



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

FACOLTÀ DI INGEGNERIA
CORSO DI LAUREA IN INGEGNERIA INFORMATICA E DELL'AUTOMAZIONE

Progettazione di soluzioni per il networking in ambito industriale

Designing solutions for industrial networking

Candidato:
Bedetta Alessandro

Relatore:
Prof. Gambi Ennio

Correlatore:
Ing. De Santis Adelmo

Anno Accademico 2020-2021



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

FACOLTÀ DI INGEGNERIA
CORSO DI LAUREA IN INGEGNERIA INFORMATICA E DELL'AUTOMAZIONE

Progettazione di soluzioni per il networking in ambito industriale

Designing solutions for industrial networking

Candidato:
Bedetta Alessandro

Relatore:
Prof. Gambi Ennio

Correlatore:
Ing. De Santis Adelmo

Anno Accademico 2020-2021

UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA
CORSO DI LAUREA IN INGEGNERIA INFORMATICA E DELL'AUTOMAZIONE
Via Brezze Bianche – 60131 Ancona (AN), Italy

*A tutti coloro che mi hanno permesso
di raggiungere questo traguardo...*

Sommario

In questa tesi verranno affrontate tematiche relative alla progettazione e allo sviluppo di un'infrastruttura di rete.

Nello specifico verrà analizzata una simulazione di una topologia la quale, verosimilmente, potrebbe essere la stessa riscontrata in un contesto aziendale/industriale.

Questa infrastruttura dovrà rispettare tutta una serie di specifiche, le quali ci guideranno nel processo di configurazione di una rete ad-hoc.

Indice

1	Introduzione	1
1.1	Introduzione	1
1.2	Motivazione dietro il progetto	1
2	La Topologia	3
2.1	Scopo del progetto e software utilizzati	3
2.2	Componenti	4
2.3	Specifiche	4
2.4	Richiami di teoria	5
2.5	Prime osservazioni	5
3	Configurazione	7
3.1	Scomposizione del progetto	7
3.2	Sezione 1	9
3.2.1	Link Aggregation	9
3.2.2	STP	10
3.2.3	VLAN	11
3.2.4	DHCP e Inter Vlan Routing	14
3.3	Sezione 2	16
3.3.1	ACL	16
3.3.2	NAT su AR1 e AR3	17
3.3.3	Rotte statiche e Link AR2-AR3	19
3.3.4	PPPoE Client e Server su AR2 e AR3	19
3.4	Sezione 3	22
3.4.1	DHCP	22
4	Test e note sulle prestazioni	23
4.1	Test sul funzionamento	23
4.1.1	DHCP su AR1 e AR3	23
4.1.2	Inter Vlan Routing	24
4.1.3	NAT su AR1 e AR3	26
4.1.4	Accesso a Internet	28
4.2	Test di robustezza	30
4.2.1	Test su LSW3 e LSW4	30
4.2.2	Test sul link AR2-AR3	31
4.3	Note sulle prestazioni	33

Indice

5 Note e Conclusioni	35
5.1 Note finali	35
5.2 Conclusioni	35

Elenco delle figure

2.1 Topologia fornita visualizzata tramite eNSP.	3
2.2 Divisione logica della topologia.	6
3.1 Prima sezione	7
3.2 Seconda sezione	8
3.3 Terza sezione	8
3.4 Aggiunta di un interfaccia ad un Trunk di LSW3	9
3.5 Illustrazione degli Ethernet-Trunk realizzati	9
3.6 Stato porte Switch 3	10
3.7 Stato porte Switch 4	10
3.8 Stato porte Switch 1	11
3.9 Stato porte Switch 2	11
3.10 Stato porte Switch 5	11
3.11 Configurazione interfaccia access	12
3.12 Configurazione interfaccia hybrid-tagged	12
3.13 Schema delle porte	13
3.14 Dichiarazione e assegnazione ip della vlan interface 10	14
3.15 Pool di indirizzi per le tre vlan.	14
3.16 PC1: Ip ricevuto dal dhcp e ping verso PC3 nella vlan 30	15
3.17 ACL usata per il filtraggio in uscita da AR1	16
3.18 Address group legato al NAT su AR1	17
3.19 Configurazione dell'interfaccia GigabitEthernet0/0/0 di AR1	17
3.20 Configurazione del NAT sulle interfacce Gig0/0/0 e Dialer 1 di AR3	18
3.21 Rotta statica verso 192.168.200.0 /24 su AR1	19
3.22 Rotte statiche su AR2	19
3.23 Pool di indirizzi per il Server PPPoE	20
3.24 Virtual Template per l'interfaccia da cui raggiungere il Server PPPoE	20
3.25 Assegnazione del Virtual Template all'Interfaccia	20
3.26 Configurazione del Client PPPoE	21
3.27 Binding fra Dialer 1 e interfaccia fisica	21
3.28 IP pool per la Vlan 1	22
3.29 Configurazione della VlanIf 1 su AR3	22
4.1 Negoziazione indirizzo IP col Server da parte di PC2.	23
4.2 Default GW e IP forniti dal DHCP a PC2.	24
4.3 Acquisizione IP di PC4.	24

Elenco delle figure

4.4	Negoziazione dell'indirizzo col Server su AR3.	24
4.5	Ping da PC1 a PC2.	25
4.6	ICMP Request in ingresso ad AR1.	25
4.7	ICMP Request in uscita da AR1.	26
4.8	Pacchetti in uscita da AR1.	26
4.9	Pacchetti in uscita da AR3.	27
4.10	Ping da PC1 verso AR2.	28
4.11	Ping da PC2 verso AR2.	28
4.12	Ping da PC3 verso AR2.	28
4.13	Ping da PC2 verso PC4.	29
4.14	Ruolo porte LSW2 con LSW3 funzionante.	30
4.15	Ruolo porte LSW2 con LSW3 non funzionante.	30
4.16	Ping da PC2 verso l'esterno con LSW3 fuori servizio.	31
4.17	Traffico sul link AR2-AR3.	31
4.18	Traffico sul link PPPoE.	32
4.19	Incapsulamento operato dal PPPoE sul pacchetto ICMP.	32
4.20	Packet-Loss fra AR2 e AR3.	33

Capitolo 1

Introduzione

1.1 Introduzione

Questo documento consiste in una **tesi progettuale**, ovvero mira ad illustrare i procedimenti seguiti e le soluzioni adottate per portare a completamento un progetto.

In quanto verranno trattati argomenti tecnici, verranno inseriti occasionalmente dei cenni teorici; questi ultimi tuttavia saranno finalizzati a motivare le scelte fatte in fase di progettazione e non a fornire una conoscenza completa al lettore.

A supporto della spiegazione scritta saranno anche inseriti grafici ed immagini, di cui nelle pagine precedenti è riportato un indice.

1.2 Motivazione dietro il progetto

Il progetto descritto in questa tesi rappresenta la conclusione del corso **HAINA Routing Switching**.

Questo corso mi ha fornito una preparazione molto approfondita su tutti gli argomenti riguardanti i concetti base del networking, il troubleshooting e la configurazione di dispositivi Huawei.

La maggior parte degli argomenti trattati durante tale corso sono stati di fondamentale importanza al fine di portare il progetto a completamento, rispettando tutte le specifiche fornite.

Alla base di tutto questo c'è un mio forte interesse verso il mondo del networking e della comunicazione fra dispositivi.

Oltre a questo credo che gli argomenti trattati nel corso, costituiscano una parte fondamentale del bagaglio culturale di un ingegnere informatico, il quale, dovrebbe essere anche in grado di risolvere problemi legati a tematiche, se vogliamo, non inerenti solo il mondo della programmazione.

Capitolo 2

La Topologia

2.1 Scopo del progetto e software utilizzati

Il fine di questo progetto è stato quello di applicare le conoscenze acquisite durante il corso HAINA, realizzando una configurazione di rete che rispettasse tutta una serie di specifiche fornite. A tal fine, mi è stata fornita una topologia di partenza sulla quale lavorare; quest'ultima è riportata più in basso.

L'intero progetto è stato realizzato tramite l'uso del simulatore **eNSP** che consente di ricreare strutture di rete al 100% fedeli alle topologie reali. Un' altro strumento di fondamentale importanza è stato **WhireShark**, un software finalizzato al packet-sniffing; eseguibile direttamente da eNSP, mi ha offerto la possibilità di andare ad visualizzare tutti i pacchetti che venivano trasmessi dai dispositivi.

