



**UNIVERSITA' POLITECNICA DELLE MARCHE**  
**FACOLTA' DI INGEGNERIA**

---

Corso di Laurea triennale in Ingegneria Elettronica

*Implementazione virtuale di una rete enterprise privata*

*Virtual implementation of a private enterprise network*

Relatore:

**Prof. Ennio Gambi**

Tesi di Laurea di:

**Filippo Pimpini**

Correlatore:

**Prof. Adelmo De Santis**

*A.A. 2019/2020*

# Ringraziamenti

Prima di procedere con la trattazione, vorrei dedicare qualche riga a tutti coloro che mi sono stati vicini in questo percorso di crescita personale e professionale.

Innanzitutto, ringrazio il mio relatore Gambi Ennio e il mio correlatore De Santis Adelmo, sempre pronti a darmi le giuste indicazioni in ogni fase della realizzazione dell'elaborato. Grazie a voi ho accresciuto le mie conoscenze e le mie competenze. Un grazie va anche a tutti gli altri professori che hanno contribuito alla mia formazione.

Ringrazio la Huawei Technologies Co. Ltd. che, in collaborazione con l'università, mi ha permesso di seguire il corso "*HCIA Routing&Switching*", tenuto dal già citato De Santis Adelmo.

Ringrazio i miei genitori, perché senza di loro non avrei mai potuto intraprendere questo percorso di studi. Ringrazio anche mia sorella per il sostegno morale e pratico.

Infine, grazie ai miei colleghi di corso e a tutti i miei amici, per avermi sempre incoraggiato fin dall'inizio del percorso universitario.

# Indice

---

<b><u>Introduzione</u></b> .....	4
<b><u>Capitolo 1</u></b>	
Scelte implementative.....	6
<b><u>Capitolo 2</u></b>	
PPPoE Server.....	8
<b><u>Capitolo 3</u></b>	
PPPoE Client.....	10
<b><u>Capitolo 4</u></b>	
Introduzione a IPv6.....	15
<b><u>Capitolo 5</u></b>	
Tunnel GRE e IPv6 addresses.....	18
<b><u>Conclusione</u></b> .....	24
<b><u>Appendice A</u></b>	
Implementazione VLAN.....	26
<b><u>Bibliografia</u></b> .....	29

## Introduzione

Il progetto preso in esame consiste nell'implementare nell'ambiente simulato eNSP (Enterprise Network Simulator), programma sviluppato da Huawei Technologies, la rete enterprise rappresentata in figura 1. La topologia rappresenta lo schema di una rete enterprise composta da 8 router AR2220 e uno switch S5700, dispositivi di rete prodotti da Huawei ed implementati nel simulatore con le stesse caratteristiche di quelli reali.

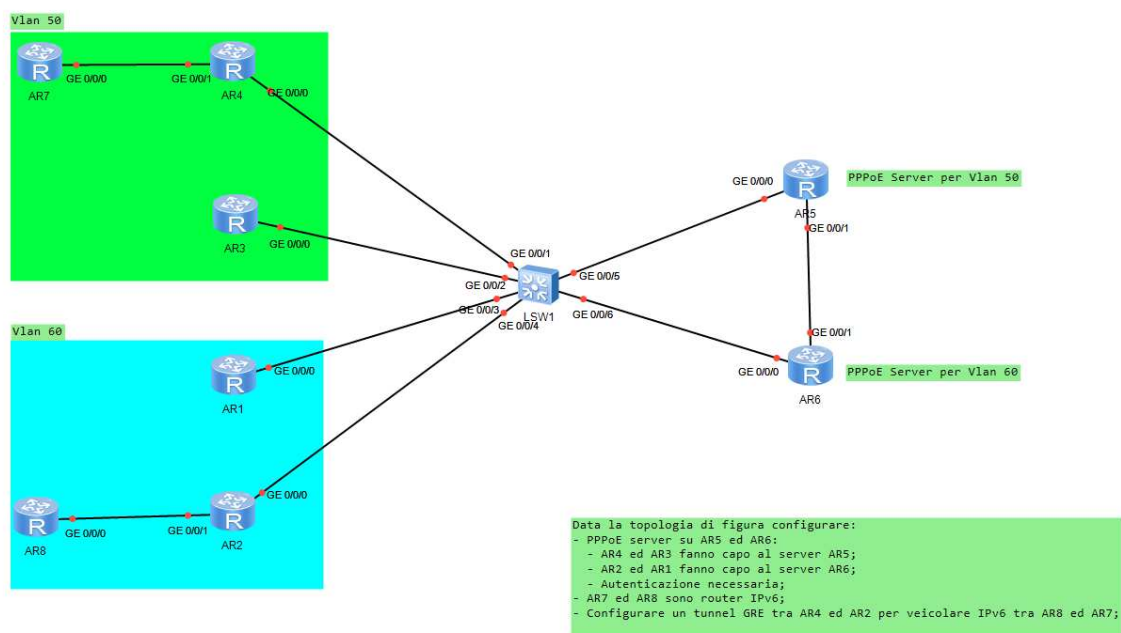


Figura 1, rete da implementare con specifiche di progetto

Per configurare un dispositivo reale si deve accedere alla sua command window tramite la porta console, una porta seriale RJ-45, o mini-usb, presente nel case, collegando un calcolatore attraverso la sua COM Port, oppure da remoto attraverso l'interfaccia VTY.

Nel simulatore invece, essendo assente la parte fisica, i collegamenti sono virtualizzati all'interno del calcolatore e per accedere alle command window è sufficiente cliccare sui dispositivi.

Analizzando la rete di figura 1, partendo dalla disposizione dei router, possiamo immaginare che rappresenti un'azienda composta da tre sedi: la sede centrale e due sedi distaccate.

La rete può essere quindi divisa in tre parti:

- la prima è quella appartenente alla sede centrale, che comprende i router AR5 e AR6, questi infatti svolgono il ruolo di server e offrono la connettività a due VLAN. In particolare, sono dei PPPoE server, è necessaria quindi un'autenticazione da parte dei router che vi si connettono. Ciò ai fini di garantire la sicurezza del collegamento.
- le due sedi distaccate dell'azienda appartengono ognuna ad una VLAN, una composta da AR3, AR4 e AR7, l'altra da AR1, AR2 e AR8. La tecnologia VLAN permette di segmentare lo stesso dominio di broadcast, creando reti logicamente non comunicanti tra di loro. Le due VLAN, infatti, sono connesse attraverso lo stesso switch, ma per poter comunicare devono obbligatoriamente far passare il traffico attraverso la sede centrale, che può quindi stabilire delle regole di comunicazione.  
AR1, AR2 sono PPPoE-Client di AR6, mentre AR3 E AR4 sono PPPoE-Client di AR5.

Un'altra specifica di progetto riguarda i router AR7 ed AR8. Essi sono router IPv6 e, per poter stabilire una comunicazione tra di loro, è necessario veicolare IPv6 in un tunnel GRE.

GRE è un protocollo IP che permette di far comunicare macchine appartenenti a reti locali separate, senza che queste debbano usare protocolli diversi da quelli che già usavano localmente.<sup>1</sup>

Nei prossimi capitoli verranno analizzate le configurazioni di tutti i router, per poter implementare una rete in grado di soddisfare le specifiche richieste.

---

<sup>1</sup> Protocollo di tunneling, da Wikipedia, l'enciclopedia libera

# Capitolo 1

## Scelte implementative

Come detto, la rete di figura 1 è costituita da due Vlan, ognuna delle quali fa capo ad un PPPoE-Server.

PPPoE è un protocollo che permette di incapsulare frame PPP in frame Ethernet, fornendo le caratteristiche standard tipiche di un protocollo PPP come le funzionalità di autenticazione, cifratura e compressione.<sup>2</sup> PPP supporta diversi Network Control Protocols (NCP) come IP Control Protocol (IPCP) o Internetwork Packet Exchange Control Protocol (IPXCP), per abilitare e configurare i moduli IP, negoziando alcuni parametri specifici ed assegnando nel nostro caso gli indirizzi ai clients (ovvero gli Authenticated, mentre il server è detto Authenticator). PPP permette di utilizzare due diversi protocolli di autenticazione, PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol). La principale differenza tra i due è che nel secondo solo il nome utente viene trasferito senza cifratura.

Si è scelto di implementare un'autenticazione di tipo CHAP: prendendo per esempio la Vlan50, AR5 svolge il ruolo di Authenticator mentre AR4 e AR3 quello di Authenticated, a questi verrà assegnato un indirizzo IP, tramite PPP IPCP, solamente dopo essersi autenticati.

La Vlan50 è associata allo spazio di indirizzi 192.168.50.0/24 di indirizzi IP privati, mentre la Vlan60 allo spazio di indirizzi 192.168.60.0/24.

Alle interfacce GE 0/0/1 di AR5 e AR6 verranno assegnati indirizzi IP della rete 10.0.0.0/30, rispettivamente 10.0.0.1/30 e 10.0.0.2/30. Queste interfacce, insieme a tutte le interfacce dei router che si affacciano verso lo switch centrale, avranno attivo il processo OSPF per poter aggiornare correttamente le tabelle di Routing.

---

<sup>2</sup> PPPoE, da Wikipedia, l'enciclopedia libera

Per quanto riguarda i router AR7 e AR8 (vedi figura 1), essi dovranno comunicare tramite indirizzi IPv6: saranno assegnati loro indirizzi global unicast, rispettivamente con i prefissi 2001:0DB8:1111::/64 EUI-64 e 2001:0DB8:0000::/64 EUI-64.

Vedremo che, per poter mettere in contatto i due router tramite un tunnel GRE, sarà necessario assegnare loro anche indirizzi link-local, così come alle interfacce G0/0/1 di AR4 e AR2 e alle loro interfacce di tipo tunnel. Anche qui sarà attivato un processo OSPF, in questo caso OSPFv3, per permettere ai router di poter indirizzare i pacchetti in modo corretto. Si analizzerà IPv6 in un capitolo dedicato (capitolo 4).

