

FirstAssignment

Gian Maria Gennai

October 2023

1 Introduzione

All'interno di questo testo vedremo in breve come ho simulato una piccola rete IPv6 formata da due host e un router.

2 Simulation Network IPv6 - GNS3

Per fare la simulazione ho utilizzato **GNS3**, per il semplice fatto che è disponibile anche per il sistema operativo Windows. GNS3 è un simulatore con un'interfaccia grafica che permette di creare manualmente la struttura della rete per poi andare a settare i vari dispositivi sul terminale di ogni componente.

GNS3 oltre a simulare la rete ci permette anche di avere una rappresentazione grafica della struttura generale(*figura 1*).

3 Setup

Nella *figura 1*, possiamo vedere la struttura della rete che è formata da 2 host(**PC1**, **PC2**), uno switch e un router(**c3745**). Accanto ai vari dispositivi possiamo vedere i propri indirizzi.

Dopo aver disposto i vari dispositivi, collegati e avviata la simulazione, ho potuto aprire il terminale per andare a settare gli indirizzi.

Nella *figura 2* vediamo il codice per impostare gli indirizzi IPv6 dei dispositivi di host. In figura 3 invece abbiamo il codice che mi permette di abilitare alla modifica il router e poi il settaggio degli indirizzi IPv6 con annesso il collegamento ai due dispositivi di host. Abbiamo che con '*ipv6 address 2001:DB8:1::1/64*' impostiamo l'indirizzo del router e dopo andiamo ad assegnare a questo indirizzo quello dei due host tramite il comando '*ipv6 route...*'.

4 Test

Adesso, dopo aver completato l'intero setup della rete, possiamo andare a vedere se tutto funziona correttamente oppure se ci sono alcuni problemi interni.

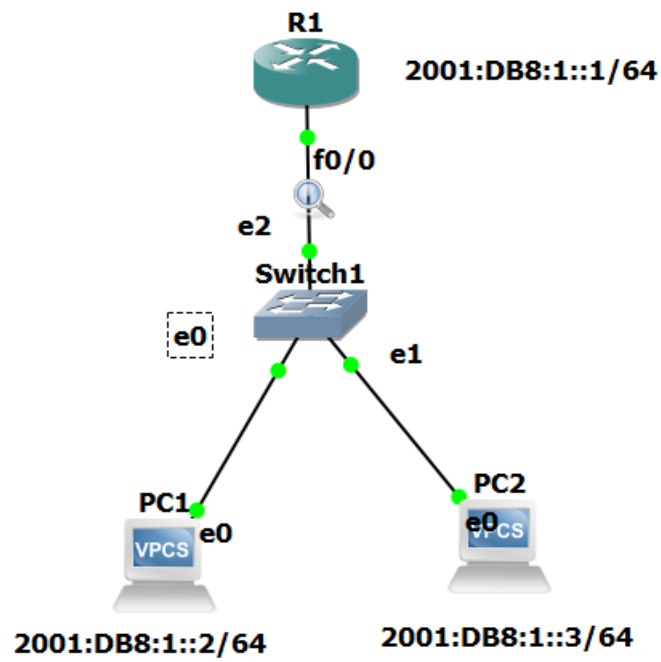


Figure 1: Schema simulazione rete IPv6

```
PC1> ip 2001:DB8:1::2/64
PC1 : 2001:db8:1::2/64
```

(a) Indirizzo PC1

```
PC2> ip 2001:DB8:1::3/64
PC1 : 2001:db8:1::3/64
```

(b) Indirizzo PC2

Figure 2: Indirizzi PC1 e PC2

```

R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ipv6 address 2001:DB8:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ipv6 route 2001:DB8:1::1/64 2001:DB8:1::2
R1(config)#ipv6 route 2001:DB8:1::1/64 2001:DB8:1::3
R1(config)#exit
R1#wr
Building configuration...
[OK]
R1#

```

Figure 3: Setup router c3745

```

show
NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PORT
PC1       0.0.0.0/0    0.0.0.0      00:50:79:66:68:00  10020  127.0.0.1:10021
          fe80::250:79ff:fe66:6800/64
          2001:db8:1:0:2050:79ff:fe66:6800/64 eui-64

PC1> ping 2001:db8:1:0:2050:79ff:fe66:6801

2001:db8:1:0:2050:79ff:fe66:6801 icmp6_seq=1 ttl=63 time=62.032 ms
2001:db8:1:0:2050:79ff:fe66:6801 icmp6_seq=2 ttl=63 time=30.534 ms
2001:db8:1:0:2050:79ff:fe66:6801 icmp6_seq=3 ttl=63 time=30.224 ms
2001:db8:1:0:2050:79ff:fe66:6801 icmp6_seq=4 ttl=63 time=30.369 ms
2001:db8:1:0:2050:79ff:fe66:6801 icmp6_seq=5 ttl=63 time=30.466 ms

```

Figure 4: Informazioni PC1 e ping verso PC2

In *figura 4* sono mostrate le informazioni relative all'host PC1.

