l'aggiunta dell'impostazione del tipo di rete P2P per OSPF tramite `ip ospf network point-to-point`.

```
interface gigabitEthernet 0/0/0
ip address 192.168.12.1 255.255.255.0
ip ospf network point-to-point
interface gigabitEthernet 0/0/1
ip address 192.168.13.1 255.255.255.0
ip ospf network point-to-point
```

A questo punto si puó controllare la corretta configurazione degli IP con `do show ip interface brief`; il "do" serve per forzare il comando "show" in configuration mode, altrimenti per usarlo si dovrebbe tornare in user mode.

É stato in seguito configurato il processo OSPF. Dalla configuration mode si avvia un processo OSPF con il comando `router ospf 1` (1 é il nome del processo avviato all'interno del router, per coerenza si é tenuto lo stesso nome in ogni router), che modifica il prompt in `R1(config-router)#`. Viene assegnato l'identificativo del router con `router-id 1.1.1.1` e vengono aggiunte le reti al processo OSPF con il comando "network", seguite dalla wildcard mask (complementare della network mask) e dall'area di appartenenza.

```
network 192.168.11.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.255 area 0
network 192.168.13.0 0.0.0.255 area 0
```

Infine vengono attivate le due interfacce fisiche con il comando `no shutdown` da eseguire in interface configuration mode; ció é necessario poiché nei dispositivi Cisco, di default, le interfacce fisiche sono spente.

Giunti a questo punto, é bene fare un controllo della configurazione usando i vari comandi `show ip ospf 1`, `show ip ospf neighbor`, `show ip ospf database`, `show ip ospf interface` e `show ip route ospf`.

4.2 Configurazione router 2

Per configurare il router 2 la sua console é connessa direttamente al PC tramite un classico cavo seriale RJ45-DB9 e un adattatore DB9-USB. Inserendo tale cavo in una porta USB del PC, il sistema operativo Windows crea automaticamente una interfaccia virtuale COM (communications port) che rappresenta una porta seriale. A tale interfaccia COM viene associato un numero che va conosciuto per poter aprire il collegamento seriale tamite il software PuTTY; tale numero si puó vedere in Gestione Dispositivi (Device Manager) di Windows, come mostrato in Figura 4.1.