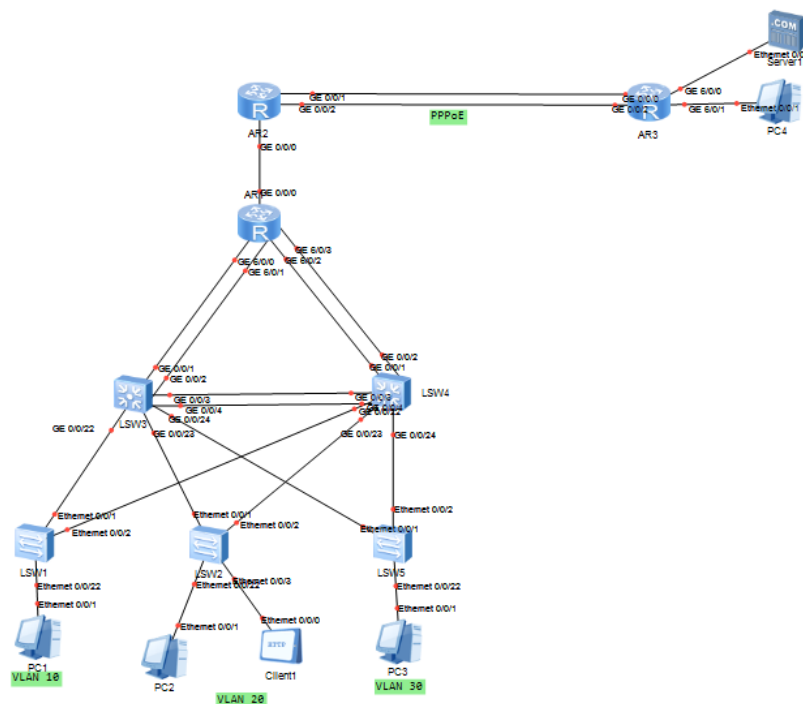


Figura 2.1: Topologia fornita visualizzata tramite eNSP.

2.2 Componenti

Come è possibile osservare nel grafico 2.1 la topologia è composta da :

- 3 Router AR2220 (**AR1, AR2, AR3**).
- 5 Switch (**LSW1, LSW2, LSW3, LSW4, LSW5**)
 - 2 Switch S5700
 - 3 Switch S3700
- 4 PC (**PC1, PC2, PC3, PC4**)
- Un Server DNS/HTTP/FTP (**Server 1**)
- Un Client HTTP/FTP (**Client 1**)

2.3 Specifiche

Di seguito sono riportate le **specifiche** che la topologia completamente configurata avrebbe dovuto rispettare.

- Configurare STP in modo tale che LSW3 sia primary root e LSW4 sia secondary root.
- Configurare Link Aggregation dove necessario.
- Configurare un DHCP server su AR1 per i calcolatori delle VLAN 10 20 e 30.
- AR1 dovrà effettuare l'Inter VLAN Routing fra le stesse VLAN elencate nel punto precedente.
- Solo i nodi appartenenti alla VLAN 20 dovranno essere capaci di accedere ad Internet, ma non potranno inviare traffico sulla porta 80.
- Configurare PPPoE Client e Server tra AR2 ed AR3; La connessione PPPoE dovrà essere un backup per la connessione Ethernet presente, pertanto dovrà attivarsi solo in caso di outage.
- Configurare DHCP e NAT su AR3 per PC4.

2.4 Richiami di teoria

Di seguito verranno molto sinteticamente richiamate alcune definizioni relative a protocolli e termini tecnici menzionati durante la definizione delle specifiche.

- **STP** : Spanning Tree Protocol, Si tratta di un protocollo di livello 2, finalizzato ad evitare che sulla topologia siano presenti dispositivi collegati a loop, i quali potrebbero peggiorare di molto le prestazioni della rete (**Broadcast Storm**). Questo protocollo assegna dei ruoli alle porte degli Switch, i quali a questo punto presenteranno delle interfacce attive e altre inattive; queste ultime da utilizzare come backup nel caso in cui il path principale presenti dei malfunzionamenti.
- **Root** : Nodo della rete che, nell'ambito dell'STP, ha priorità maggiore (Bridge ID più basso), si tratta quindi del device a partire dal quale viene costruito l'albero di attraversamento della topologia. Tutte le sue porte hanno ruolo designated e sono in stato di forwarding.
- **Link Aggregation** : Si tratta di una tecnica per accomunare più interfacce fisiche sotto un'unica interfaccia logica; permette di aumentare la banda massima del canale e di avere una maggiore robustezza del link.
- **DHCP** : Dynamic Host Configuration Protocol, si tratta di un protocollo che consente di assegnare automaticamente indirizzi IP agli endpoint di una rete. Viene configurato su di un server il quale, su richiesta, andrà a selezionare un ip da un pool definito dall'amministratore di rete, e lo assegnerà al device che lo ha richiesto.
- **PPPoE** : Il Point-to-Point Protocol (PPP) nasce come protocollo per permettere la comunicazione punto-punto su mezzi seriali. Supporta svariati protocolli di livello 3 e permette anche l'utilizzo di meccanismi di autenticazione quali il PAP e il CHAP. Sono questi i benefici che hanno fatto sopravvivere il PPP all'avvento delle connessioni Ethernet. Il PPPoE non è altro che l'adattamento del PPP ai link Ethernet.
- **NAT** : Il Network Address Translation, permette ai dispositivi di una LAN di comunicare con l'esterno, mappando gli indirizzi privati su IP pubblici.

2.5 Prime osservazioni

Ad un primo sguardo mi sono accorto di come questa topologia potesse essere suddivisa in tre regioni principali.

La prima parte è identificata dalla LAN al di sotto di AR1, la seconda è la catena di router AR1-AR2-AR3 e la terza parte è rappresentata dalla LAN collegata ad AR3.

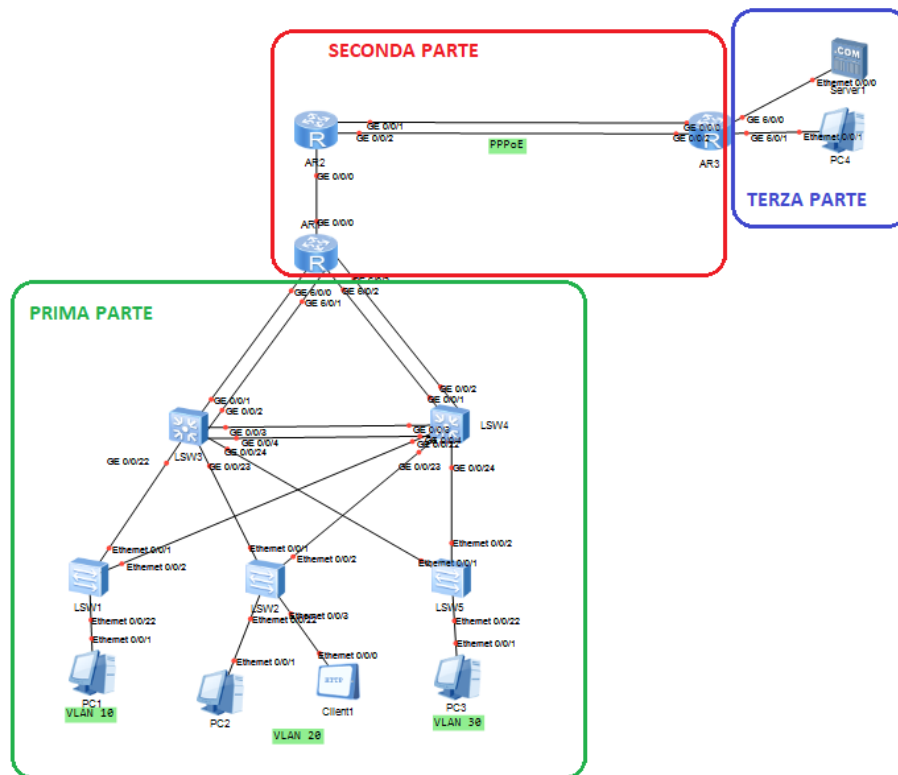


Figura 2.2: Divisione logica della topologia.

Dalla prima specifica (riguardante STP) è possibile già intuire come sarà diretto il traffico da AR1. Di fatto LSW4 e LSW3 saranno due Switch ridondanti; ovvero uno dei due servirà da backup nel caso l'altro dovesse avere qualche problema. Le specifiche precisano che dovrà essere LSW3 lo switch di default, e le stesse ci dicono che nella parte di rete sotto AR1 dovranno essere presenti tre domini di broadcast, rappresentati dalle tre VLAN 10, 20 e 30; queste ultime dovranno essere in grado di comunicare tra loro grazie alla configurazione che andrò a fare su AR1. La specifica che impedisce alle VLAN 10 e 30 di accedere ad internet e alla 20 di trasmettere traffico dalla porta 80, renderà necessario configurare il NAT su AR1 in modo particolare. Maggiore attenzione sarà richiesta anche dalla gestione del link fra AR2 e AR3; infatti questo dovrà essere un link capace di resistere ad un malfunzionamento della connessione Ethernet principale, in presenza del quale, dovrà subentrare la connessione secondaria basata su una Session PPPoE. Infine, in ottica più pratica, c'è da dire che in quanto tutte le connessioni fra i dispositivi sono state realizzate usando link Ethernet, la distanza coperta da questi ultimi non dovrà mai superare un massimo di circa 100 metri.