I programmi che saranno utilizzati al fine del progetto sono eNSP e Wireshark, un programma detto “packet sniffer” utilizzato per il troubleshooting e per lo sviluppo di protocolli o di software di comunicazione.<sup>3</sup>

---

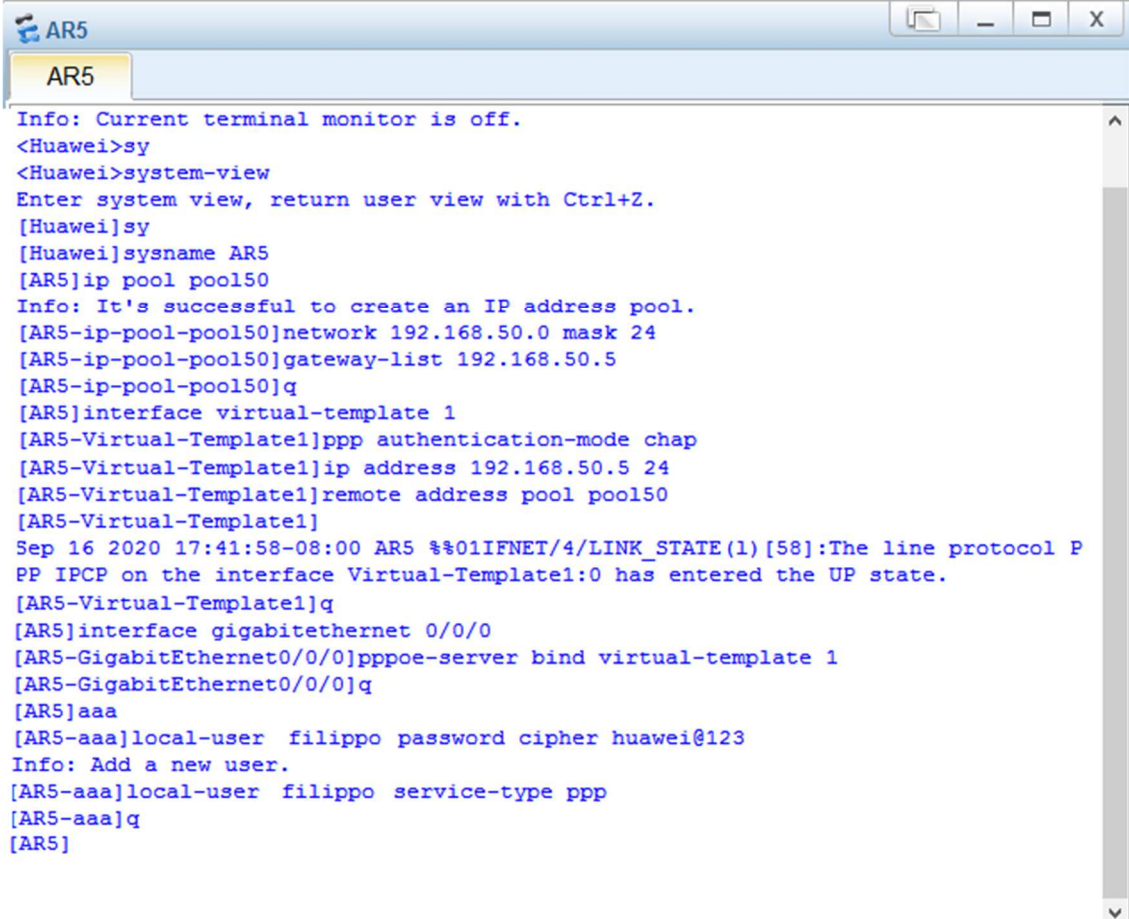
<sup>3</sup> Wireshark, da Wikipedia, l'enciclopedia libera

## Capitolo 2

### PPPoE Server

Per la configurazione di un PPPoE server è necessaria la creazione di un pool di indirizzi, nel quale viene specificato lo spazio di indirizzi di destinazione e l'indirizzo di gateway. Dopodichè si configura l'interfaccia virtuale "Virtual-Template", nella quale si specifica il tipo di autenticazione, l'indirizzo IP da assegnare all'interfaccia e il pool precedentemente creato. L'ultimo step consiste in legare l'interfaccia reale e quella virtuale, attraverso un bind, e da creare le credenziali di accesso tramite il servizio AAA, un protocollo che realizza le tre funzioni di autenticazione, autorizzazione e accounting.<sup>4</sup>

In figura 2 è illustrata la sequenza di comandi effettuata su AR5:



```
Info: Current terminal monitor is off.
<Huawei>sy
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sy
[Huawei]sysname AR5
[AR5]ip pool pool150
Info: It's successful to create an IP address pool.
[AR5-ip-pool-pool150]network 192.168.50.0 mask 24
[AR5-ip-pool-pool150]gateway-list 192.168.50.5
[AR5-ip-pool-pool150]q
[AR5]interface virtual-template 1
[AR5-Virtual-Template1]ppp authentication-mode chap
[AR5-Virtual-Template1]ip address 192.168.50.5 24
[AR5-Virtual-Template1]remote address pool pool150
[AR5-Virtual-Template1]
Sep 16 2020 17:41:58-08:00 AR5 %01IFNET/4/LINK_STATE(1)[58]:The line protocol P
PP IPCP on the interface Virtual-Template1:0 has entered the UP state.
[AR5-Virtual-Template1]q
[AR5]interface gigabitethernet 0/0/0
[AR5-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[AR5-GigabitEthernet0/0/0]q
[AR5]aaa
[AR5-aaa]local-user filippo password cipher huawei@123
Info: Add a new user.
[AR5-aaa]local-user filippo service-type ppp
[AR5-aaa]q
[AR5]
```

Figura 2, configurazione PPPoE Server su AR5

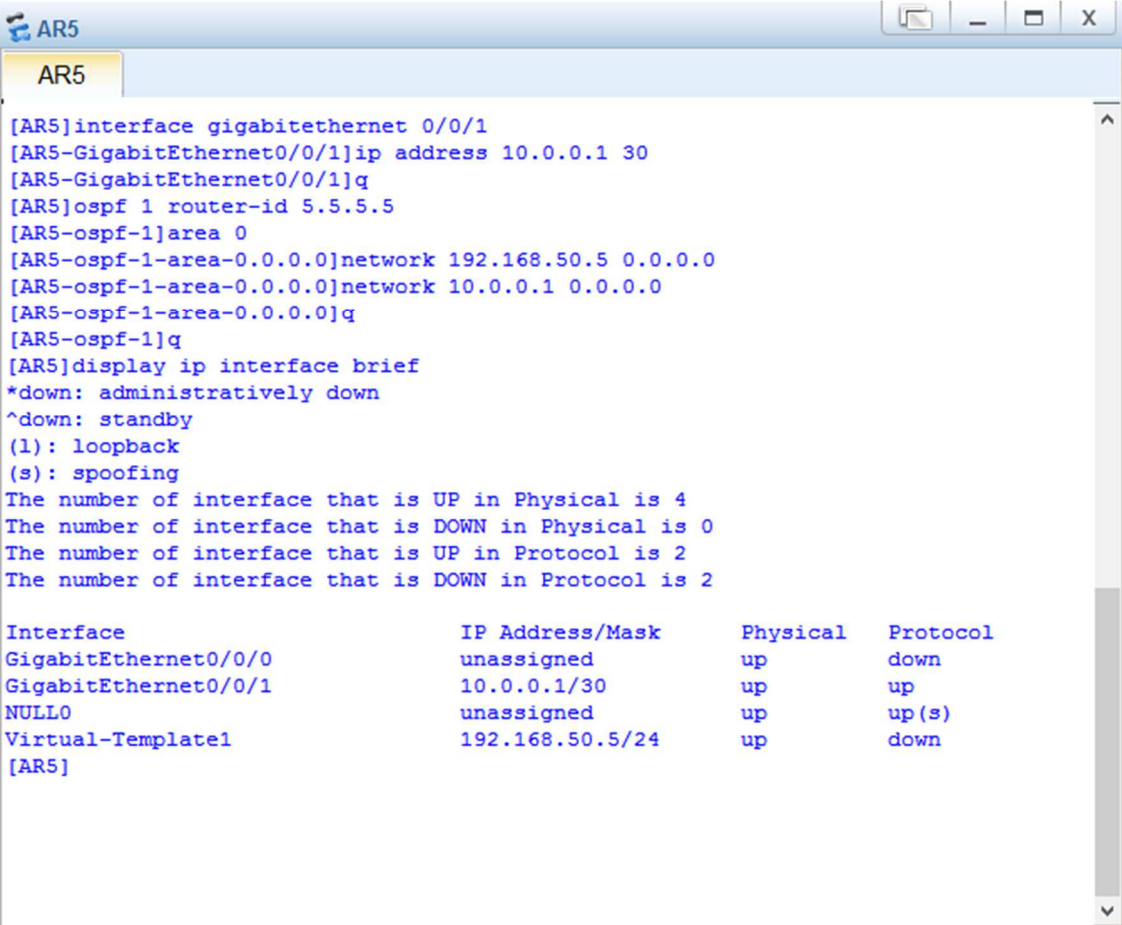
<sup>4</sup> AAA, da Wikipedia, l'enciclopedia libera



Il procedimento è identico per AR6, con le seguenti differenze:

- il pool è denominato pool60, ha come network 192.168.60.0/24 e come gateway 192.168.60.6
- l'interfaccia virtuale ha come IP 192.168.60.6/24
- il local-user è "utente1" ed ha come password huawei@456

Per completezza si riporta in questo capitolo anche la restante configurazione di AR5, dove viene assegnato l'IP 10.0.0.1/30 all'interfaccia G0/0/1 e viene attivato OSPF su entrambe le interfacce. Anche in questo caso per AR6 il procedimento è il medesimo (IP address 10.0.0.2/30).



```
[AR5]interface gigabitethernet 0/0/1
[AR5-GigabitEthernet0/0/1]ip address 10.0.0.1 30
[AR5-GigabitEthernet0/0/1]q
[AR5]ospf 1 router-id 5.5.5.5
[AR5-ospf-1]area 0
[AR5-ospf-1-area-0.0.0.0]network 192.168.50.5 0.0.0.0
[AR5-ospf-1-area-0.0.0.0]network 10.0.0.1 0.0.0.0
[AR5-ospf-1-area-0.0.0.0]q
[AR5-ospf-1]q
[AR5]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2

Interface                IP Address/Mask      Physical  Protocol
GigabitEthernet0/0/0     unassigned           up        down
GigabitEthernet0/0/1     10.0.0.1/30         up        up
NULL0                    unassigned           up        up(s)
Virtual-Template1        192.168.50.5/24     up        down
[AR5]
```

Figura 3, Configurazione AR5: GE0/0/1, OSPF e visualizzazione degli indirizzi delle interfacce

Da questo punto in poi si considererà, come router-id OSPF, il numero del router ripetuto quattro volte: per AR5 il router-id è 5.5.5.5, per AR6 6.6.6.6 e così anche per gli altri router.