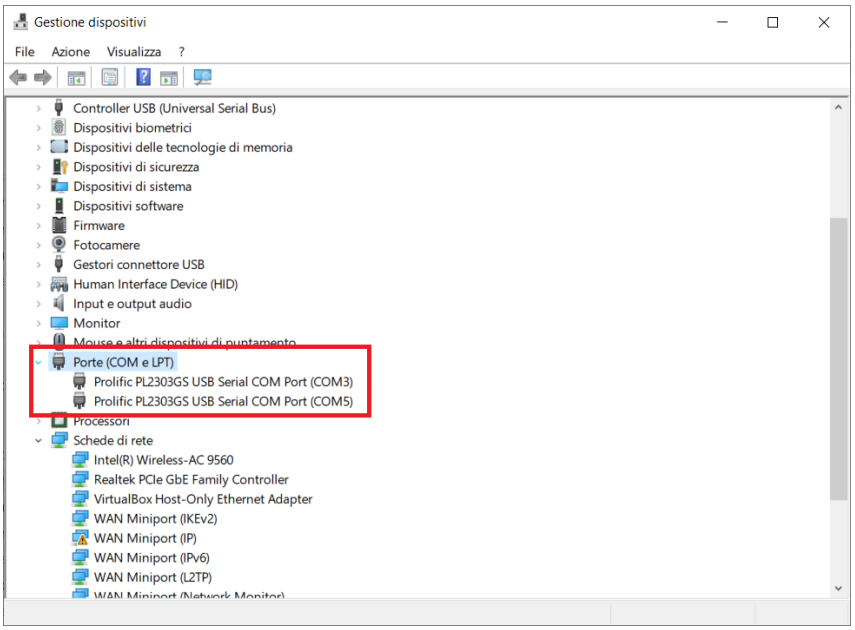


Figura 4.1: Gestione Dispositivi, con evidenziate le porte COM

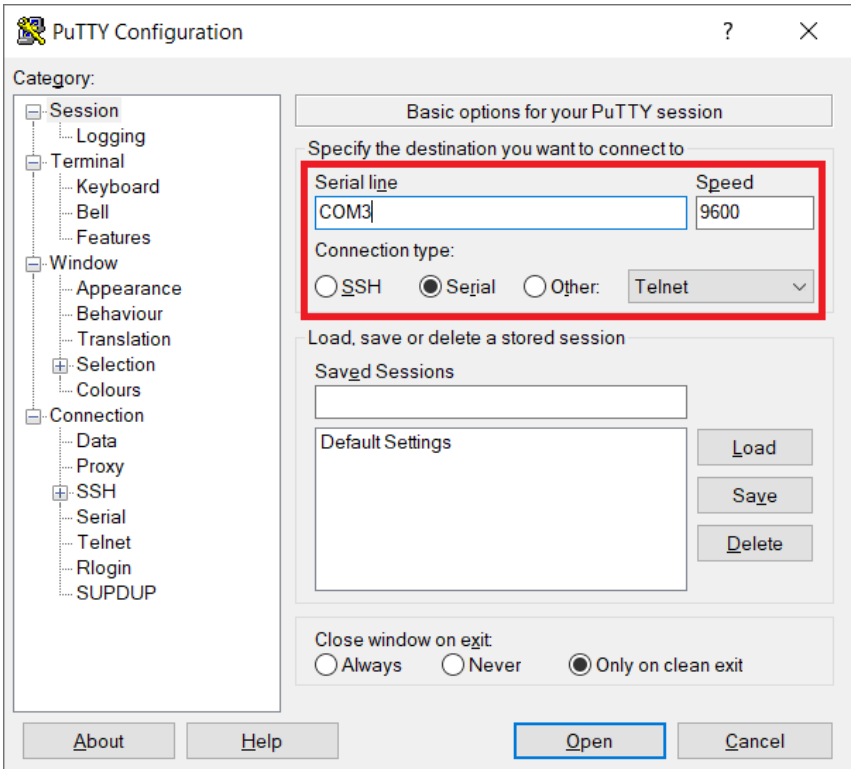


Figura 4.2: Impostazioni di PuTTY per la connessione tramite cavo seriale alla console del router 2

La configurazione del router 2 é molto simile a quella del router 1, essendo entrambi router Cisco. Si parte dal rifiutare il dialogo di configurazione iniziale e si effettuano gli stessi tre passaggi iniziali: creazione di una password per la modalitá di enable, eliminazione della risoluzione automatica tramite DNS dei comandi non riconosciuti e impostazione di un nome.

```
enable
configure terminal
enable secret <password>
no ip domain-lookup
hostname R2
```

Segue la creazione della interfaccia Loopback, l'assegnazione degli IP e l'impostazione del tipo di rete OSPF.

```
interface Loopback 2
ip address 192.168.22.2 255.255.255.0
interface gigabitEthernet 0/0/0
ip address 192.168.12.2 255.255.255.0
ip ospf network point-to-point
interface gigabitEthernet 0/0/1
ip address 192.168.23.2 255.255.255.0
ip ospf network point-to-point
```

Nuovamente con `do show ip interface brief` si puó verificare che gli IP coincidano con lo schema della topologia desiderata, che include le associazioni interfaccia-indirizzo.
La configurazione del processo OSPF consiste negli stessi passaggi del router precedente, cambiando soltanto l'identificativo del router e le reti coinvolte.

```
router ospf 1
router-id 2.2.2.2
network 192.168.22.0 0.0.0.255 area 0
network 192.168.12.1 0.0.0.255 area 0
network 192.168.23.1 0.0.0.255 area 0
```

Come ultimi passaggi, vengono riattivate le interfacce con il comando `no shutdown` (da eseguire nella modalitá di configurazione delle interfacce fisiche appropriate) e vengono effettuati i vari "show" per verificare la corretta configurazione.

Tale controllo premette di identificare subito errori, permettendone una correzione immediata prima che si aggiungano altri fattori. In Figura 4.3 é evidenziato un possibile errore derivante dal comando errato `ospf network point-to-point` al posto di `ip ospf network point-to-point`, infatti il primo viene automaticamente completato a `ospfv3 network point-to-point` e accettato, agendo sul protocollo OSPFv3 inveche che sull'OSPFv2 trattato.

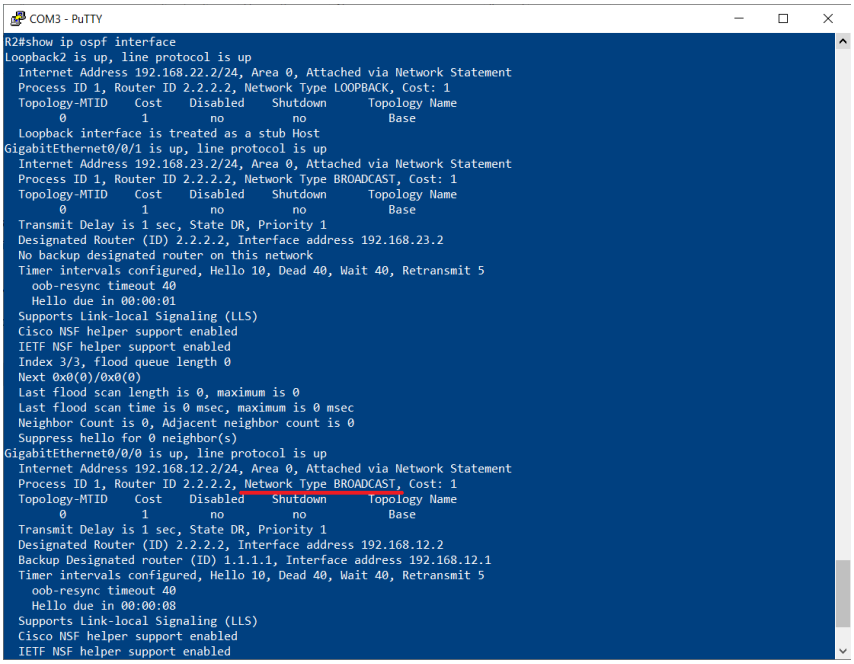


Figura 4.3: Esecuzione del comando `show ip ospf interface` sul router 2, che mostra l'errata configurazione del tipo di rete

Tramite il comando `ping` (packet internet groper) si puó verificare la raggiunibiltá delle interfacce Loopback e quelle connesse verso il router 3.