Capitolo 3

Configurazione

3.1 Scomposizione del progetto

Come detto durante la descrizione della topologia, la rete di partenza poteva essere divisa in tre macro aree. Di conseguenza è stato abbastanza naturale procedere con la configurazione di un'area per volta. Nello specifico, la prima zona di cui mi sono occupato è stata la LAN collegata ad AR1. La configurazione di questa parte della topologia richiedeva soprattutto una buona conoscenza dei protocolli di livello 2 della pila ISO/OSI.

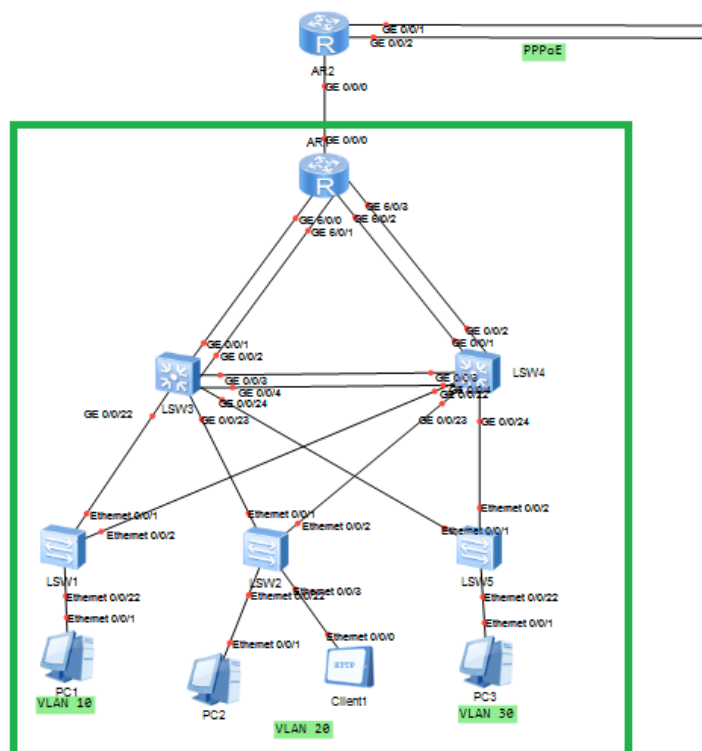


Figura 3.1: Prima sezione

Capitolo 3 Configurazione

Sistemata questa prima LAN e verificato che tutto al suo interno funzionasse, sono passato alla configurazione dei tre router presenti nella topologia.

In quest'area il procedimento che ha richiesto più tempo è stato sicuramente il settaggio del link a prova di guasto presente tra AR2 e AR3.

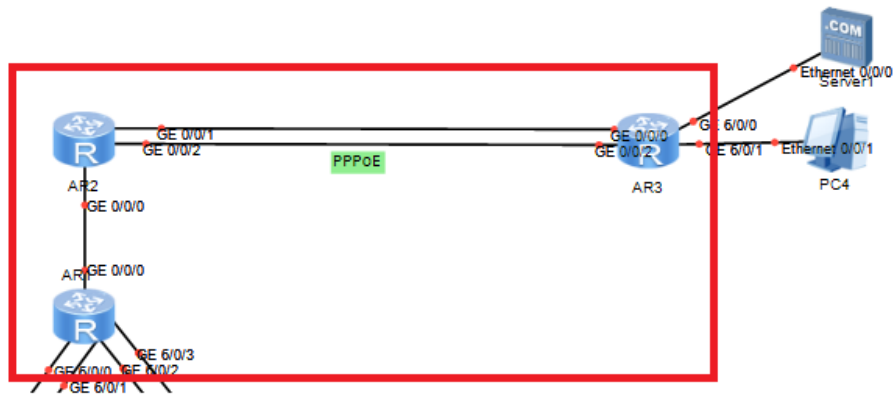


Figura 3.2: Seconda sezione

L'ultima area di cui mi sono occupato è stata quella relativa alla LAN facente capo a AR3; essendo composta da soli due endpoint la sua è stata la configurazione che in assoluto ha richiesto meno tempo.

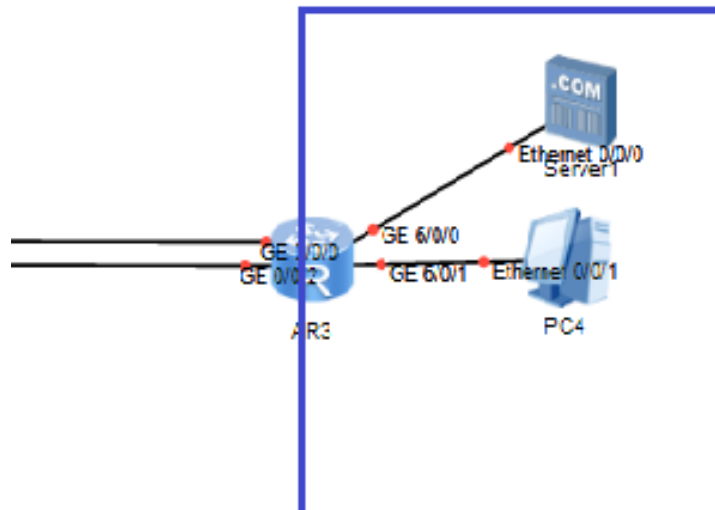


Figura 3.3: Terza sezione

3.2 Sezione 1

3.2.1 Link Aggregation

La prima cosa che ho fatto è stato configurare le interfacce logiche, dette **Ethernet Trunk**, per il link aggregation.

Essendo i link fra AR1 e i due Switch sottostanti le "arterie" principali di questa LAN, è giustificato l'utilizzo di più collegamenti fisici da aggregare, in quanto, questi saranno i tratti di rete potenzialmente attraversati dal maggior traffico. Come già accennato nei richiami teorici l'aggregazione in interfacce logiche viene fatta per garantire una larghezza di banda maggiore. Quindi, una volta entrato nelle system view dei dispositivi, ho creato le interfacce logiche utilizzando il comando *interface Eth-Trunk <n° trunk>*.

Fatto questo ho legato le interfacce fisiche ai corrispondenti Trunk usando il comando *trunkport <interfaccia>*.

```
<LSW3>system-view
Enter system view, return user view with Ctrl+Z.
[LSW3]interface Eth-Trunk 1
[LSW3-Eth-Trunk1]trunkport GigabitEthernet 0/0/4
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Figura 3.4: Aggiunta di un interfaccia ad un Trunk di LSW3

Nel far questo è importante ricordare che le interfacce fisiche da aggregare devono avere caratteristiche e proprietà uniformi. Ad esempio non è possibile unire una porta Ethernet con una GigabitEthernet.

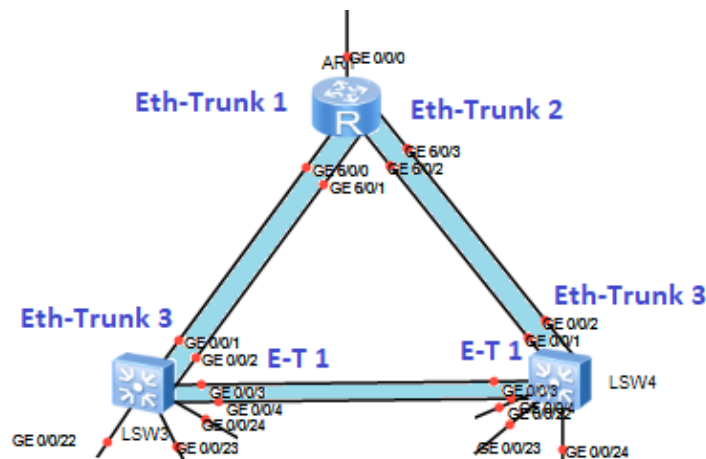


Figura 3.5: Illustrazione degli Ethernet-Trunk realizzati

3.2.2 STP

Come scritto nelle specifiche, usando STP dovevo essere in grado di rendere LSW3 il root primario e LSW4 il secondario. Ciò vuol dire che, fra i due, sarà lo Switch 3 a trasmettere i pacchetti ai nodi sotto di lui; Lo Switch 4 servirà solo da backup nel caso in cui LSW3 dovesse presentare un malfunzionamento.

Per far assumere questo comportamento alla topologia è bastato andare ad agire sul bridge ID degli Switch.

Questo può essere fatto in due modi:

- Usando il comando `stp root <primary / secondary>`.
- Andando ad agire sulla priorità dei dispositivi (il MAC-Address ovviamente non possiamo cambiarlo) usando il comando `stp priority <0-61440>`.

In questo caso è stato usato il primo comando.