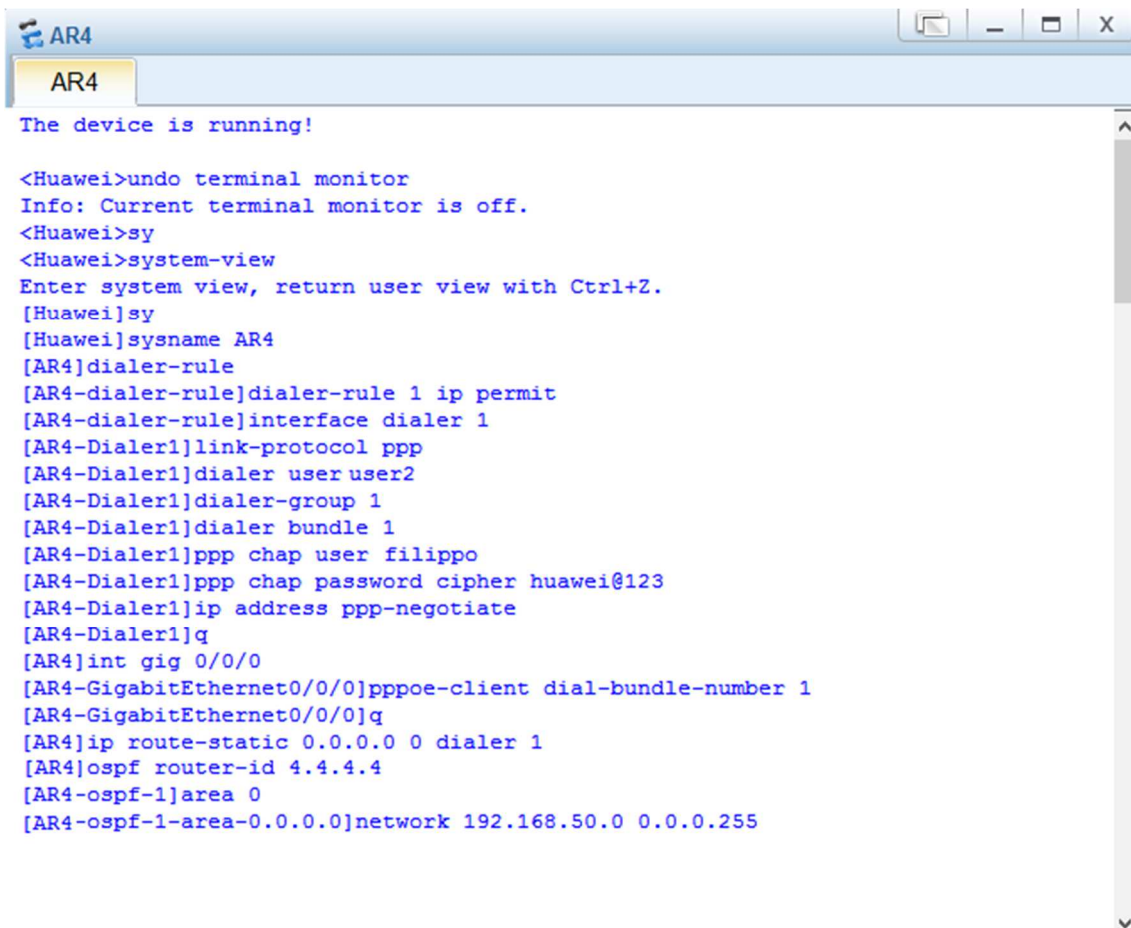
## Capitolo 3

### PPPoE Client

Per poter configurare un PPPoE-Client è necessario far uso di un'altra interfaccia virtuale, detta "dialer", che per essere utilizzata a tale scopo deve essere abilitata ad avere un indirizzo IP.

All'interno della configurazione di tale interfaccia bisogna specificare il link-protocol (PPP) e le credenziali di autenticazione PPPoE, per poi effettuare anche qui un bundle con un'interfaccia reale.

In figura 4 è riportata la configurazione di AR4. AR3, per la Vlan50, e AR1 AR2, per la Vlan60, hanno una configurazione analoga, con le rispettive credenziali.



```
AR4
AR4
The device is running!

<Huawei>undo terminal monitor
Info: Current terminal monitor is off.
<Huawei>sy
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sy
[Huawei]sysname AR4
[AR4]dialer-rule
[AR4-dialer-rule]dialer-rule 1 ip permit
[AR4-dialer-rule]interface dialer 1
[AR4-Dialer1]link-protocol ppp
[AR4-Dialer1]dialer user user2
[AR4-Dialer1]dialer-group 1
[AR4-Dialer1]dialer bundle 1
[AR4-Dialer1]ppp chap user filippo
[AR4-Dialer1]ppp chap password cipher huawei@123
[AR4-Dialer1]ip address ppp-negotiate
[AR4-Dialer1]q
[AR4]int gig 0/0/0
[AR4-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
[AR4-GigabitEthernet0/0/0]q
[AR4]ip route-static 0.0.0.0 0 dialer 1
[AR4]ospf router-id 4.4.4.4
[AR4-ospf-1]area 0
[AR4-ospf-1-area-0.0.0.0]network 192.168.50.0 0.0.0.255
```

Figura 4, configurazione PPPoE Client su AR4 ed attivazione OSPF

Oltre alle operazioni sopra elencate si è creata una rotta statica verso il rispettivo server, per ogni indirizzo di destinazione e si è attivato OSPF.

Per un'analisi più approfondita della connessione client-server si riporta un grab Wireshark (figura 5) in cui si mostrano i frames scambiati tra AR4 e AR5 per stabilire la comunicazione:

No.	Time	Source	Destination	Protocol	Length	Info
33	60.297000	HuaweiTe_8b:3b:48	Broadcast	PPPoED	60	Active Discovery Initiation (PADI)
34	60.344000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPPoED	60	Active Discovery Offer (PADO) AC-Name='AR500e0fc1348e7'
35	60.344000	HuaweiTe_86:59:5f	HuaweiTe_8b:3b:48	PPPoED	60	Active Discovery Offer (PADO) AC-Name='AR600e0fc86595f'
36	60.360000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPPoED	60	Active Discovery Request (PADR) AC-Name='AR500e0fc1348e7'
37	60.375000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPPoED	60	Active Discovery Session-confirmation (PADS) AC-Name='AR500e0fc1348e7'
38	60.407000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP LCP	60	Configuration Request
39	60.438000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP LCP	60	Configuration Request
40	60.469000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP LCP	60	Configuration Ack
43	63.375000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP LCP	60	Configuration Request
44	63.375000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP LCP	60	Configuration Request
45	63.391000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP LCP	60	Configuration Nak
46	63.407000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP LCP	60	Configuration Ack
47	63.422000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP LCP	60	Configuration Request
48	63.438000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP LCP	60	Configuration Ack
49	63.469000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP CHAP	60	Challenge (NAME='', VALUE=0x6a4ab3e28cef9cb06d47c7fb0cdb92c9)
50	63.485000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP CHAP	60	Response (NAME='filippo', VALUE=0x2b651b38099f26b17f8131400454fa6e)
51	63.516000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP CHAP	60	Success (MESSAGE='Welcome to .')
52	63.516000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP IPCP	60	Configuration Request
53	63.516000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP IPCP	60	Configuration Request
54	63.532000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP IPCP	60	Configuration Ack
55	63.563000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP IPCP	60	Configuration Nak
56	63.563000	HuaweiTe_8b:3b:48	HuaweiTe_13:48:e7	PPP IPCP	60	Configuration Request
57	63.610000	HuaweiTe_13:48:e7	HuaweiTe_8b:3b:48	PPP IPCP	60	Configuration Ack

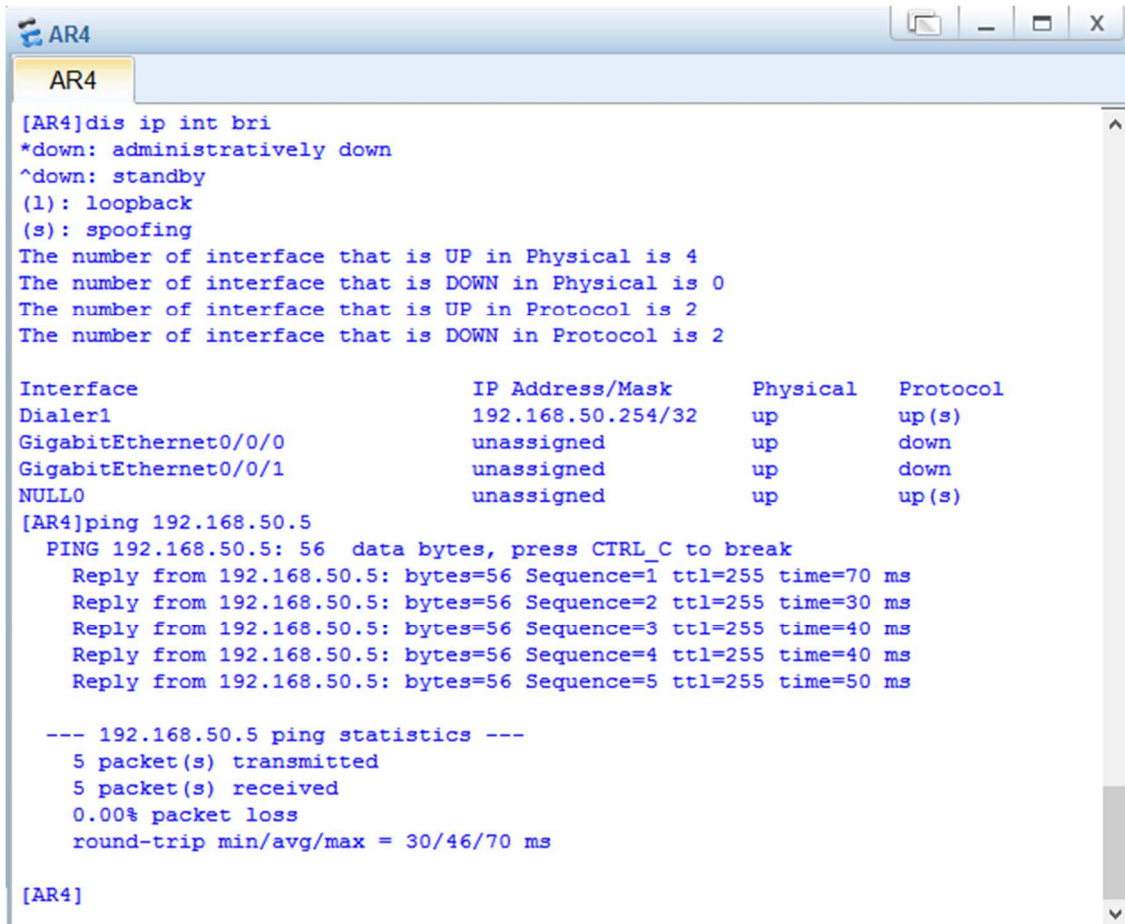
```

<
  Frame 50: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
  Ethernet II, Src: HuaweiTe_8b:3b:48 (00:e0:fc:8b:3b:48), Dst: HuaweiTe_13:48:e7 (00:e0:fc:13:48:e7)
  PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0003
    Payload Length: 30
  Point-to-Point Protocol
  PPP Challenge Handshake Authentication Protocol
    Code: Response (2)
    Identifier: 1
    Length: 28
    Data
      Value Size: 16
      Value: 2b651b38099f26b17f8131400454fa6e
      Name: filippo
  
```

Figura 5, Grab Wireshark: pacchetti scambiati tra AR4 ed AR5 per stabilire la connessione PPPoE

Si possono suddividere i frames in quattro aree: la prima in cui i due router si scambiano frames di tipo PPPoE, in cui si possono notare le fasi di initalization, offer, request e session-confirmation, dalla quale il numero di sessione è ben definito; la seconda in cui si stabilisce una connessione di tipo PPP tramite le Configuration Request e Ack; la terza in cui si ha la fase di autenticazione CHAP, dove solo il nome utente è in chiaro; e la quarta, dove il server assegna l'IP al client tramite IPCP.