4.3 Configurazione router 3

Analogamente al router 1, la console del router 3 é raggiungibile tramite il server MOXA del laboratorio, come mostrato in Figura 4.4. Al riavvio del router Huawei[11], è necessario impostare una password e decidere se interrompere il processo di autoconfigurazione (Auto-Config); nel nostro caso, per chiari motivi, va fermato.

La configurazione comincia con l'entrata in system view (appunto tramite il comando `system-view`) e l'impostazione del nome R3 tramite `sysname R3`. La parte successiva riguarda le interfacce, a cui viene impostato l'indirizzo IP con `ip address <address> <prefix-length>` e il tipo di interfaccia point-to-point nel processo OSPF con `ospf network-type p2p`.

```
interface gigabitEthernet 0/0/0
ip address 192.168.23.3 24
ospf network-type p2p
interface gigabitEthernet 0/0/1
ip address 192.168.13.3 24
ospf network-type p2p
```

```
interface gigabitEthernet 0/0/2
ip address 192.168.34.3 24
ospf network-type p2p
```

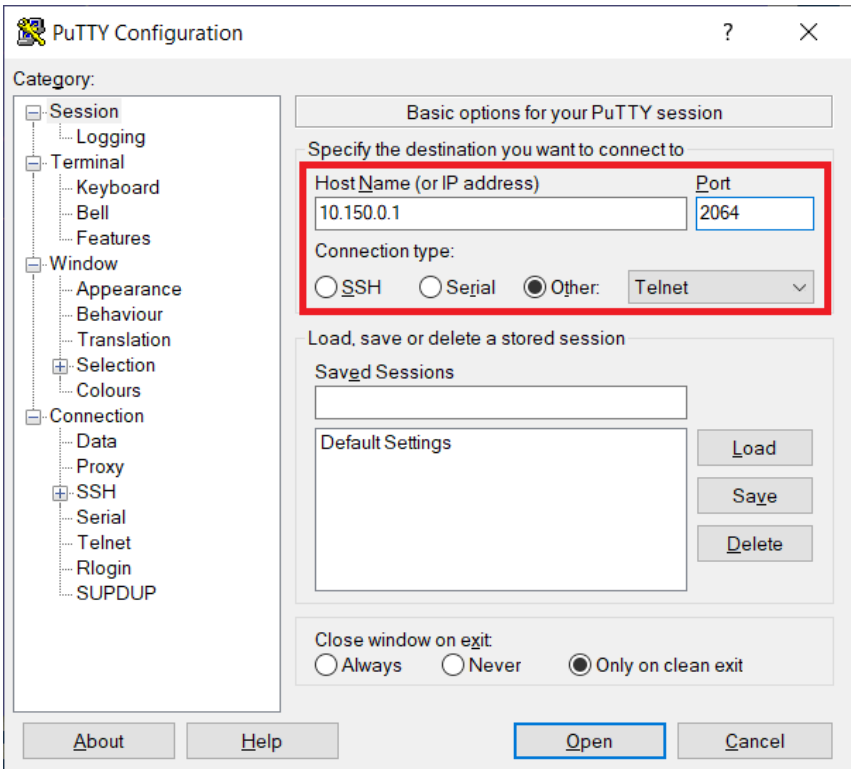


Figura 4.4: Impostazioni di PuTTY per la connessione tramite telnet verso il server MOXA per l'accesso alla console del router 3

Si puó verificare questa parte di configurazione con `display ip interface brief`. Per quanto rigurada la configurazione del processo OSPF, il router Huawei é leggermente diverso dal router Cisco. Viene avviato con il comando `ospf 1 router-id 3.3.3.3`, che assegna anche l'identificativo 1 al processo e 3.3.3.3 al router. All'interno del processo OSPF vanno prima create le aree (con il comando `area <area-id>`) e in seguito vanno aggiunte, all'interno delle aree, le reti comprese (con `network <address> <wildcard-mask>`). In questo caso si ha soltanto l'area 0:

```
area 0
network 192.168.13.0 0.0.0.255
network 192.168.23.0 0.0.0.255
network 192.168.34.0 0.0.0.255
```

Si puó controllare la corretta configurazione tornando con `quit` nella configurazione di OSPF (il prompt passa da `R3-ospf-1-area-0.0.0.0` a `R3-ospf-1`) e usando il comando `display this`; tale comando permette di controllare rapidamente la lista di tutte le configurazioni, eccetto quelle predefinite, di una interfaccia o di un protocollo.