```
<LSW3>dis stp bri
MSTID  Port                Role  STP State  Protection
0      GigabitEthernet0/0/3  DESI  FORWARDING  NONE
0      GigabitEthernet0/0/22 DESI  FORWARDING  NONE
0      GigabitEthernet0/0/23 DESI  FORWARDING  NONE
0      GigabitEthernet0/0/24 DESI  FORWARDING  NONE
0      Eth-Trunk1          DESI  FORWARDING  NONE
0      Eth-Trunk3          ROOT  FORWARDING  NONE
<LSW3>
```

Figura 3.6: Stato porte Switch 3

```
<LSW4>dis stp bri
MSTID  Port                Role  STP State  Protection
0      GigabitEthernet0/0/22 DESI  FORWARDING  NONE
0      GigabitEthernet0/0/23 DESI  FORWARDING  NONE
0      GigabitEthernet0/0/24 DESI  FORWARDING  NONE
0      Eth-Trunk1          ALTE  DISCARDING  NONE
0      Eth-Trunk3          ROOT  FORWARDING  NONE
<LSW4>
```

Figura 3.7: Stato porte Switch 4

Come è possibile osservare nelle due immagini 3.6 e 3.7, LSW3 ha tutte le porte in stato di Designated (Ad eccezione di quella verso AR1), ciò vuol dire che sarà lui, di default, a occuparsi del forwarding del traffico.

Nello stato di LSW4 invece si vede come l'interfaccia Eth-Trunk1 sia in stato Alternate; questo vuol dire che quell'interfaccia sarà utilizzata come backup.

E' anche interessante osservare come modificando la priorità di LSW3 e LSW4 sia variato anche lo stato delle porte degli Switch inferiori (LSW1, LSW2, LSW5).

```
<LSW1>dis stp bri
MSTID  Port                Role  STP State  Protection
  0    Ethernet0/0/1      ROOT  FORWARDING NONE
  0    Ethernet0/0/2      ALTE  DISCARDING NONE
  0    Ethernet0/0/22     DESI  FORWARDING NONE
<LSW1>
```

Figura 3.8: Stato porte Switch 1

```
<LSW2>dis stp bri
MSTID  Port                Role  STP State  Protection
  0    Ethernet0/0/1      ROOT  FORWARDING NONE
  0    Ethernet0/0/2      ALTE  DISCARDING NONE
  0    Ethernet0/0/3      DESI  FORWARDING NONE
  0    Ethernet0/0/22     DESI  FORWARDING NONE
<LSW2>
```

Figura 3.9: Stato porte Switch 2

```
<LSW5>dis stp bri
MSTID  Port                Role  STP State  Protection
  0    Ethernet0/0/1      ROOT  FORWARDING NONE
  0    Ethernet0/0/2      ALTE  DISCARDING NONE
  0    Ethernet0/0/22     DESI  FORWARDING NONE
<LSW5>
```

Figura 3.10: Stato porte Switch 5

Come vediamo, su tutti e tre gli Switch, le porte che collegano a LSW4 sono in stato di Alternate. Questa è un'ulteriore conferma del fatto che lo Switch 4 sarà utilizzato come backup in caso di guasto.

3.2.3 VLAN

Subito dopo la configurazione di STP mi sono occupato della gestione delle VLAN 10 20 e 30. Dalle specifiche sapevo che sarebbe stato il Router 1 a doversi occupare dell'instradamento dei pacchetti fra queste ultime.

Prima di pensare ad AR1 però, mi sono occupato di configurare correttamente tutti i link della LAN. Come sappiamo dalla teoria del networking, per riconoscere a quale VLAN un pacchetto è indirizzato viene utilizzato un tag che indica l'ID della Vlan in questione. Questo tag è gestito dalle interfacce stesse della rete. Nel mio caso ho scelto di utilizzare delle porte di tipo **Hybrid tagged** e **Access**.

- **Access** : Permettono di specificare un Port-Vlan ID (P-Vid); Accettano frame taggati solo se il loro Vlan-ID coincide col P-Vid; questi ultimi prima di essere trasmessi vengono privati del tag. Quando ricevono un frame non taggato, aggiungono il tag contenente il loro PVID.
Questo tipo di porte viene utilizzato per collegare gli endpoint agli Switch.
- **Hybrid tagged** : Permettono di specificare una serie di Vlan-ID consentiti. Accettano e ritrasmettono frame taggati a patto che il loro Vlan-ID sia fra gli ID permessi.
Questo tipo di porte è utilizzato per realizzare i collegamenti tra i vari Switch.

Per specificare queste caratteristiche delle porte ho utilizzato i comandi

- *port link-type hybrid*
- *port hybrid tagged vlan <pvid permessi>*
- *port link-type access*
- *port default vlan <pvid>*

```
[LSW2-Ethernet0/0/22]port link-type access
[LSW2-Ethernet0/0/22]port default vlan 20
```

Figura 3.11: Configurazione interfaccia access

```
[LSW2-GigabitEthernet0/0/2]port link-type hybrid
[LSW2-GigabitEthernet0/0/2]port hybrid tagged vlan 10 20 30
```

Figura 3.12: Configurazione interfaccia hybrid-tagged

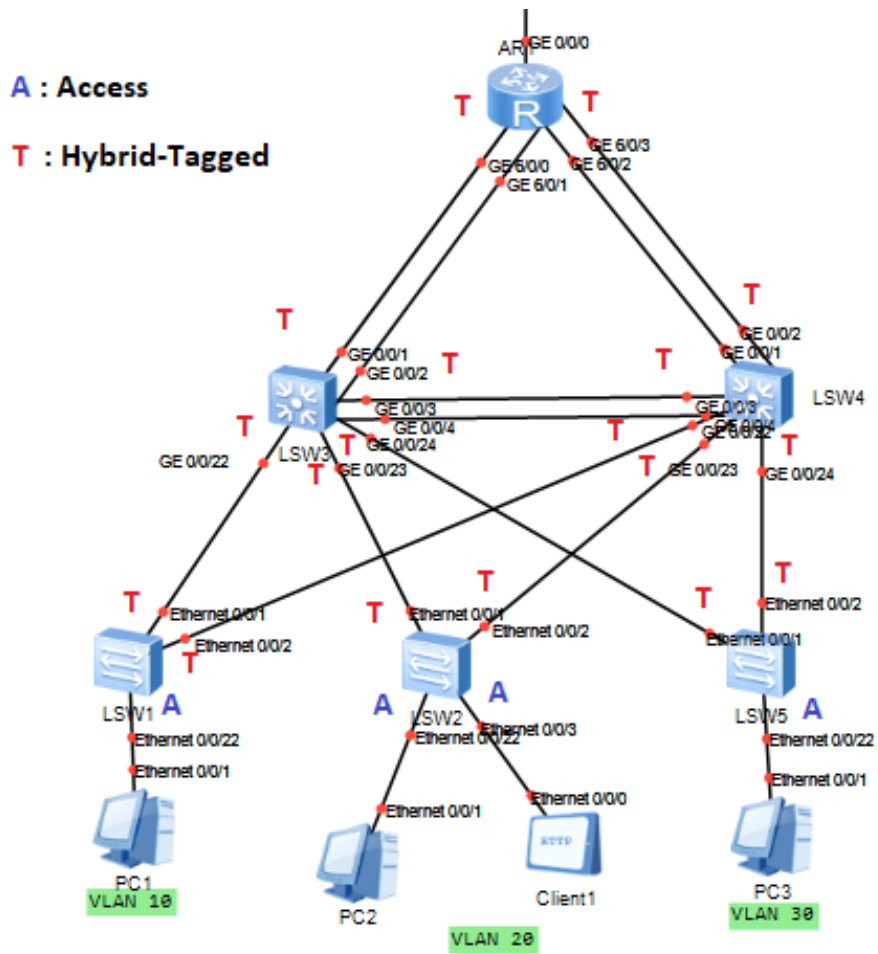


Figura 3.13: Schema delle porte

3.2.4 DHCP e Inter Vlan Routing

Il protocollo **DHCP** viene utilizzato per assegnare indirizzi ip agli host di una rete. Da specifiche sapevo che il Server il quale sarebbe andato a svolgere questo compito si sarebbe dovuto trovare sul Router 1. AR1 è collegato alla rete sottostante tramite interfacce di livello due; per questo ho dovuto trovare un modo di creare delle interfacce di livello tre che avrebbero svolto la funzione di gateway per i PC nelle varie vlan. Queste interfacce vengono dette **Vlan interfaces**, e ognuna di loro fa riferimento ad una particolare vlan. Su queste porte logiche può essere configurato un indirizzo ip e fanno capo a tutte le interfacce fisiche legate alla vlan in questione. Il comando per dichiarare queste porte è *interface Vlanif <Vlan ID>*, mentre usando *ip address <IP + Subnet MAsk>* è possibile assegnare un ip.