Oltre alle informazioni relative agli indirizzi tra cui l'indirizzo **link local**(**fe80::250...**) e **global**(**2001:db8:...**), possiamo vedere(in *figura 4*) che viene mandato un ping verso l'altro host interno alla rete (PC2) e che viene data una risposta conseguenza del fatto che è stato trovato correttamente chi si stava cercando. In *figura 5* possiamo vedere come il router R1 identifica i suoi neighbor ovvero PC1 e PC2 tramite indirizzi IPv6.

```

R1#show ipv6 neighbor
IPv6 Address                               Age Link-layer Addr State Interface
2001:DB8:1:0:2050:79FF:FE66:6801           6 0050.7966.6801 STALE Fa0/0
2001:DB8:1:0:2050:79FF:FE66:6800           6 0050.7966.6800 STALE Fa0/0

```

Figure 5: Router's neighbor

1 0.000000	::	ff02::2	ICMPv6	62 Router Solicitation
2 0.000000	::	ff02::2	ICMPv6	62 Router Solicitation
3 4.341140	::	ff02::1:ff8b:0	ICMPv6	78 Neighbor Solicitation for fe80::c601:28ff:feb8:0
4 4.403660	::	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
5 4.419881	::	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
6 4.686762	::	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
7 4.702476	c4:01:28:b8:00:00	CDP/VTP/DTP/PagP/UD...	CDP	399 Device ID: R1 Port ID: FastEthernet0/0
8 4.718645	c4:01:28:b8:00:00	DEC-MOP-Remote-Cons...	0x6002	77 DEC DNA Remote Console
9 5.350304	fe80::c601:28ff:feb8:0	ff02::1	ICMPv6	86 Neighbor Advertisement fe80::c601:28ff:feb8:0 (rtr, ovr) is at c4:01:28:b8:00:00
10 5.365931	fe80::c601:28ff:feb8:0	ff02::1	ICMPv6	118 Router Advertisement from c4:01:28:b8:00:00
11 5.381717	fe80::c601:28ff:feb8:0	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
12 5.397348	fe80::c601:28ff:feb8:0	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
13 5.413075	fe80::c601:28ff:feb8:0	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
14 5.428961	::	ff02::1:ff00:1	ICMPv6	78 Neighbor Solicitation for 2001:db8:1::1
15 5.647814	fe80::c601:28ff:feb8:0	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
16 5.692813	c4:01:28:b8:00:00	CDP/VTP/DTP/PagP/UD...	CDP	399 Device ID: R1 Port ID: FastEthernet0/0
17 6.145962	fe80::c601:28ff:feb8:0	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
18 6.350358	2001:db8:1::1	ff02::1	ICMPv6	86 Neighbor Advertisement 2001:db8:1::1 (rtr, ovr) is at c4:01:28:b8:00:00
19 6.50215	fe80::c601:28ff:feb8:0	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
20 6.697436	c4:01:28:b8:00:00	CDP/VTP/DTP/PagP/UD...	CDP	399 Device ID: R1 Port ID: FastEthernet0/0

Figure 6: Analisi pacchetti con Wireshark

4.1 Analisi pacchetti con Wireshark

Adesso possiamo analizzare il flusso dei pacchetti interni alla rete tramite un software dedicato, nel nostro caso **Wireshark**. Come vediamo nella *figura 6* abbiamo la lista dei pacchetti scambiati all'interno della rete.

Qui abbiamo una lista che mi rappresenta cosa rappresentano le colonne nell'immagine presa da Wireshark.

- I: tempo
- II: Indirizzo Sorgente
- III: Indirizzo Destinazione
- IV: Protocollo
- V: Lunghezza del pacchetto catturato
- VI: Informazione relativa al pacchetto catturato

In generale possiamo vedere alcuni pacchetti che non hanno l'indirizzo sorgente e questo perché sono azioni di scoperta della rete infatti possiamo vedere che nell'ultima colonna abbiamo un '*Multicast Listener Report Message v2*' il quale mi indica che un dispositivo sta partecipando attivamente ad un gruppo multicast IPv6 e sta confermando la sua intensione a ricevere traffico multicast relativo a quel gruppo, poi abbiamo '*Router sollecitation*' che invece mi indica un messaggio di scoperta inviato da un host IPv6 per richiedere informazioni sui router disponibili nella rete locale e poi abbiamo una '*Neighbor sollicitaion*' che viene fatta anche questa durante la fase di scoperta e serve per un host per andare a scoprire l'indirizzo fisico(**MAC**) di un altro host sempre all'interno della stessa rete locale, la risposta a questo sollecito viene data tramite il '*Neighbor advertisement*'. Altri pacchetti che possiamo notare sono quelli del protocollo **CDP** dovuti al router c3745 che sono messaggi di rete inviati dai dispositivi di rete **Cisco** per scambiare informazioni sulla topologia di rete, sulle connessioni tra dispositivi e su altre informazioni relative ai dispositivi Cisco all'interno di una rete.