Controlli addizionali vanno svolti con `display ospf peer brief`, `dislay ospf routing`, `display ip routing-table protocol ospf`, `dislay ospf interface` e soprattutto con il comando `ping`.

Tramite `ping` é stata verificata la raggiungibilitá dal router 3 verso tutte le interfacce di rete giá configurate e la raggiungibilitá dai router 1 e 2 verso le interfacce del router 3.

4.4 Configurazione router 4

La connessione alla console del router 4 avviene tramite cavo seriale e adattatore USB, rispetto al router 2 cambia ovviamente il numero della porta COM ma anche il baud rate della connessione, che infatti va impostato a 115200 bit/s.

La CLI del sitema operativo ATOS (Aethra Telecommunications Operating System), presente su tutti i dispositivi Aethra[12], si differenzia da quelle usate in precedenza in quanto é strutturata ad albero. Per accedere ad un parametro per modificarlo é necessario raggiungere il corrispondente nodo nell'albero o specificarne il percorso. Per entrare in un nodo va usato il suo nome, con il comando `up` si torna al nodo padre e con `top` si torna alla radice; il comando `tree` mostra le proprietá del nodo includendo i sottonodi. Per aggiungere una nuova opzione si usa il comando `add`, per rimuovere un'opzione aggiunta `del` e per impostare un parametro si usa `set`.

Al primo avvio, per accedere alla riga di comando viene richiesto un nome utente, che deve avere almeno un carattere, e va lasciato vuoto il campo password. Dopo aver ottenuto l'accesso a livello amministratore (indicato da » nel prompt), in cui si ha completo controllo sul dispositivo, si puó modificare la password. Per farlo bisogna entrare nel nodo `system` e usare il comando `password ADMIN <empty> <nuova password> <ripetizione password>`. In questo caso ADMIN indica il priviledge level a cui si sta modificando la password ed "<empty>" rappresenta la keyword da usare in quanto la password da modificare é assente. Rimanendo nel nodo `system`, si imposta un nome per il router con `set name R4`.

Tramite il comando `conf running` si puó vedere come l'interfaccia eth0 abbia giá un indirizzo IP preimpostato (192.168.1.1); per cui prima di procedere con la configurazione, va eliminato questo default con `set interfaces eth0 ip address 0.0.0.0` e `set interfaces eth0 ip netmask 0.0.0.0`.

Con i comandi seguenti si assegnano gli IP desiderati alle interfacce utilizzate:

```
add interfaces IFC eth1 eth1
set interfaces eth1 ip address 192.168.34.4/24
add interfaces IFC eth2 eth2
set interfaces eth2 ip address 192.168.1.1/24
```

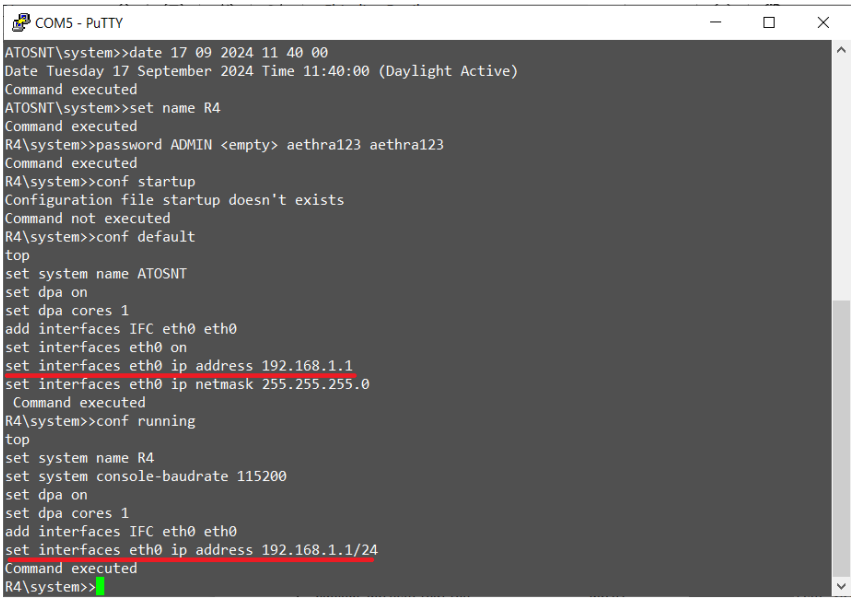


Figura 4.5: Configurazione di default del router 4, con evidenziata la configurazione dell'interfaccia eth0

Con i successivi comandi viene abilitato il server DHCP sull'interfaccia eth2, usando come spazio degli indirizzi la rete 192.168.1.0/24 e impostando il router 4 come default gateway per i DHCP client. In questo modo é sufficiente collegare il PC per ottenere un IP valido a comunicare con tutta la topologia realizzata.

```
set dhcpserver on
add dhcpsever IFC eth2
set dhcpserver eth2 startaddress 192.168.1.2
set dhcpserver eth2 endaddress 192.168.1.254
set dhcpserver eth2 netmask 255.255.255.0
set dhcpserver eth2 defaultrouter 192.168.1.1
```

Viene creato un processo OSPF con identificativo 1 tramite `add ip ospf ospf 1`. In questo modo viene aggiunto un sottonodo "1" al nodo ospf. Viene assegnato l'identificativo del router con `set ip ospf 1 static-router-id 4.4.4.4`.