Attraverso il comando “*display ip interface brief*” si osserva che all’interfaccia Dialer 1 di AR4 è stato assegnato l’indirizzo IP 192.168.50.254 e che il ping tra AR4 e AR5 funziona:



```
[AR4]dis ip int bri
*down: administratively down
^down: standby
(1): loopback
(s): spoofing
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2

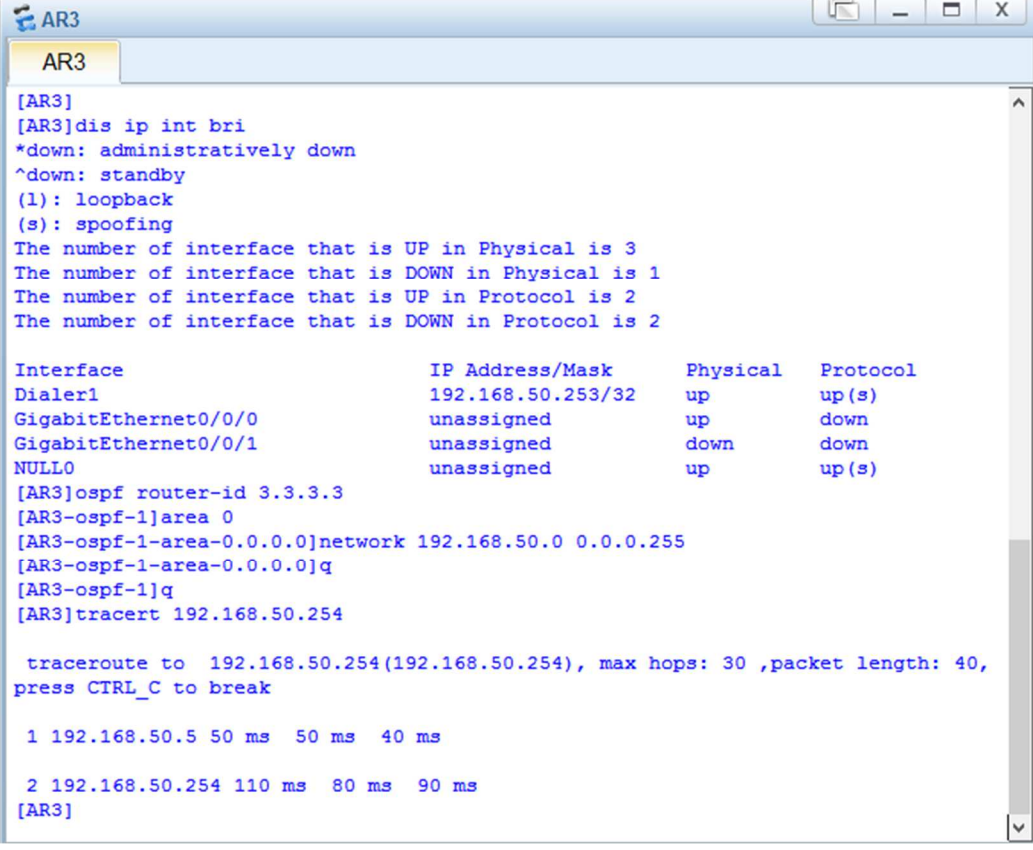
Interface                IP Address/Mask      Physical  Protocol
Dialer1                   192.168.50.254/32    up        up(s)
GigabitEthernet0/0/0      unassigned            up        down
GigabitEthernet0/0/1      unassigned            up        down
NULL0                     unassigned            up        up(s)
[AR4]ping 192.168.50.5
  PING 192.168.50.5: 56 data bytes, press CTRL_C to break
    Reply from 192.168.50.5: bytes=56 Sequence=1 ttl=255 time=70 ms
    Reply from 192.168.50.5: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 192.168.50.5: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 192.168.50.5: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 192.168.50.5: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 192.168.50.5 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/46/70 ms

[AR4]
```

Figura 6, *display ip interface brief* in AR4 e ping verso AR5

Applicando lo stesso procedimento ad AR3 e agli altri client della Vlan60, si può osservare che la comunicazione tra due client avviene sempre attraverso la mediazione dei server: di uno solo, in caso della comunicazione all’interno della stessa Vlan (figura 7), o di entrambi, in caso di comunicazione tra Vlan diverse (figura 8).



```

AR3
[AR3]
[AR3]dis ip int bri
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2

Interface                IP Address/Mask      Physical  Protocol
Dialer1                  192.168.50.253/32    up        up(s)
GigabitEthernet0/0/0    unassigned           up        down
GigabitEthernet0/0/1    unassigned           down      down
NULL0                   unassigned           up        up(s)

[AR3]ospf router-id 3.3.3.3
[AR3-ospf-1]area 0
[AR3-ospf-1-area-0.0.0.0]network 192.168.50.0 0.0.0.255
[AR3-ospf-1-area-0.0.0.0]q
[AR3-ospf-1]q
[AR3]tracert 192.168.50.254

  traceroute to 192.168.50.254(192.168.50.254), max hops: 30 ,packet length: 40,
  press CTRL_C to break

  1 192.168.50.5 50 ms  50 ms  40 ms

  2 192.168.50.254 110 ms  80 ms  90 ms
[AR3]

```

Figura 7, display ip interface brief su AR3 e tracert verso AR4



```

AR2
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>
<AR2>tracert 192.168.50.254

  traceroute to 192.168.50.254(192.168.50.254), max hops: 30 ,packet length: 40,
  press CTRL_C to break

  1 192.168.60.6 60 ms  40 ms  40 ms

  2 10.0.0.1 50 ms  40 ms  40 ms

  3 192.168.50.254 90 ms  80 ms  90 ms
<AR2>tracert 192.168.50.253

  traceroute to 192.168.50.253(192.168.50.253), max hops: 30 ,packet length: 40,
  press CTRL_C to break

  1 192.168.60.6 80 ms  60 ms  40 ms

  2 10.0.0.1 40 ms  40 ms  60 ms

  3 192.168.50.253 80 ms  80 ms  80 ms
<AR2>

```

Figura 8, tracert da AR2 verso AR4 ed AR3

Riassumendo, lo stato delle interfacce ora è il seguente:

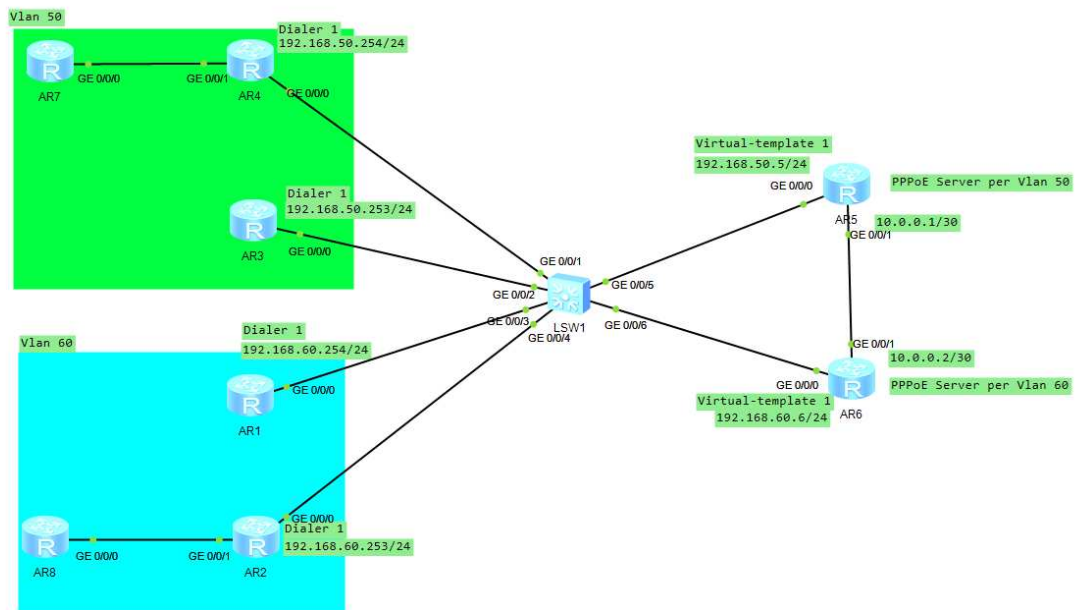


Figura 9, stato delle interfacce dopo aver stabilito le connessioni PPPoE

## Capitolo 4

### Introduzione ad IPv6

IPv6 è un protocollo che nasce nella fine degli anni 90' per fronteggiare la drastica diminuzione degli indirizzi IPv4. Mentre le tecniche di CIDR e NAT riescono a mitigare il problema temporaneamente, IPv6 è stato creato per durare nel tempo. Oggi diventa un protocollo irrinunciabile e sempre più sono i nodi ed i provider che lo implementano nativamente.

Il maggior vantaggio rispetto ad IPv4 è la diversa lunghezza dei campi degli indirizzi, che sono composti da 128 bit, invece di 32. Questi indirizzi sono anche più facilmente configurabili grazie ad un processo di autoconfigurazione.

L'header IPv6 contiene anche un campo chiamato flow label, un'etichetta utilizzata dal mittente per identificare delle sequenze di pacchetti per i quali richiede un trattamento speciale da parte del router: pacchetti appartenenti allo stesso traffic flow sono trasmessi usando lo stesso percorso, in modo tale che la sequenza non venga alterata. Questa tecnica assume particolare importanza soprattutto per le comunicazioni VoIP, riducendo la latenza.<sup>5</sup>

L'header può supportare anche delle estensioni, che supportano parametri aggiuntivi utili, per esempio, alla frammentazione o a IPSec, standard utilizzato per la sicurezza delle connessioni. Questo è possibile grazie al campo *Next header*.