```
[AR1]interface vlanif 10
[AR1-Vlanif10]ip address 192.168.10.254 24
```

Figura 3.14: Dichiarazione e assegnazione ip della vlan interface 10

Lo step successivo è stato quello della creazione dei **ip pool** dai quali il dhcp sarebbe poi andato a selezionare gli indirizzi da assegnare.

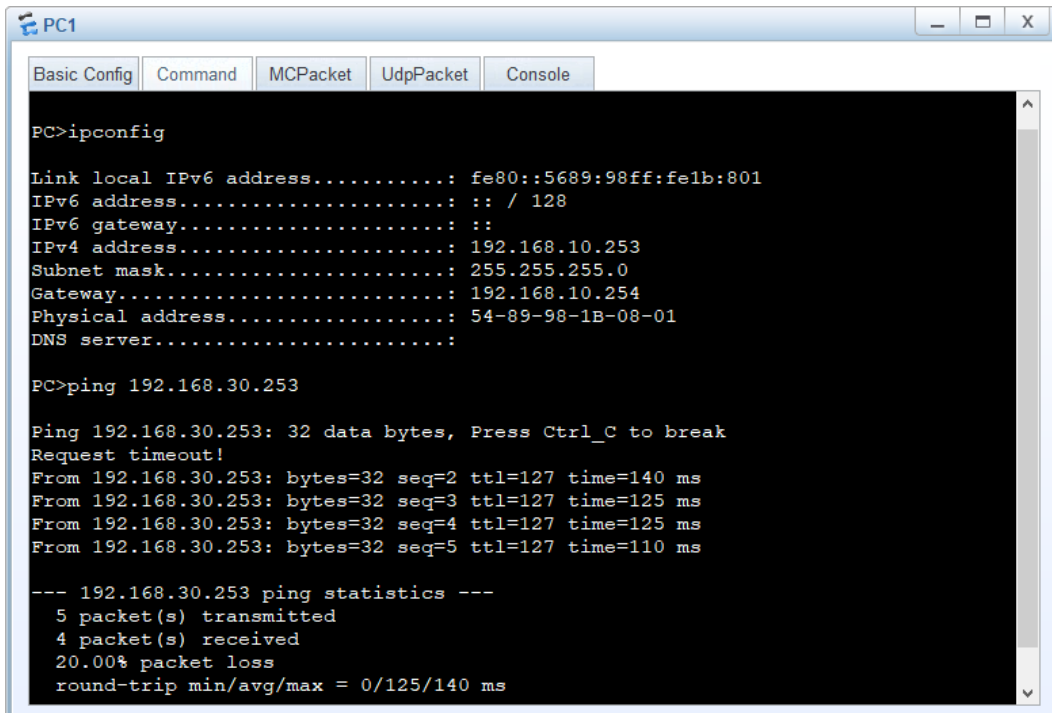
Ho scelto di creare tre pool di indirizzi, uno per ogni vlan. Gli indirizzi 192.168.10.254, 192.168.20.254 e 192.168.30.254 sono stati utilizzati come ip di gateway rispettivamente per le vlan 10, 20 e 30. Abilitate le funzioni di dhcp server su AR1 usando il comando *dhcp enable*, e legate le vlan interface ai rispettivi pool col comando *dhcp select global*, il server dhcp è completamente funzionante.

```
ip pool PoolVlan10
 gateway-list 192.168.10.254
 network 192.168.10.0 mask 255.255.255.0
 lease day 0 hour 12 minute 0
#
ip pool PoolVlan20
 gateway-list 192.168.20.254
 network 192.168.20.0 mask 255.255.255.0
 lease day 0 hour 12 minute 0
#
ip pool PoolVlan30
 gateway-list 192.168.30.254
 network 192.168.30.0 mask 255.255.255.0
 lease day 0 hour 12 minute 0
#
```

Figura 3.15: Pool di indirizzi per le tre vlan.

Per quanto riguarda l'**inter vlan routing** non sono state necessarie ulteriori operazioni , in quanto il router è in grado nativamente di instradare pacchetti tra gli spazi di indirizzi relativi alle interfacce direttamente connesse.

Una volta accesi i pc, essi ricevevano automaticamente un indirizzo ip dal Router 1 e di conseguenza gli era possibile comunicare con i terminali presenti nelle altre VLAN.



```
PC1
Basic Config Command MCPacket UdpPacket Console
PC>ipconfig
Link local IPv6 address.....: fe80::5689:98ff:fe1b:801
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.10.253
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.10.254
Physical address.....: 54-89-98-1B-08-01
DNS server.....:

PC>ping 192.168.30.253

Ping 192.168.30.253: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.30.253: bytes=32 seq=2 ttl=127 time=140 ms
From 192.168.30.253: bytes=32 seq=3 ttl=127 time=125 ms
From 192.168.30.253: bytes=32 seq=4 ttl=127 time=125 ms
From 192.168.30.253: bytes=32 seq=5 ttl=127 time=110 ms

--- 192.168.30.253 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/125/140 ms
```

Figura 3.16: PC1: Ip ricevuto dal dhcp e ping verso PC3 nella vlan 30

3.3 Sezione 2

Passiamo ora a illustrare la configurazione presente sui Router AR1, AR2 e AR3. Come è possibile immaginare in quest'area della topologia sono state trattate problematiche riconducibili a livelli più alti della pila ISO/OSI (principalmente livello 3).

3.3.1 ACL

Le access-control-list, ACL, possono essere definite come delle liste ordinate di regole le quali vanno a stabilire dei criteri di accesso alle risorse di una rete; ciascuna regola esprime delle condizioni o proprietà dell'oggetto da valutare, e se queste proprietà sono verificate indica quale decisione prendere. Nel mio caso, come è possibile intuire dalle specifiche, sono state utilizzate per gestire il traffico diretto da AR1; in particolare abbiamo dovuto :

- Permettere l'accesso alla rete esterna solo agli endpoint della VLAN 20.
- Non permettere il passaggio di pacchetti provenienti dalla porta numero 80.

Per far questo mi sono avvalso di una particolare tipologia di ACL, dette ACL advanced, caratterizzate da un id compreso nel range 3000-3999. Queste access-control-list permettono di filtrare o selezionare il traffico, sulla base di un grande numero di parametri che possono essere anche specifici per un particolare protocollo. La sintassi per la dichiarazione di queste regole risulta assai complessa se comparata a quella delle ACL Basic ($id \in [2000, 2999]$).

Di seguito viene riportata quella utilizzata nel progetto per soddisfare le due specifiche riportate precedentemente.

```
acl number 3000
 rule 5 deny tcp source-port eq www
 rule 10 permit ip source 192.168.20.0 0.0.0.255
 rule 15 deny ip source 192.168.10.0 0.0.0.255
 rule 20 deny ip source 192.168.30.0 0.0.0.255
 #
```

Figura 3.17: ACL usata per il filtraggio in uscita da AR1

Come si può notare viene permesso il traffico proveniente dalla VLAN 20 (IP di rete 192.168.20.0 / 24) e negato quello inviato dalle VLAN 10 e 30; viene anche negato il traffico in uscita sulla porta 80 (nell'immagine indicata come www).

Nella sezione a seguire descriverò la soluzione adottata per applicare questa ACL al Router 1.

3.3.2 NAT su AR1 e AR3

Il Network Address Translation, NAT, è una tecnica finalizzata alla traduzione degli IP presenti in una rete privata. Il dispositivo che andrà a svolgere queste operazioni dovrà essere un device di livello 3, nel mio caso un Router. La tipologia di nat utilizzata su AR1 è detta **NAT dinamico**; quest'ultimo al momento dell'instradamento dei pacchetti, va ad associare ogni IP della LAN a un indirizzo pubblico preso da un pool di IP.

L'insieme di indirizzi IP da cui il nat va a pescare, dovrebbe sempre essere dimensionato in proporzione alla mole di utenza che pensiamo potrebbe voler accedere alla rete nelle ore di punta. Nel mio caso i PC della LAN che potevano accedere ad Internet erano solo due, tuttavia, prevedendo un possibile aumento nel numero di elaboratori, ho deciso di dare al pool un range di indirizzi che va dal 192.168.100.11 al 192.168.100.21.

```
#
nat address-group 1 192.168.100.11 192.168.100.21
#
```

Figura 3.18: Address group legato al NAT su AR1

Definito il pool di indirizzi, sono passato a configurare il NAT vero e proprio; Nel far ciò ho anche legato la ACL precedentemente dichiarata al NAT, così da effettuare il filtraggio prima nella traduzione dell'indirizzo.