Tramite `add ip ospf area 0.0.0.0` viene creata l'area backbone (il nome dell'area deve essere espresso nel formato di un indirizzo IP) e contestualmente viene creato il sottonodo area-0.0.0.0, a cui vanno aggiunte le interfacce eth1 ed eth2. I comandi seguenti, inoltre, specificano per eth1 il tipo di rete point-to-point e rendono eth2 una interfaccia passiva, ovvero un'interfaccia la cui rete connessa viene propagata agli altri router, ma in cui non si stabiliscono adiacenze in quanto non sono presenti altri router.

```
add ip ospf 1 IFC eth1 area-0.0.0.0
set ip ospf 1 eth1 network-type point-to-point
add ip ospf 1 IFC eth2 area-0.0.0.0
```

```
set ip ospf 1 eth2 passive-ifc on
```

Per verificare che tutto funzioni si possono usare i comandi `show ip ospf 1 work` e `show ip route status` e controllare la raggiungibilitá delle interfacce Loopback 1 e 2 tramite ping. Analogamente si puó fare ping dai router precedenti verso le interfacce del router 4. Va notato che, finché non viene connessa, l'interfaccia eth2 viene considerata down e senza indirizzo IP e dunque non é raggiungibile.

Come ultimo passaggio, vengono salvate le configurazioni di tutte le macchine. Su router 1 e 2 (Cisco) si possono usare i comandi `write` oppure `copy running-config startup-config`; sul router 3 (Huawei) si adopera `save` mentre per il router 4 (Aethra) si usa `system save`.

Capitolo 5

Verifica

Avendo abilitato un DHCP server nel router 4, quando viene collegato un PC alla porta eth2 del router Aethra tramite un cavo Ethernet, il PC può ottenere automaticamente un indirizzo IP. Per sfruttare tale possibilitá, va specificata l'impostazione automatica/DHCP per l'indirizzo IP dell'interfaccia Ethernet del PC; ad esempio in un sistema operativo Windows ció va fatto nelle impostazioni, nella sezione "Rete e Internet" e successivamente "Ethernet".

Per conoscere quale indirizzo é stato assegnato esistono comandi shell che mostrano gli IP delle interfacce, ovvero `ifconfig` per Linux e MacOs e `ipconfig` per Windows. É mostrato in Figura 5.1 che l'indirizzo IP del PC é 192.168.1.2 .

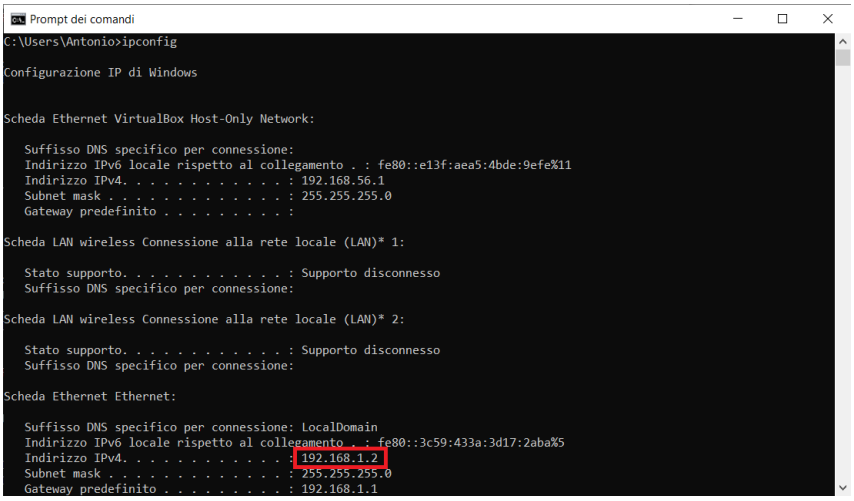


Figura 5.1: Esecuzione del comando `ipconfig` nella Command shell di Windows, con evidenziato l'indirizzo IP ricevuto tramite DHCP

Va notato che normalmente il firewall del sistema operativo Windows blocca i tentativi di ping (ICMP Echo Request) per cui vanno abilitati dalle impostazioni o semplicemente va disattivato il firewall. Come dalle console dei router, si possono effettuare ping dalla Command shell del PC. Come mostrato in parte in Figura 5.2 sono raggiungibili tutte le interfacce della rete, incluse le Loopback virtuali.

Ovviamente é possibile anche fare ping da tutti i router verso il PC, come in Figura 5.3.