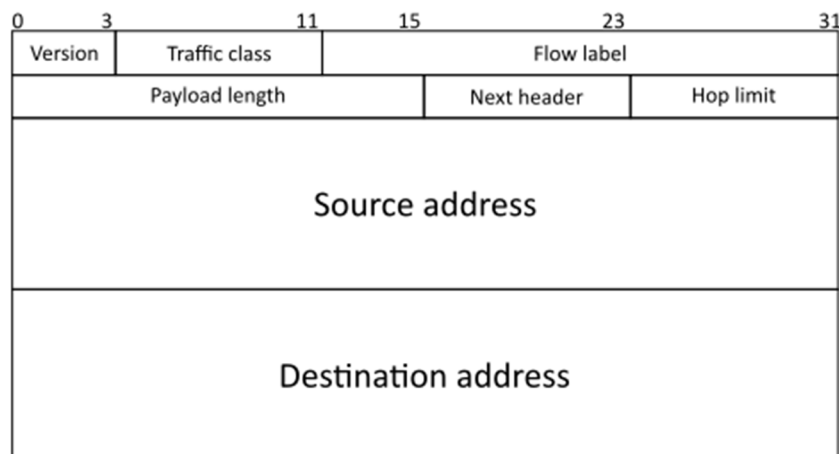


Figura 10, IPv6 Header. Immagine di Wikipedia, l'enciclopedia libera

<sup>5</sup> Header IPv6, da slides del corso "HCIA Routing&Switching"

Gli indirizzi IPv6 sono composti da un prefisso e da un Interface ID, essi sono comunemente scritti attraverso una notazione esadecimale. Il prefisso riservato alla documentazione, utilizzato anche nel progetto, è 2001:0DB8::/32.

Gli indirizzi IPv6 possono essere suddivisi in più categorie: global unicast, link-local, unique local unicast, multicast, solicited node multicast e anycast.

- Global unicast: utilizzati per reti pubbliche, il campo interface ID è di 64-bit.
- Link-local: Vengono utilizzati per veicolare dati di protocolli accessori e per i protocolli di routing. I primi 10 bit sono impostati al valore FE80, seguono 54bit impostati a zero.  
Infatti, sono utilizzati per comunicazioni locali, ovvero in un contesto che non prevede necessità di suddivisione in sottoreti.
- Unique Local Unicast: possono essere considerati degli indirizzi “privati” IPv6.
- Multicast addresses: si distinguono per il prefisso FFxx::/8, sono riservati all’utilizzo all’interno di alcuni protocolli (es. FF02::1 All Nodes Addresses, FF02::2 All Routers Addresses).
- Solicited Node Multicast: viene calcolato a partire dall’indirizzo unicast di interfaccia. I primi 104 bit sono pari a FF02::1:FF e gli ultimi 24 corrispondono a quelli dell’indirizzo unicast di interfaccia. Viene utilizzato per pacchetti di tipo Router Solicitation o Neighbor Solicitation (che saranno analizzati tra poco).
- Gli indirizzi anycast: permettono a più dispositivi di essere associati allo stesso indirizzo.

Come anticipato, la capacità di autoconfigurazione degli indirizzi IPv6 in un’interfaccia è un grande vantaggio. Questo è possibile attraverso la ricezione di tutte le informazioni necessarie dagli altri nodi della rete. L’autoconfigurazione è detta Stateless Address Auto-Configuration (SLAAC).

La SLAAC si basa sullo scambio di alcuni messaggi sulla rete: Router Solicitation (RS), che corrisponde ad una richiesta di informazioni ad un nodo di rete, e Router advertisement (RA), che contiene informazioni sulla configurazione di rete e l’indirizzo del router. Il primo avviene ponendo come destination address un indirizzo multicast, il secondo può essere solicited, nel caso di un precedente RS, o unsolicited.



L'interface ID di un IPv6 address può essere configurato manualmente o generato attraverso uno standard chiamato IEEE 64-bit Extended Unique Identifier (EUI-64), che utilizza l'indirizzo MAC address del dispositivo come in figura 11.

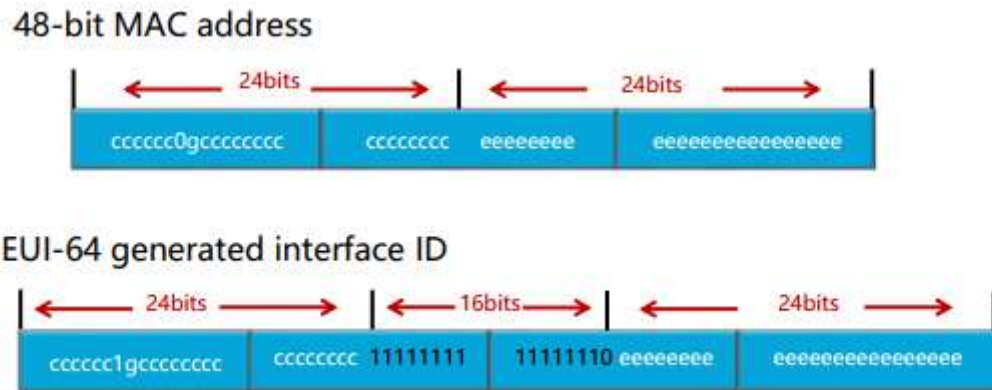


Figura 11, funzionamento EUI-64. Immagine di Huawei Technologies Co., Ltd: slide del corso "HCIA Routing&Switching"

Lo SLAAC si basa anche su un altro protocollo, che può essere paragonato ad ARP in IPv4: il Neighbor Discovery Protocol. Esso definisce una coppia di messaggi chiamati Neighbor Solicitation (NS) e Neighbor Advertisement (NA): il Neighbor Solicitation chiede ad un host con un dato indirizzo IPv6, di rispondere con il suo MAC-address mentre il Neighbor Advertisement (NA) può essere sia in risposta ad un NS che unsolicited, quindi inviato a FF02::1.

Infine, prima che un indirizzo sia assegnato ad un'interfaccia, il Duplicate Address Detection (DAD) si occupa di verificare se questo sia già associato ad un altro nodo. Il DAD può essere paragonato al gratuitous ARP.

Oltre allo SLAAC un altro metodo per la configurazione di IPv6 è il DHCPv6. Come il normale DHCP, esso si basa su un'architettura Client-Server. Dato che il progetto preso in esame prevede l'utilizzo di soli due router con indirizzi IPv6 global unicast, si è deciso di non analizzare questo protocollo.

## Capitolo 5

### Tunnel GRE e IPv6 addresses

Come già anticipato nel primo capitolo le interfacce GE 0/0/0 di AR7 e AR8 hanno sia indirizzi IPv6 global unicast che link-local. Tramite queste interfacce essi possono comunicare rispettivamente con AR4 e AR2, che devono quindi avere indirizzi link-local nelle interfacce GE 0/0/1.

Si è deciso di popolare le tabelle di routing IPv6 tramite OSPFv3 invece di implementare le rotte statiche per rendere la rete più dinamica possibile. Anche le interfacce di tipo tunnel di AR4 e AR2 devono quindi avere indirizzi link-local per poter utilizzare OSPFv3 su di esse.

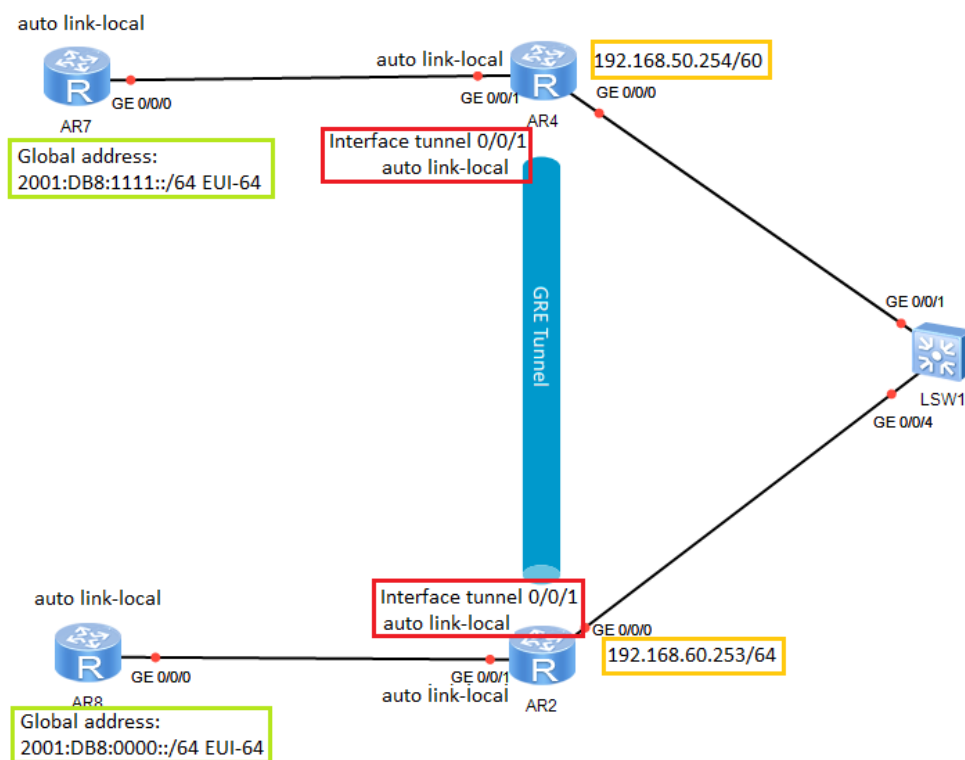
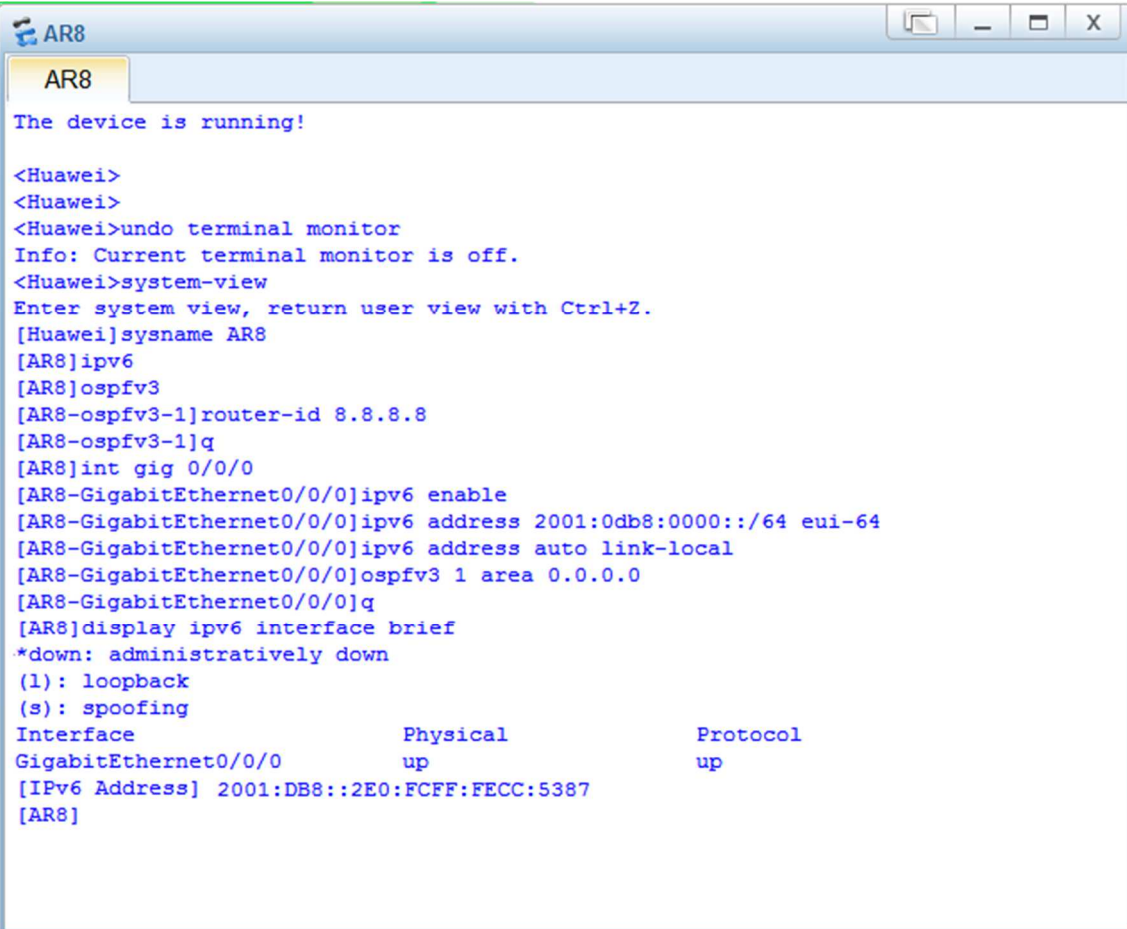