```
#
interface GigabitEthernet0/0/0
 ip address 192.168.100.1 255.255.255.0
 nat outbound 3000 address-group 1 no-pat
#
```

Figura 3.19: Configurazione dell'interfaccia GigabitEthernet0/0/0 di AR1

Nella configurazione dell'interfaccia pubblica del Router 1 è possibile osservare come è stato settato il NAT e l'indirizzo IP assegnato.

Si vede che è stata applicata la ACL 3000 dichiarata in precedenza e che l'address-group 1 è stato passato come pool di indirizzi. Infine il parametro no-pat indica che ogni endpoint sarà mappato su un unico indirizzo preso dal pool, senza ricorrere alla mappatura sulle porte (NAPT).

Fatto tutto questo, i pacchetti (Solo dalla Vlan 20 e da porte diverse dalla 80) in uscita da Router 1 saranno mappati sugli indirizzi dell'address-group 1. In questa sezione della topologia il NAT è stato utilizzato anche in un altro caso, ovvero su AR3, dove è servito per mappare gli indirizzi della LAN a destra del Router 3.

Capitolo 3 Configurazione

La configurazione data a questo NAT presenta caratteristiche del tutto diverse da quelle date al NAT su AR1. Qui il NAT doveva essere realizzato in modo da consentire l'accesso continuativo al Server 1 e il ping al PC4.

Per far questo mi sono avvalso di una particolare tipologia di NAT detto **NAT statico**; a differenza del dinamico non presenta un pool di indirizzi su cui mappare gli IP locali, ma si limita ad associare ad ogni indirizzo interno un IP globale fisso. Questo NAT viene utilizzato quando la rete presenta dei servizi che devono sempre essere accessibili dall'esterno per mezzo di un indirizzo costante.

Per quanto riguarda il Server 1 sono stati configurati tre indirizzi pubblici differenti 192.168.200.100/101/102 rispettivamente per i protocolli **HTTP, ICMP e FTP**. L'utilizzo di tre ip separati consente di avere una maggiore flessibilità di configurazione, ad esempio si potrebbero impostare acl diverse per ogni protocollo; oltre a questo se in futuro dovesse essere necessario scalare i server per rispondere a pattern di traffico maggiori, questa soluzione agevolerebbe notevolmente le procedure. E' stato anche configurato un indirizzo apposito per la mappatura del PC4, il quale sarà raggiungibile (tramite ICMP) all'IP 192.168.200.103.

Oltre al NAT Statico, su AR3 è stato anche applicato **Easy IP**, in visione di altri endpoint che potrebbero entrare a far parte della topologia in futuro. Easy IP rappresenta un'ulteriore tipologia di NAT a disposizione e si basa sul mappare gli indirizzi interni della LAN su un unico indirizzo globale, questa volta su porte diverse, in modo da distinguere i vari host. L'indirizzo globale utilizzato coincide con l'indirizzo dell'interfaccia pubblica del router.

L'intera configurazione del NAT descritta (Statico + Easy IP) è stata applicata alle interfacce GigabitEthernet0/0/2 e Dialer 1; su quest'ultima interfaccia si tornerà più avanti quando si tratterà del link fra AR2-AR3 e del PPPoE.

```
nat static protocol icmp global 192.168.200.101 inside 192.168.40.128 netmask 255.255.255.255
nat static protocol tcp global 192.168.200.100 www inside 192.168.40.128 www netmask 255.255.255.255
nat static protocol tcp global 192.168.200.102 ftp inside 192.168.40.128 ftp netmask 255.255.255.255
nat static protocol icmp global 192.168.200.103 inside 192.168.40.253 netmask 255.255.255.255
nat outbound 2000
```

Figura 3.20: Configurazione del NAT sulle interfacce Gig0/0/0 e Dialer 1 di AR3

Il comando *nat outbound 2000* è il comando utilizzato per configurare Easy IP; il numero 2000 si riferisce all'ID di una ACL Basic utilizzata solo per specificare che ai nodi della LAN a destra di AR3 è permesso accedere alla rete esterna.

3.3.3 Rotte statiche e Link AR2-AR3

La gestione delle rotte di instradamento dei tre router è stata fatta tramite l'uso di **rotte statiche**, dichiarate usando il comando `ip static-route <IP-Rete destinataria> <netmask> <IP/Interfaccia>`. Ad esempio nel router AR1 è stata dichiarata la rotta verso la rete 192.168.200.0 / 24 la quale contiene tutti gli ip pubblici corrispondenti ai nodi della LAN legata a AR3.

Questa rotta indica che per raggiungere tale rete si devono instradare i pacchetti sull'interfaccia GigabitEthernet0/0/0 di AR2 avente come IP 192.168.100.2.

```
ip route-static 192.168.200.0 255.255.255.0 192.168.100.2
```

Figura 3.21: Rotta statica verso 192.168.200.0 /24 su AR1

Allo stesso modo su AR2 è stata definita una rotta per instradare i pacchetti con Destination IP Address appartenente allo spazio 192.168.100.0 /24.

Di maggiore interesse su AR2 però è la configurazione fatta per quanto riguarda il collegamento verso AR3. Questo link infatti, si legge da specifiche, deve essere in grado di passare ad una comunicazione PPPoE nel caso in cui si presentasse un'interruzione sul link Ethernet principale. Per far questo ho deciso di creare due rotte di instradamento sia su AR2 che su AR3 con una preference differente. Sapendo che minore è la preference e maggiore è la priorità del canale, ho assegnato al link Ethernet una preference pari a 1 e al link PPPoE una pari a 255. Così facendo, in una situazione di normale funzionamento il traffico sarà trasmesso sul link Ethernet; il collegamento PPPoE sarà utilizzato come mezzo di comunicazione solo nel caso in cui il link Ethernet non dovessero essere più disponibile.

```
ip route-static 192.168.100.0 255.255.255.0 192.168.100.1
ip route-static 192.168.200.0 255.255.255.0 192.168.200.2 preference 1
ip route-static 192.168.200.0 255.255.255.0 192.168.250.254 preference 255
```

Figura 3.22: Rotte statiche su AR2

3.3.4 PPPoE Client e Server su AR2 e AR3

Per configurare un link PPP over Ethernet è necessario stabilire un client ed un server sui dispositivi agli estremi del collegamento. In questo caso il client è configurato su AR3 ed il suo compito è richiedere al server di stabilire una Session PPPoE in grado di supportare la comunicazione per mezzo del protocollo PPP sul mezzo Ethernet.

Il compito del server, configurato su AR2, è quello di passare al client una serie di parametri necessari a stabilire la Sessione; fra questi parametri, in primis, c'è il Session ID, ovvero un valore univoco identificatore della sessione.

Capitolo 3 Configurazione

Nel mio caso il server si occupa anche di assegnare un indirizzo IP all'interfaccia di comunicazione del client in modo da permettere l'instradamento di pacchetti IP incapsulati.

Questo indirizzo, come è possibile dedurre dalle soluzioni adottate in precedenza, è preso da un pool.

Infine, come meccanismo di autenticazione per il client PPP, è stato scelto il CHAP.

```
ip pool poolPPPoE1
network 192.168.250.0 mask 255.255.255.0
```

Figura 3.23: Pool di indirizzi per il Server PPPoE

```
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool poolPPPoE1
 ip address 192.168.250.1 255.255.255.0
#
```

Figura 3.24: Virtual Template per l'interfaccia da cui raggiungere il Server PPPoE

Il Virtual Template racchiude i parametri caratteristici del Server PPPoE, in questo caso il pool di IP e la modalità di autenticazione.

```
interface GigabitEthernet0/0/1
 pppoe-server bind Virtual-Template 1
#
```

Figura 3.25: Assegnazione del Virtual Template all'Interfaccia

Analizziamo ora la configurazione del Client PPPoE.

```
interface Dialer1
 link-protocol ppp
 ppp chap user pc4@huawei
 ppp chap password cipher $$$qTJ.0vvfBMGZ<8B\p5=T,$PT$$$
 ip address ppp-negotiate
 dialer user LAN1
 dialer bundle 1
 dialer-group 1
 nat static protocol icmp global 192.168.200.101 inside 192.168.40.128 netmask 2
 55.255.255.255
 nat static protocol tcp global 192.168.200.100 www inside 192.168.40.128 www ne
 tmask 255.255.255.255
 nat static protocol tcp global 192.168.200.102 ftp inside 192.168.40.128 ftp ne
 tmask 255.255.255.255
 nat static protocol icmp global 192.168.200.103 inside 192.168.40.253 netmask 2
 55.255.255.255
 nat outbound 2000
 #
```

Parametri PPPoE

NAT STATICO
+
EASY IP

Figura 3.26: Configurazione del Client PPPoE

Le informazioni del client sono racchiuse in un interfaccia logica chiamata Dialer 1. Questa interfaccia racchiude alcuni parametri tra cui le credenziali per l'autenticazione ed ha il compito di gestire la configurazione dell'IP e del PPP. Oltre a questo si può notare come il NAT relativo al link PPPoE sia dichiarato qui e non, come si potrebbe pensare, sull'interfaccia fisica.

Questo Dialer va poi legato alla porta fisica vera e propria, che in questo caso è la GigabitEthernet0/0/0.

```
[AR3]int GigabitEthernet 0/0/0
[AR3-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1 on-demand
```

Figura 3.27: Binding fra Dialer 1 e interfaccia fisica

3.4 Sezione 3

Questa ultima sezione, include la LAN collegata al Router 3 e, come è possibile immaginare, è stata la parte di topologia più semplice da configurare.

3.4.1 DHCP

Osservando AR3 mi sono subito accorto che le porte che lo collegano al PC4 e al Server 1 sono porte di livello due. Ciò vuol dire che, come era stato necessario per la prima LAN, si sarebbero dovute utilizzare delle Vlan interface finalizzate ad avere dei gateway DHCP.

In questo caso, a differenza di quanto fatto durante la configurazione di AR1, ho sfruttato la Vlan 1, già definita di default su tutti i router AR2220.

Sono quindi andato avanti andando a creare il pool di indirizzi, che in questo caso ho fatto coincidere con lo spazio di indirizzi 192.168.40.0 /24.