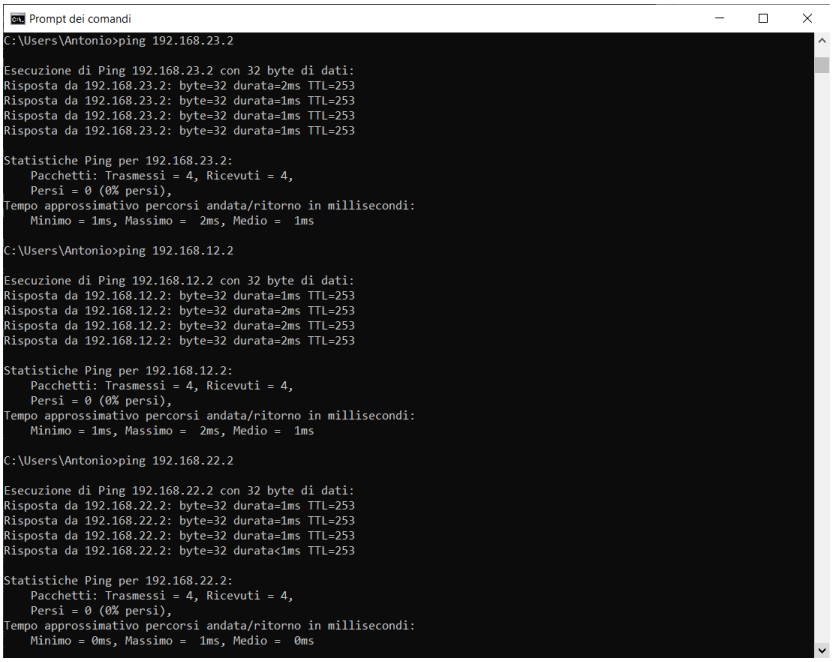


Figura 5.2: Verifica del funzionamento di OSPF tramite esecuzione del comando `ping` (verso le interfacce del router 2) nella Command shell di Windows

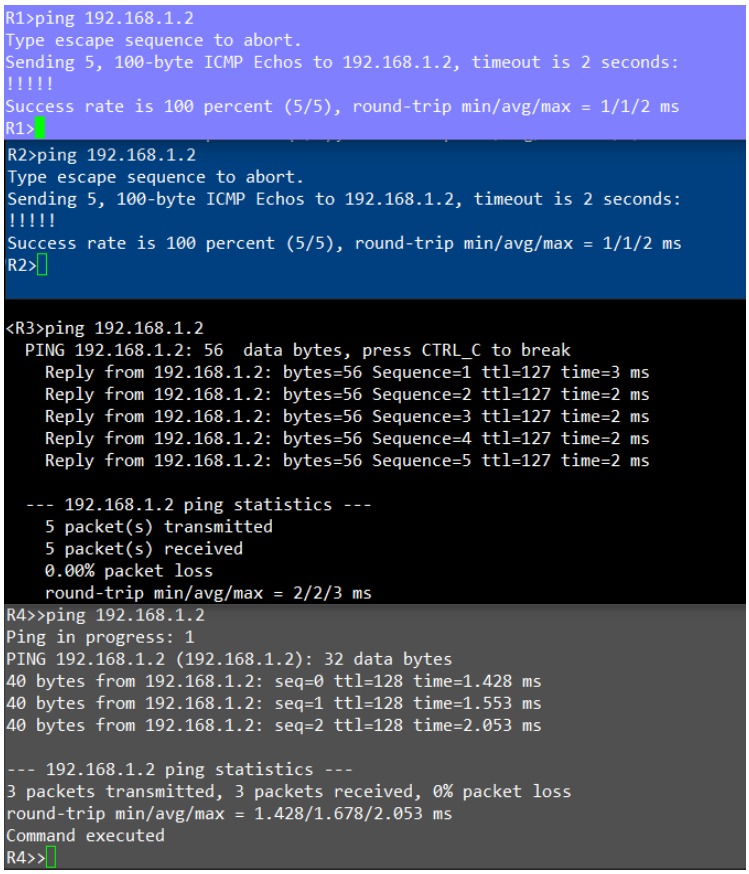


Figura 5.3: Esecuzione del comando `ping` verso il PC nella console dei quattro router

Tramite lo strumento traceroute (comando `tracert` su Windows) possiamo analizzare il percorso effettuato dai pacchetti per raggiungere le interfacce Loopback e la rete 192.168.12.0/24; tutte richiedono il passaggio per il router 4 (192.168.1.1), il router 3 (192.168.34.3) e alternativamente uno tra il router 1 o 2. Si puó vedere il percorso inverso usando il comando `traceroute` su router Cisco (`tracert` su Huawei ed Aethra).