Figura 12, interfacce IPv6 e tunnel GRE

La configurazione di AR8 è la seguente:



```
AR8
The device is running!

<Huawei>
<Huawei>
<Huawei>undo terminal monitor
Info: Current terminal monitor is off.
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname AR8
[AR8]ipv6
[AR8]ospfv3
[AR8-ospfv3-1]router-id 8.8.8.8
[AR8-ospfv3-1]q
[AR8]int gig 0/0/0
[AR8-GigabitEthernet0/0/0]ipv6 enable
[AR8-GigabitEthernet0/0/0]ipv6 address 2001:0db8:0000::/64 eui-64
[AR8-GigabitEthernet0/0/0]ipv6 address auto link-local
[AR8-GigabitEthernet0/0/0]ospfv3 1 area 0.0.0.0
[AR8-GigabitEthernet0/0/0]q
[AR8]display ipv6 interface brief
*down: administratively down
(1): loopback
(s): spoofing
Interface                Physical      Protocol
GigabitEthernet0/0/0     up           up
[IPv6 Address] 2001:DB8::2E0:FCFF:FECC:5387
[AR8]
```

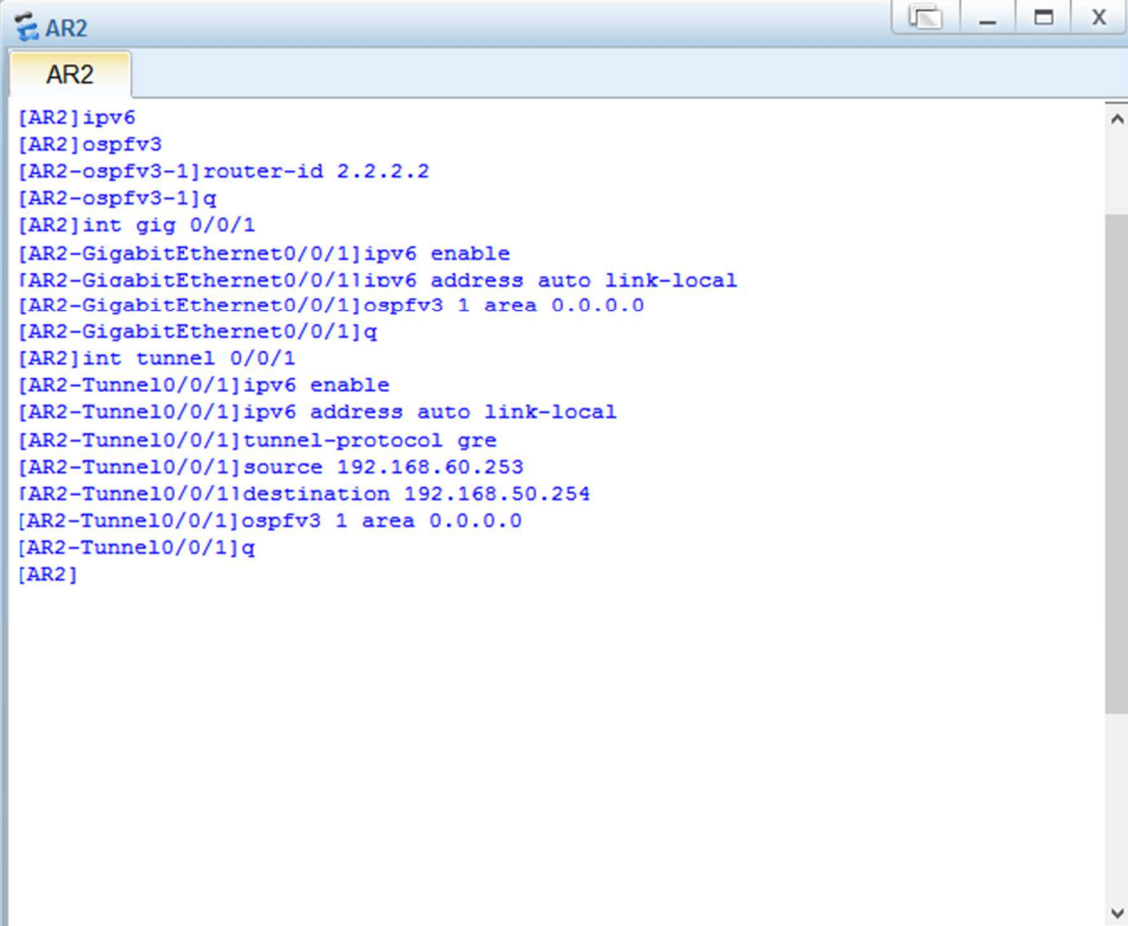
Figura 13, configurazione IPv6 di AR8: global unicast e link-local addresses, attivazione di OSPFv3.

Si nota la diversa configurazione di OSPFv3 rispetto ad OSPFv2: il router-id (anche qui corrispondente al numero del router) è specificato all'interno del processo OSPFv3 e l'attivazione avviene direttamente all'interno dell'interfaccia.

Con un “display ipv6 interface brief” vediamo che l'indirizzo IPv6 global unicast di AR8 è 2001:DB8::2E0:FCFF:FECC:5387/64. Facendo lo stesso per AR7 il suo indirizzo IPv6 global unicast è 2001:DB8:1111:0:2E0:FCFF:FE70:66D9/64.

Per poter mettere in comunicazione AR7 e AR8 si implementa un Generic routing encapsulation tunnel (GRE tunnel) tra AR2 e AR4. Questo deve avere come source ip-address, l'indirizzo dell'interfaccia verso la sede centrale dell'azienda e, come destination address, il corrispondente indirizzo dell'altro end-point.

Come mostrato in figura 14, dopo aver abilitato IPv6 su GE 0/0/1 e sull'interfaccia Tunnel 0/0/1, si attiva il processo di autoconfigurazione dell'indirizzo link-local su entrambe le interfacce. Successivamente si configura il protocollo OSPFv3 (slegato completamente dal processo OSPFv2 utilizzato per mettere in comunicazione le due Vlan). Il source del tunnel è 192.168.60.253, indirizzo di AR2 verso la sede centrale, e come destination 192.168.50.254, indirizzo corrispondente di AR4.

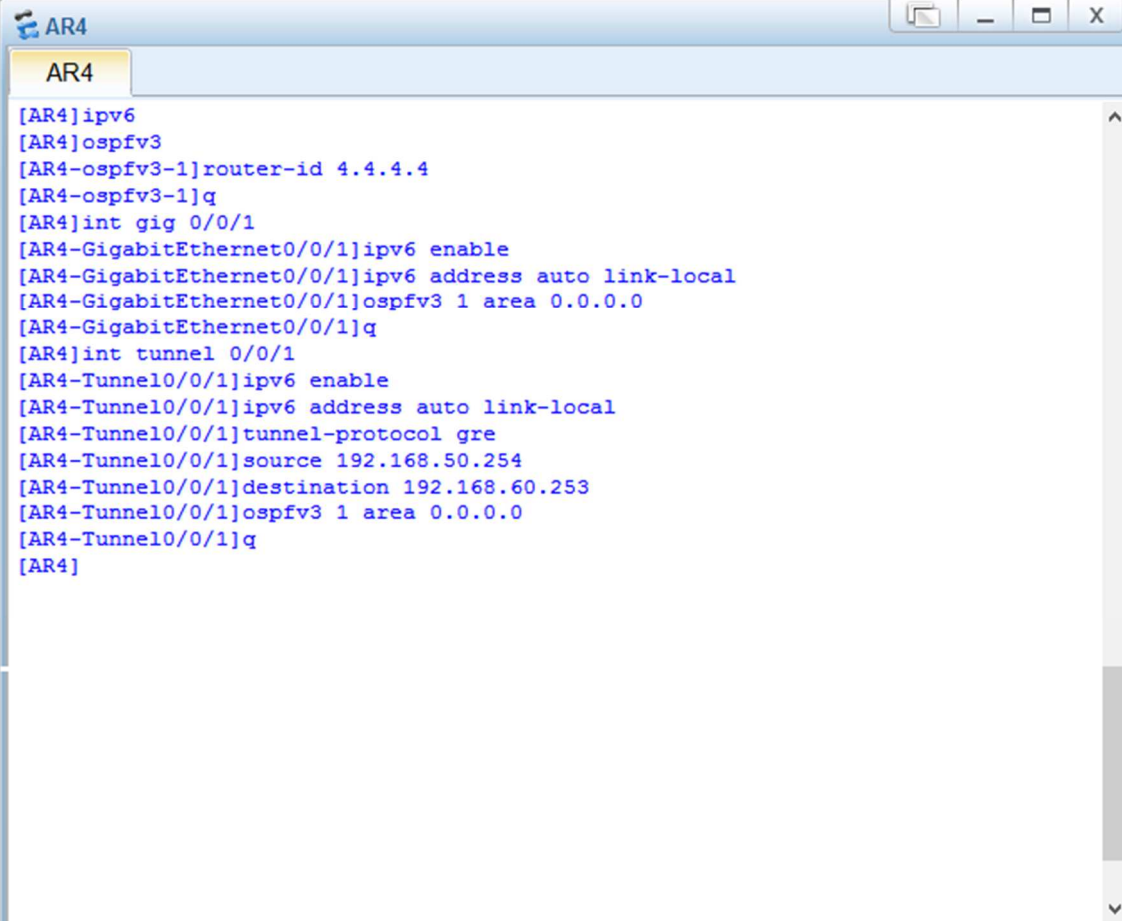


```
[AR2]ipv6
[AR2]ospfv3
[AR2-ospfv3-1]router-id 2.2.2.2
[AR2-ospfv3-1]q
[AR2]int gig 0/0/1
[AR2-GigabitEthernet0/0/1]ipv6 enable
[AR2-GigabitEthernet0/0/1]ipv6 address auto link-local
[AR2-GigabitEthernet0/0/1]ospfv3 1 area 0.0.0.0
[AR2-GigabitEthernet0/0/1]q
[AR2]int tunnel 0/0/1
[AR2-Tunnel0/0/1]ipv6 enable
[AR2-Tunnel0/0/1]ipv6 address auto link-local
[AR2-Tunnel0/0/1]tunnel-protocol gre
[AR2-Tunnel0/0/1]source 192.168.60.253
[AR2-Tunnel0/0/1]destination 192.168.50.254
[AR2-Tunnel0/0/1]ospfv3 1 area 0.0.0.0
[AR2-Tunnel0/0/1]q
[AR2]
```