```
ip pool PoolVlan1
 gateway-list 192.168.40.254
 network 192.168.40.0 mask 255.255.255.0
 lease day 0 hour 12 minute 0
#
```

Figura 3.28: IP pool per la Vlan 1

Infine, abilitato il DHCP Server, ho assegnato alla Vlan Interface 1 l'indirizzo IP 192.168.40.254 e lo ho legato al pool globale.

```
interface Vlanif1
 ip address 192.168.40.254 255.255.255.0
 dhcp select global
#
```

Figura 3.29: Configurazione della VlanIf 1 su AR3

L'indirizzo IP di Server 1 è stato invece configurato manualmente per garantire coerenza con la mappatura statica realizzata nel NAT su AR3; al Server è stato assegnato l'indirizzo privato 192.168.40.128.

Capitolo 4

Test e note sulle prestazioni

Terminata la configurazione, ho iniziato a verificare che tutte le specifiche fossero soddisfatte.

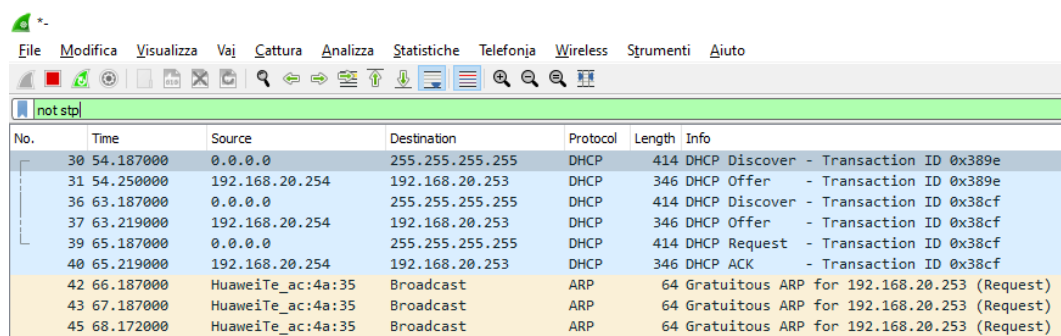
Ho iniziato svolgendo dei **test sul funzionamento di base** della rete, verificando che tutte le componenti svolgessero il loro lavoro correttamente.

In secondo luogo sono passato ad effettuare dei **test sulla robustezza** della topologia, simulando guasti a alcuni dei componenti e verificando l'operatività della rete.

4.1 Test sul funzionamento

4.1.1 DHCP su AR1 e AR3

Sono partito testando il funzionamento del DHCP su AR1. Questo è stato fatto grazie a WhireShark, andando a catturare lo scambio di messaggi fra PC2 e Server al momento dell'avviamento.



The screenshot shows a Wireshark capture of network traffic. The interface includes a menu bar (File, Modifica, Visualizza, Vaj, Cattura, Analizza, Statistiche, Telefonja, Wireless, Strumenti, Aiuto) and a toolbar. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
30	54.187000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Discover - Transaction ID 0x389e
31	54.250000	192.168.20.254	192.168.20.253	DHCP	346	DHCP Offer - Transaction ID 0x389e
36	63.187000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Discover - Transaction ID 0x38cf
37	63.219000	192.168.20.254	192.168.20.253	DHCP	346	DHCP Offer - Transaction ID 0x38cf
39	65.187000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request - Transaction ID 0x38cf
40	65.219000	192.168.20.254	192.168.20.253	DHCP	346	DHCP ACK - Transaction ID 0x38cf
42	66.187000	HuaweiTe_ac:4a:35	Broadcast	ARP	64	Gratuitous ARP for 192.168.20.253 (Request)
43	67.187000	HuaweiTe_ac:4a:35	Broadcast	ARP	64	Gratuitous ARP for 192.168.20.253 (Request)
45	68.172000	HuaweiTe_ac:4a:35	Broadcast	ARP	64	Gratuitous ARP for 192.168.20.253 (Request)

Figura 4.1: Negoziazione indirizzo IP col Server da parte di PC2.

```
Link local IPv6 address.....: fe80::5689:98ff:feac:4a35
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.20.253
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.20.254
Physical address.....: 54-89-98-AC-4A-35
DNS server.....:
```

Figura 4.2: Default GW e IP forniti dal DHCP a PC2.

Il DHCP Server configurato su AR3 è stato testato allo stesso modo. Accendendo PC4 e eseguendo il data-capture sul link che lo collega al router, è stato possibile constatare il corretto funzionamento del Server.

```
Link local IPv6 address.....: fe80::5689:98ff:fe29:44ff
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.40.253
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.40.254
Physical address.....: 54-89-98-29-44-FF
DNS server.....:
```

Figura 4.3: Acquisizione IP di PC4.

20	27.765000	0.0.0.0	255.255.255.255	DHCP	410 DHCP Discover	- Transaction ID 0x217f
23	31.765000	0.0.0.0	255.255.255.255	DHCP	410 DHCP Discover	- Transaction ID 0x217f
24	31.765000	192.168.40.254	192.168.40.253	DHCP	342 DHCP Offer	- Transaction ID 0x217f
30	40.765000	0.0.0.0	255.255.255.255	DHCP	410 DHCP Discover	- Transaction ID 0x21b0
31	40.765000	192.168.40.254	192.168.40.253	DHCP	342 DHCP Offer	- Transaction ID 0x21b0
33	42.765000	0.0.0.0	255.255.255.255	DHCP	410 DHCP Request	- Transaction ID 0x21b0
34	42.765000	192.168.40.254	192.168.40.253	DHCP	342 DHCP ACK	- Transaction ID 0x21b0
35	43.765000	HuaweiTe_29:44:ff	Broadcast	ARP	60 Gratuitous ARP for 192.168.40.253 (Request)	
37	44.750000	HuaweiTe_29:44:ff	Broadcast	ARP	60 Gratuitous ARP for 192.168.40.253 (Request)	
38	45.750000	HuaweiTe_29:44:ff	Broadcast	ARP	60 Gratuitous ARP for 192.168.40.253 (Request)	

Figura 4.4: Negoziazione dell'indirizzo col Server su AR3.

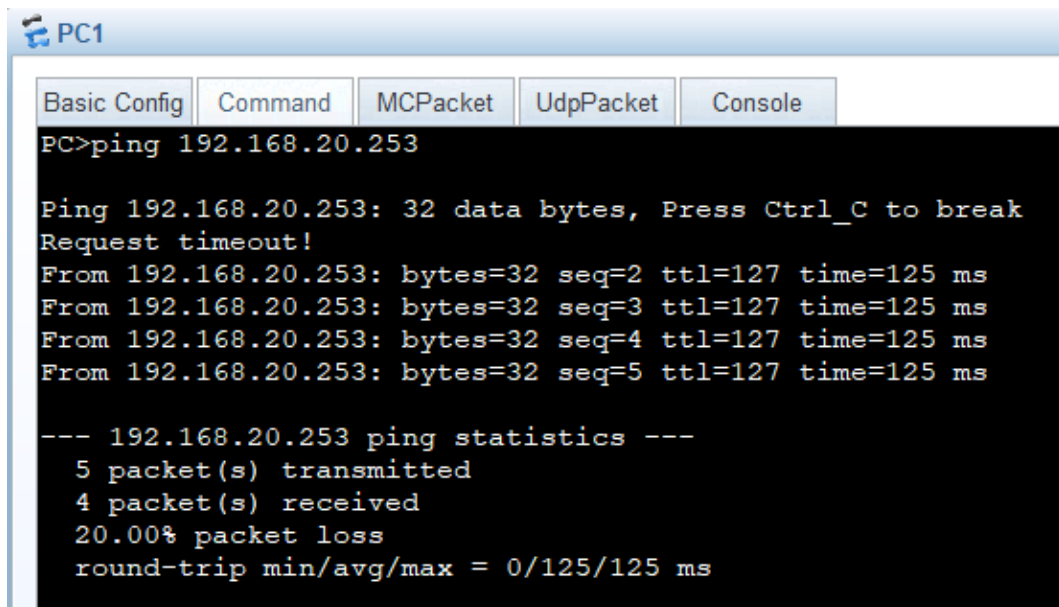
4.1.2 Inter Vlan Routing

Fatto questo sono passato a testare l'inter Vlan Routing effettuato da AR1; eseguendo dei ping fra i PC delle varie Vlan, ho visto che questi riuscivano a raggiungersi senza problemi.

Avviato il data capture in ingresso e in uscita dal router, è stato possibile verificare che i pacchetti venivano taggati e indirizzati correttamente dalle Vlan interface presenti su AR1.

Nell'immagine 4.6 è possibile notare come il tag nel frame ha come Vlan ID il valore 10, in quanto deve ancora attraversare il Router.

Al contrario nell'illustrazione 4.7 si può osservare come la stessa ping Request, in uscita dal Router, presenti come Vlan ID un valore pari a 20.