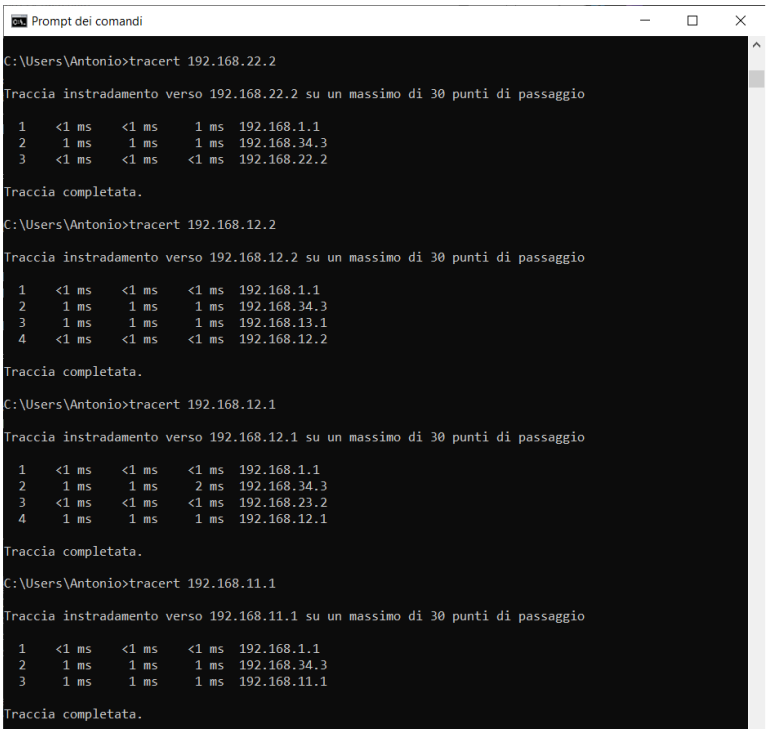


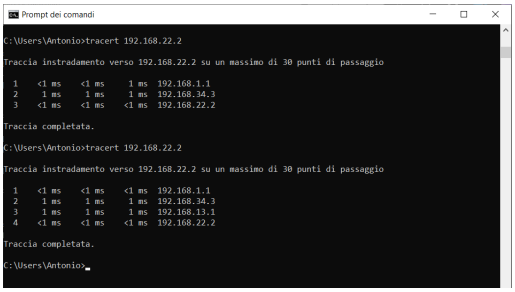
Figura 5.4: Esecuzione del comando `tracert` nella Command shell del PC per mostrare il percorso dei pacchetti

Poiché il protocollo OSPF dinamico ha come scopo anche permettere ai router di ricavare rotte alternative in caso di guasti, é bene verificare la raggiungibilitá delle interfacce di rete quando viene disconnesso qualche collegamento fisico. In Figura 5.5 é evidenziato il percorso ricavato tramite traceroute nel caso in cui si elimini il collegamento tra il router 2 e il router 3.

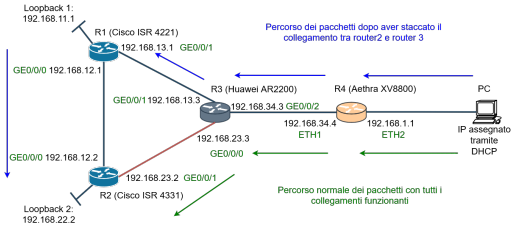
Una prova analoga prevede l'invio di un ping verso l'interfaccia Loopback 1 utilizzando il comando `ping -t 192.168.11.1`, dove l'opzione `-t` specifica che il ping continuerà fino a quando non verrà interrotto manualmente. Durante la prova, si scollega un cavo, in particolare il collegamento tra il router 1 e il router 3, per osservare il tempo necessario al protocollo OSPF per ristabilire la raggiungibilità dell'interfaccia attraverso un percorso alternativo.

Analizzando il parametro TTL, si nota che nella nuova rotta stabilita i pacchetti devono attraversare un nodo aggiuntivo, come accadeva nell'esempio precedente.

Attraverso le analisi contenute in questo capitolo, è possibile concludere che l'obiettivo prefissato è stato raggiunto: grazie all'implementazione del routing dinamico



(a) Sottofigura 1.



(b) Sottofigura 2.

Figura 5.5: Percorsi dal PC verso l'interfaccia Loopback del router 2 ricavati tramite `tracert` e mostrati nello schema della topologia

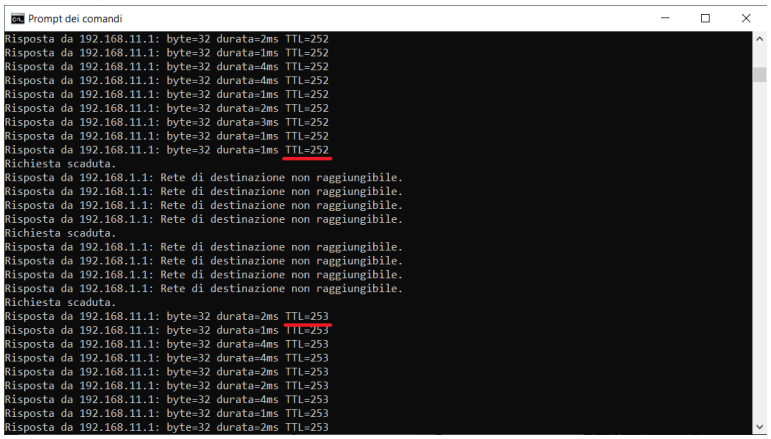


Figura 5.6: Prova del tempo di riconvergenza della rete tramite OSPF, mostrata tramite `ping` dal PC verso l'interfaccia Loopback 1. É evidenziato il cambio di TTL

mediante il protocollo OSPF, ogni interfaccia fisica e virtuale della rete risulta accessibile da qualsiasi dispositivo. Questo protocollo non solo garantisce la raggiungibilità, ma consente anche il rapido e automatico ripristino della connettività in caso di guasti ad alcuni collegamenti.