Figura 14, configurazione del tunnel GRE e degli indirizzi link-local nelle interfacce di AR2, abilitazione OSPFv3

Gli indirizzi dei PPPoE client possono cambiare ad ogni riavvio dei router, in quanto sono assegnati dal PPPoE Server. Perciò questi indirizzi sono validi solamente finché la comunicazione non si interrompe, in questo caso la configurazione appena effettuata sarebbe da modificare inserendo come source e address gli indirizzi IPv4 opportuni. Per quanto riguarda eNSP, il Server assegna per primo l'indirizzo 192.168.x.254 per poi procedere con 192.168.x.253 etc. Quindi con l'accortezza di accendere prima AR4 e AR1 ed in un secondo momento AR2 e AR3, non è necessario modificare i parametri.

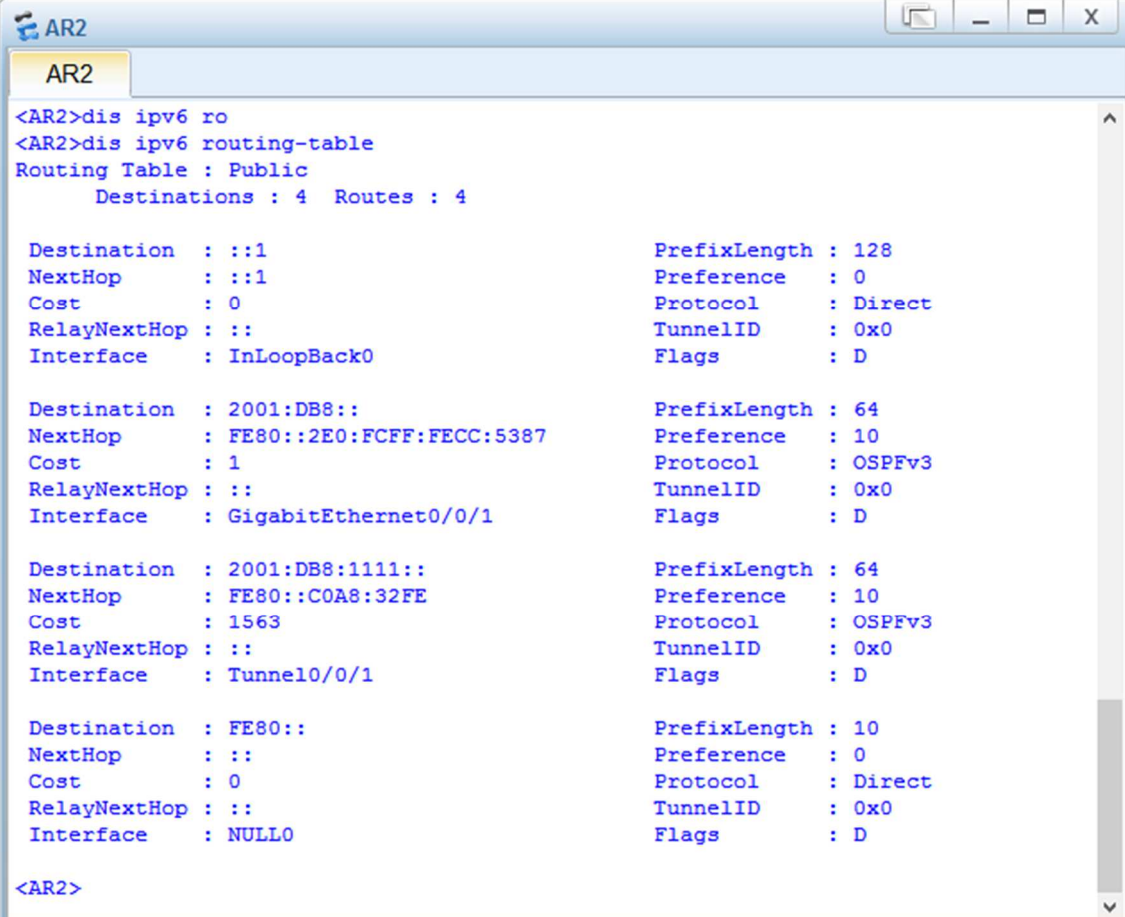
Per AR4 la configurazione è la medesima con source e destination invertiti, oltre che, ovviamente, al router-id diverso:



```
[AR4]ipv6
[AR4]ospfv3
[AR4-ospfv3-1]router-id 4.4.4.4
[AR4-ospfv3-1]q
[AR4]int gig 0/0/1
[AR4-GigabitEthernet0/0/1]ipv6 enable
[AR4-GigabitEthernet0/0/1]ipv6 address auto link-local
[AR4-GigabitEthernet0/0/1]ospfv3 1 area 0.0.0.0
[AR4-GigabitEthernet0/0/1]q
[AR4]int tunnel 0/0/1
[AR4-Tunnel0/0/1]ipv6 enable
[AR4-Tunnel0/0/1]ipv6 address auto link-local
[AR4-Tunnel0/0/1]tunnel-protocol gre
[AR4-Tunnel0/0/1]source 192.168.50.254
[AR4-Tunnel0/0/1]destination 192.168.60.253
[AR4-Tunnel0/0/1]ospfv3 1 area 0.0.0.0
[AR4-Tunnel0/0/1]q
[AR4]
```

Figura 15, configurazione del tunnel GRE e degli indirizzi link-local nelle interfacce di AR4, abilitazione OSPfv3

Per verificare il corretto funzionamento di OSPFv3, analizziamo la Routing table IPv6 dei router, in figura 16 si riporta quella di AR2:



```
<AR2>dis ipv6 ro
<AR2>dis ipv6 routing-table
Routing Table : Public
  Destinations : 4  Routes : 4

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

Destination : 2001:DB8::          PrefixLength : 64
NextHop     : FE80::2E0:FCFF:FECC:5387 Preference   : 10
Cost       : 1                   Protocol     : OSPFv3
RelayNextHop : ::                TunnelID    : 0x0
Interface  : GigabitEthernet0/0/1 Flags       : D

Destination : 2001:DB8:1111::     PrefixLength : 64
NextHop     : FE80::COA8:32FE     Preference   : 10
Cost       : 1563                Protocol     : OSPFv3
RelayNextHop : ::                TunnelID    : 0x0
Interface  : Tunnel10/0/1        Flags       : D

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

<AR2>
```

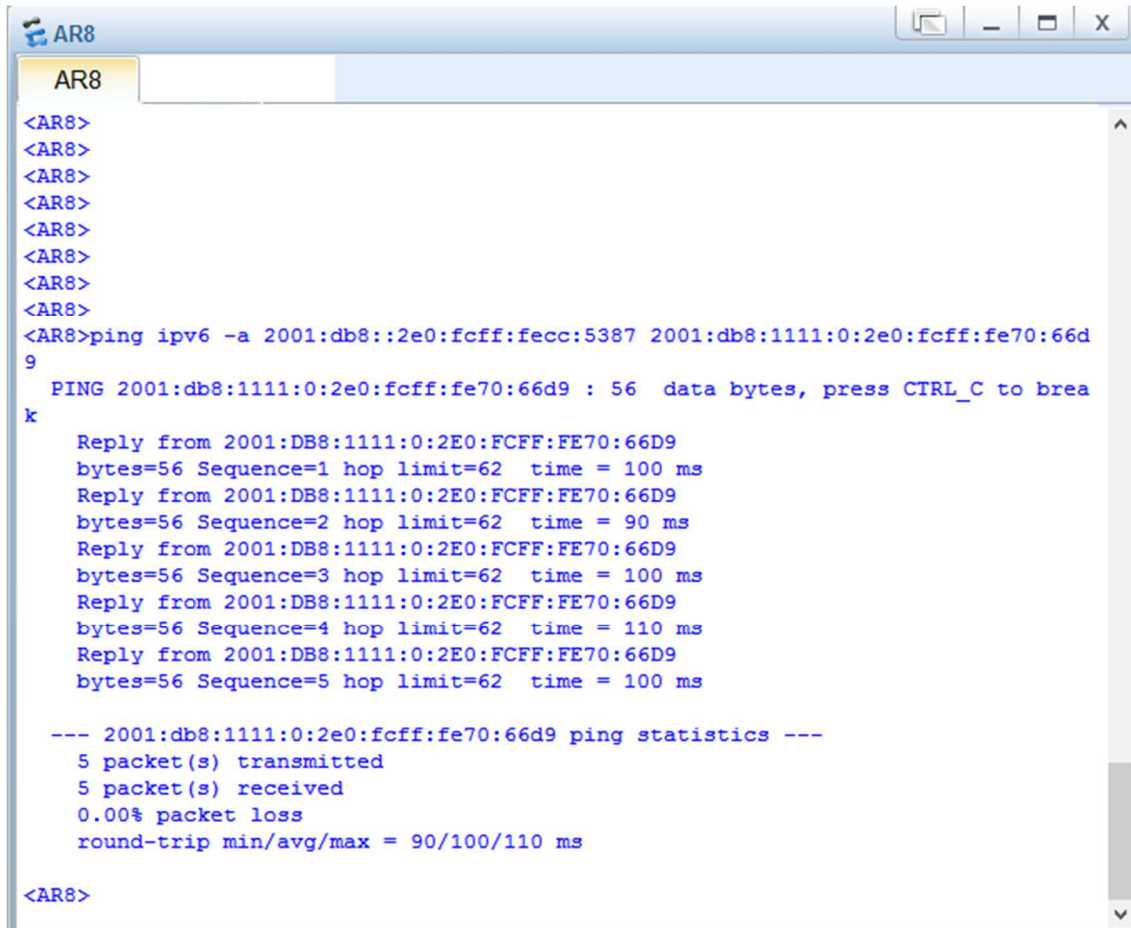
Figura 16, IPv6 routing-table di AR2

Notare che le rotte calcolate dal protocollo di instradamento sono la seconda e la terza dell'elenco:

- la destination 2001:DB8:: è raggiungibile attraverso l'interfaccia GE 0/0/1, il next hop è indicato come indirizzo link-local e corrisponde a quello della GE 0/0/0 di AR8.
- la destination 2001:DB8:1111:: è raggiungibile invece attraverso l'interfaccia Tunnel 0/0/1, anche in questo caso il next hop è un link-local, quello dell'interfaccia Tunnel 0/0/1 di AR4.

Per verificare che il collegamento sia funzionante, effettuiamo un ping IPv6 tra i due router.

All'interno del comando, al contrario del normale ping IPv4, è necessario specificare l'indirizzo di source:



```
AR8
AR8
<AR8>
<AR8>
<AR8>
<AR8>
<AR8>
<AR8>
<AR8>
<AR8>
<AR8>
<AR8>ping ipv6 -a 2001:db8::2e0:fcff:fecc:5387 2001:db8:1111:0:2e0:fcff:fe70:66d9
9
PING 2001:db8:1111:0:2e0:fcff:fe70:66d9 : 56 data bytes, press CTRL_C to break
Reply from 2001:DB8:1111:0:2E0:FCFF:FE70:66D9
bytes=56 Sequence=1 hop limit=62 time = 100 ms
Reply from 2001:DB8:1111:0:2E0:FCFF:FE70:66D9
bytes=56 Sequence=2 hop limit=62 time = 90 ms
Reply from 2001:DB8:1111:0:2E0:FCFF:FE70:66D9
bytes=56 Sequence=3 hop limit=62 time = 100 ms
Reply from 2001:DB8:1111:0:2E0:FCFF:FE70:66D9
bytes=56 Sequence=4 hop limit=62 time = 110 ms
Reply from 2001:DB8:1111:0:2E0:FCFF:FE70:66D9
bytes=56 Sequence=5 hop limit=62 time = 100 ms

--- 2001:db8:1111:0:2e0:fcff:fe70:66d9 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 90/100/110 ms

<AR8>
```

Figura 17, ping IPv6 da AR8 ad AR7

Il ping tra AR8 e AR7 è andato a buon fine, perciò l'obiettivo del progetto è stato raggiunto e tutte le specifiche sono state soddisfatte.

## Conclusione

In conclusione al progetto, è interessante analizzare la struttura del frame inviato per effettuare l'Echo Request, generato durante l'operazione di ping IPv6 effettuata nel capitolo precedente:

```
▶ Frame 88: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface -, id 0
  Ethernet II, Src: HuaweiTe_60:0e:d8 (00:e0:fc:60:0e:d8), Dst: HuaweiTe_86:59:5f (00:e0:fc:86:59:5f)
    ▶ Destination: HuaweiTe_86:59:5f (00:e0:fc:86:59:5f)
    ▶ Source: HuaweiTe_60:0e:d8 (00:e0:fc:60:0e:d8)
    Type: PPPoE Session (0x8864)
  PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0002
    Payload Length: 130
  Point-to-Point Protocol
    Protocol: Internet Protocol version 4 (0x0021)
  Internet Protocol Version 4, Src: 192.168.60.253, Dst: 192.168.50.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 128
    Identification: 0x000b (11)
    ▶ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 254
    Protocol: Generic Routing Encapsulation (47)
    Header checksum: 0xcaf7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.60.253
    Destination: 192.168.50.254
  Generic Routing Encapsulation (IPv6)
    ▶ Flags and Version: 0x0000
    Protocol Type: IPv6 (0x86dd)
  Internet Protocol Version 6, Src: 2001:db8::2e0:fcff:fecc:5387, Dst: 2001:db8:1111:0:2e0:fcff:fe70:66d9
    0110 .... = Version: 6
    ▶ .... 0000 0000 .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... 0000 0000 0000 0000 = Flow Label: 0x000000
    Payload Length: 64
    Next Header: ICMPv6 (58)
    Hop Limit: 63
    Source: 2001:db8::2e0:fcff:fecc:5387
    Destination: 2001:db8:1111:0:2e0:fcff:fe70:66d9
    [Source SA MAC: HuaweiTe_cc:53:87 (00:e0:fc:cc:53:87)]
    [Destination SA MAC: HuaweiTe_70:66:d9 (00:e0:fc:70:66:d9)]
  Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x56b7 [correct]
    [Checksum Status: Good]
    Identifier: 0xd0ab
    Sequence: 256
    [Response In: 89]
  ▶ Data (56 bytes)
```

Figura 18, grab di Wireshark: struttura del frame che contiene un echo request effettuato da AR8



Il grab Wireshark di figura 18 proviene da uno *start data capture* all'interfaccia dello switch.

Il pacchetto IPv6 è veicolato da GRE, il quale a sua volta è protetto da PPPoE. Il frame è così composto:



Figura 19, rappresentazione del frame di figura 18. Immagine creata a partire da frammenti di immagine provenienti dalle slide del corso "HCIA Routing&Switching" di Huawei Technologies Co., Ltd.

Analizziamo ora i vari campi del frame ethernet:

- la sessione PPPoE è avviata ed ha come Session ID 0x0002;
- la comunicazione IPv4 è protetta da autenticazione chap, dove l'autenticator è in questo caso è AR6;
- il campo data del pacchetto IPv4 comprende il restante del frame, eccetto l'FCS;
- il protocollo indicato nell'header IPv4 è GRE, il quale a sua volta trasporta IPv6;
- l'header IPv6 contiene le informazioni source e destination (rispettivamente AR8 e AR7) e nel campo "Next Header" ha ICMPv6;
- ICMPv6 è di tipo Echo (ping) Request.
- L'FCS è la parte finale del frame e serve per il riconoscimento di eventuali errori di ricezione all'interno del frame stesso.

Ora che la rete aziendale è completamente configurata, è possibile accedervi attraverso personal computer, o dispositivi wireless una volta configurato l'access-point nei router. All'interno delle due VLAN è possibile utilizzare dispositivi IPv4 ed IPv6, senza dover implementare particolari configurazioni, grazie alla presenza di router che possono offrire entrambe le connettività. Eventualmente è possibile configurare dei NAT, per poter sfruttare gli spazi degli indirizzi già esistenti. Un altro miglioramento possibile è quello di creare una ridondanza delle connessioni, per poter rendere la rete più robusta. Questo può avvenire, per esempio, attraverso l'utilizzo di link-aggregation o la presenza di più switch.

## Appendice A

### Implementazione VLAN

L'aggiunta di questa appendice è dovuta alla possibilità di implementare in modo diverso le VLAN. Infatti, nella rete fin qui progettata si è scelto di non configurare queste nello switch centrale, quando invece sarebbe potuto essere utile nel controllo del traffico tra le due LAN virtuali.

È opportuno quindi fare una considerazione: dato che il traffico tra le due VLAN passa sempre attraverso AR5 e AR6, ovvero i rispettivi PPPoE server, è possibile controllare il traffico anche attraverso l'aggiunta di ACL in questi router. Un'ACL (Access Control List) è una lista ordinata di regole associata alle risorse di un sistema informatico che stabilisce delle regole, dette permessi, in base alle quali gli utenti o processi possono accedervi e compiere le operazioni specificate.<sup>6</sup>

Se si volesse, ad esempio, impedire ad AR3 di comunicare con i router appartenenti alla Vlan60, si potrebbe introdurre un'ACL di tipo traffic filter in AR5 (GE 0/0/1 outbound) o in AR6 (Ge 0/0/1 inbound), in cui si vieta alla sorgente 192.168.50.253 di poter far transitare i pacchetti in quelle interfacce, quindi di impedire la comunicazione con la Vlan60:

```
AR5
<AR5>
<AR5>sy
<AR5>system-view
Enter system view, return user view with Ctrl+Z.
[AR5]acl 2000
[AR5-acl-basic-2000]rule 5 deny source 192.168.50.253 0.0.0.0
[AR5-acl-basic-2000]rule 10 permit source any
[AR5-acl-basic-2000]q
[AR5]int gig 0/0/1
[AR5-GigabitEthernet0/0/1]traffic-filter outbound acl 2000
[AR5-GigabitEthernet0/0/1]q
[AR5]
```

Figura 20, creazione di un'ACL in AR5 per bloccare il traffico proveniente da AR3

<sup>6</sup> Lista di controllo accessi, da Wikipedia, l'enciclopedia libera

Con l'ACL implementata in figura 20, AR3 non è in grado di inviare pacchetti ad AR6, AR1 e AR2, ma può solo riceverli.

Effettuando quindi un ping con questi dispositivi, questo avrà esito negativo:

```
AR3
The device is running!

<AR3>ping 192.168.60.254
  PING 192.168.60.254: 56 data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

--- 192.168.60.254 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
```

Figura 21, ping fallito da AR3 verso AR1

Come detto ad inizio appendice questa non è l'unica scelta possibile: nel caso si scegliesse di configurare le VLAN sullo switch sarebbe infatti possibile controllare l'accesso alle porte di questo a seconda della VLAN di appartenenza.

La configurazione da effettuare sarebbe la seguente:

- Creazione delle Vlan50 e Vlan60 dello switch tramite il comando “*vlan batch 50 60*”
- Indicare il tipo di porta nelle interfacce con “*port link-type access/trunk*”  
GE 0/0/1, GE 0/0/2, GE 0/0/3 e GE 0/0/4 di tipo access  
GE 0/0/5 e GE 0/0/6 di tipo trunk
- Assegnare la vlan di appartenenza alle porte di tipo access con “*port default vlan 50/60*”
- Per poter far viaggiare i frame sempre in modalità untagged assegnare alla porta trunk GE 0/0/5 l'ID 50 e a GE 0/0/6 l'ID 60 tramite “*port trunk pvid vlan 50/60*”
- A seconda delle esigenze permettere il traffico nelle porte trunk tramite “*port trunk allow-pass vlan x y*”

Con quest'ultimo comando è possibile, come fatto con le ACL, stabilire delle regole di comunicazione.

In questo caso però ci sono maggiori limitazioni, in quanto non è possibile “isolare” un solo router, ma si comprende l'intera LAN virtuale.

## Bibliografia

- “*HCNA Networking Study Guide*”, Huawei Technologies Co., Ltd., Springer.
- Slides del corso “*HCIA Routing&Switching*” Basic e Intermediate, Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

### Software:

- eNSP, guida di installazione al link:  
<https://support.huawei.com/enterprise/it/management-system/ensp-pid-9017384>
- Wireshark, installazione al link:  
<https://www.wireshark.org/download.html>
- GIMP - GNU Image Manipulation Program, maggiori informazioni in:  
<https://www.gimp.org/>
- Hedex Lite, installazione al link:  
<https://support.huawei.com/carrier/docview!docview?nid=SCL1000005027&path=PAN-ET/PAN-T/PAN-T-HedEx>