Capitolo 6

Possibili sviluppi

L'uso del protocollo OSPF rende piú semplice e rapida l'aggiunta di ulteriori nodi, in quanto non é necessario impostare rotte statiche ma é sufficiente configurare correttamente il processo OSPF. Inoltre, l'uso di router di diversi fornitori dimostra l'elevata flessibilitá della rete.

Un importante mancanza nell'ottica di rendere piú realistica la topologia realizzata come simulazione di una rete aziendale é la connessione a global internet. A causa del giá citato problema di saturazione degli indirizzi IPv4 diventa necessario implementare, nel router direttamente connesso alla rete dell'internet service provider (ISP), una traduzione degli indirizzi privati in un indirizzo pubblico, detta Network Address Translation (NAT).

Sempre considerando il lavoro svolto come emulazione di una rete aziendale, é bene predisporre delle misure di sicurezza aggiuntive per evitare che malware, attacchi DDoS (Distributed Denial of Service), phishing o altri pericoli danneggino la rete interna e i beni dell'azienda che da essa dipendono. Tale protezione si potrebbe ottenere aggiungendo un firewall, ovvero un dispositivo di rete che monitora, filtra e controlla il traffico tra varie porzioni della rete sulla base di regole di sicurezza definite.

La presenza del router Aethra, intrinsecamente orientato alla Network Functions Virtualization, permetterebbe di usare, per realizzare le funzioni di un firewall, una macchina virtuale al suo interno al posto di un dispositivo fisico. Ad esempio si potrebbe usare la piattaforma open source OPNsense, basata su FreeBSD, che include strumenti per la gestione della sicurezza di rete, come il filtraggio dei contenuti, il monitoraggio del traffico e la prevenzione delle intrusioni, e possiede una interfaccia web che lo rende facile da configurare.

Capitolo 7

Conclusioni

Il lavoro svolto in questa tesi dimostra come, attraverso le conoscenze acquisite durante il corso di preparazione alla certificazione Huawei HCIA-Datacom, sia possibile configurare una rete di dispositivi eterogenei, includendo non solo apparati Huawei, ma anche quelli di altri fornitori come Cisco e Aethra.

É stata possibile l'implementazione di un protocollo di routing dinamico come OSPF, permettendo di raggiungere ogni punto della rete senza la necessità di configurazioni manuali delle rotte, aumentando la robustezza della rete stessa e consentendo la determinazione automatica di percorsi alternativi in caso di variazioni nella topologia.

Inoltre, é stato mostrato come la configurazione può essere facilmente verificata utilizzando gli strumenti ping e traceroute dopo la configurazione di ciascun elemento.

Infine, l'integrazione di un server DHCP contribuisce a rendere la topologia più realistica come emulazione di una rete aziendale.

Bibliografia

[1] Huawei Technologies Co. Ltd. *Materiale del corso di preparazione alla certificazione Huawei HCIA-Datacom V1.0*. Huawei Technologies Co. Ltd., 2020.

[2] Cisco Inc. Cisco 4221 Integrated Services Router. `https://www.cisco.com/c/it_it/support/routers/4221-integrated-services-router-isr/model.html`, 2024. Accessed: 30 September 2024.

[3] Cisco Inc. Cisco 4331 Integrated Services Router. `https://www.cisco.com/c/it_it/support/routers/4331-integrated-services-router-isr/model.html`, 2024. Accessed: 30 September 2024.

[4] Huawei Technologies Co. Ltd. AR2200 Series Enterprise Routers. `https://e.huawei.com/it/products/routers/ar2200`, 2024. Accessed: 30 September 2024.

[5] Aethra Telecommunications. Aethra XV8800WAC. `https://www.aethra.com/en/xv8800wac`, 2024. Accessed: 30 September 2024.

[6] John Moy. OSPF Version 2. RFC 2328, April 1998.

[7] Rob Coltun, Dennis Ferguson, and John Moy. OSPF for IPv6. RFC 2740, December 1999.

[8] Ralph Droms. Dynamic Host Configuration Protocol. RFC 2131, March 1997.

[9] J. Postel. Internet Control Message Protocol. RFC 792, September 1981.

[10] Wendell Odom. *CCNA 200-301 Official Cert Guide*. Cisco, 2020.

[11] Huawei Technologies Co. Ltd. *HCNA Networking Study Guide*. Springer, 2016.

[12] A TLC S.r.l. *ATOS Software User Guide*, 7.5.2.6 edition, 2024.