```

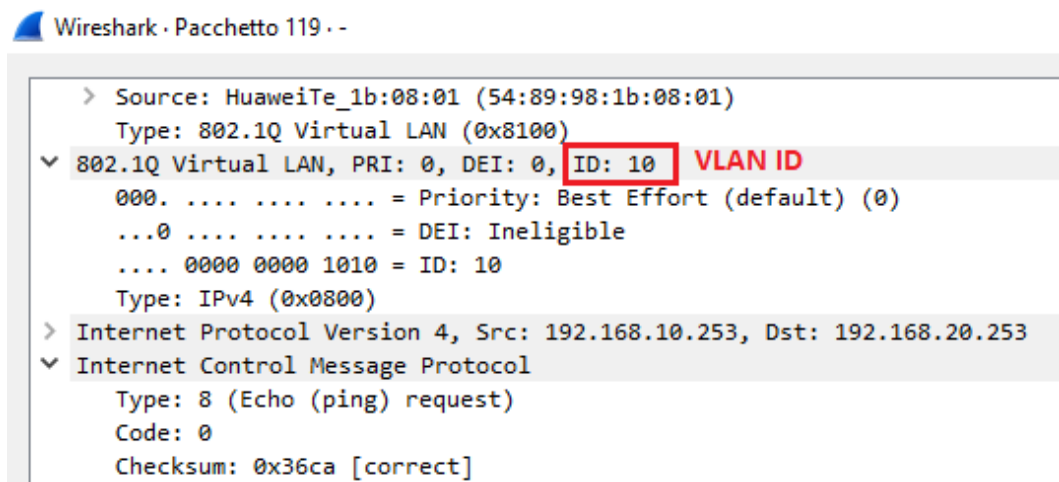
PC1
Basic Config | Command | MCPacket | UdpPacket | Console
PC>ping 192.168.20.253

Ping 192.168.20.253: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.20.253: bytes=32 seq=2 ttl=127 time=125 ms
From 192.168.20.253: bytes=32 seq=3 ttl=127 time=125 ms
From 192.168.20.253: bytes=32 seq=4 ttl=127 time=125 ms
From 192.168.20.253: bytes=32 seq=5 ttl=127 time=125 ms

--- 192.168.20.253 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/125/125 ms

```

Figura 4.5: Ping da PC1 a PC2.



```

Wireshark · Pacchetto 119 · -
  > Source: HuaweiTe_1b:08:01 (54:89:98:1b:08:01)
    Type: 802.1Q Virtual LAN (0x8100)
  ▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10 VLAN ID
    000. .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... = DEI: Ineligible
    .... 0000 0000 1010 = ID: 10
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.10.253, Dst: 192.168.20.253
  ▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x36ca [correct]

```

Figura 4.6: ICMP Request in ingresso ad AR1.

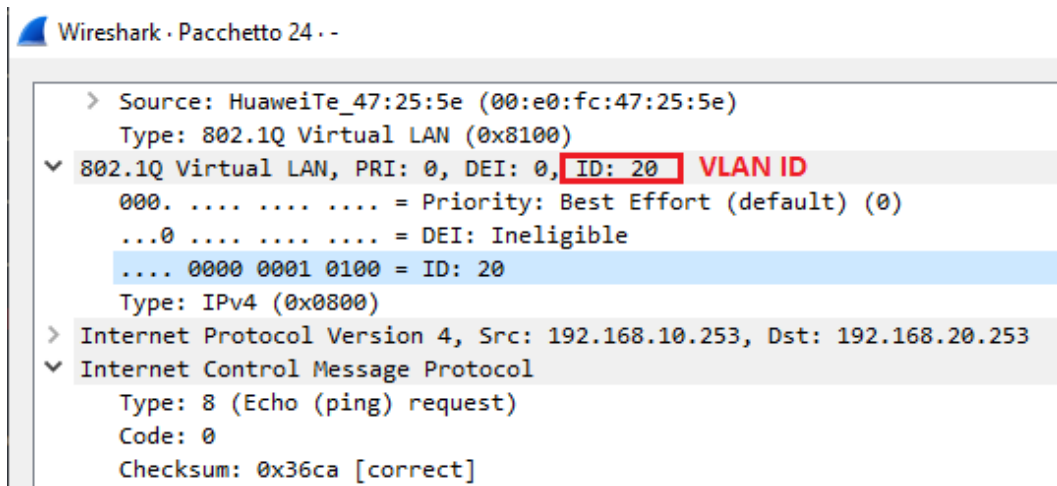


Figura 4.7: ICMP Request in uscita da AR1.

4.1.3 NAT su AR1 e AR3

Andando avanti coi test sono passato a verificare che il NAT funzionasse correttamente, sia per quanto riguarda AR1 che AR3. Per eseguire la verifica è stato sufficiente eseguire il data capture sulle interfacce pubbliche dei Router. Facendo ciò è stato possibile confermare che la traduzione degli IP avveniva correttamente.

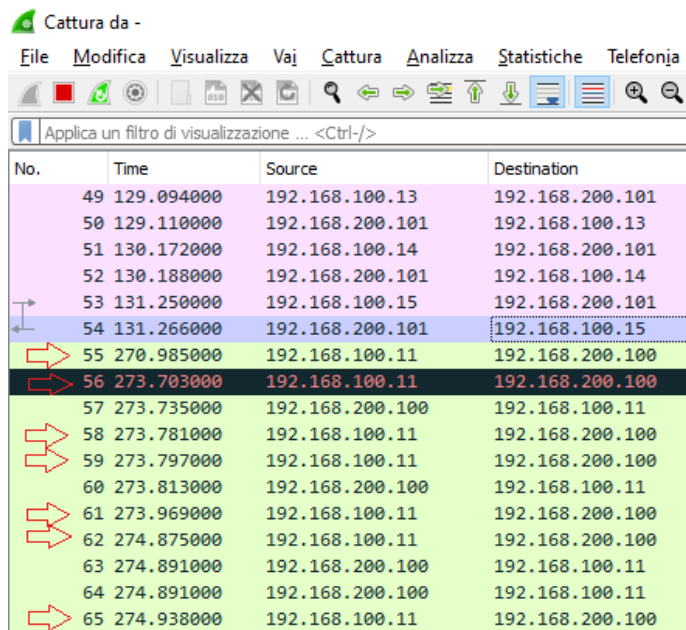
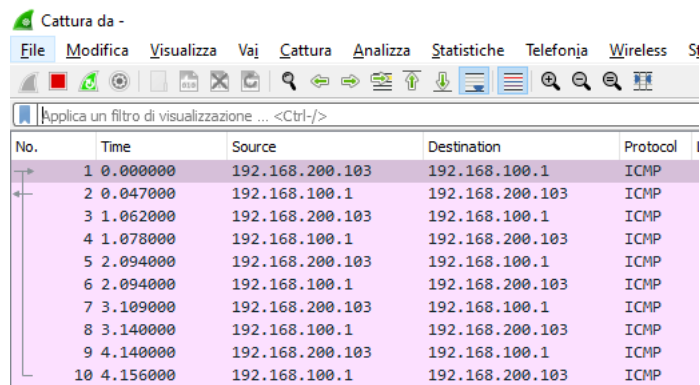


Figura 4.8: Pacchetti in uscita da AR1.

Nella figura 4.8 è possibile osservare i pacchetti in uscita da AR1 (Segnati con una freccia rossa); si vede come il Source IP sia proprio un indirizzo preso dal pool definito per il NAT sul Router 1. Lo stesso test viene fatto con entrambe le interfacce di AR3 e anche qui, come in AR1, il NAT funziona alla perfezione.

4.1 Test sul funzionamento



The screenshot shows the Wireshark interface with a capture filter set to 'Applica un filtro di visualizzazione ... <Ctrl-/>'. The packet list pane displays ten ICMP packets. The first packet is an Echo (ping) request from source 192.168.200.103 to destination 192.168.100.1. The following nine packets are Echo replies from source 192.168.100.1 to destination 192.168.200.103. The time intervals between packets are approximately 0.047s, 0.062s, 0.078s, 0.094s, 0.094s, 0.109s, 0.140s, 0.140s, and 0.156s.

No.	Time	Source	Destination	Protocol
1	0.000000	192.168.200.103	192.168.100.1	ICMP
2	0.047000	192.168.100.1	192.168.200.103	ICMP
3	1.062000	192.168.200.103	192.168.100.1	ICMP
4	1.078000	192.168.100.1	192.168.200.103	ICMP
5	2.094000	192.168.200.103	192.168.100.1	ICMP
6	2.094000	192.168.100.1	192.168.200.103	ICMP
7	3.109000	192.168.200.103	192.168.100.1	ICMP
8	3.140000	192.168.100.1	192.168.200.103	ICMP
9	4.140000	192.168.200.103	192.168.100.1	ICMP
10	4.156000	192.168.100.1	192.168.200.103	ICMP

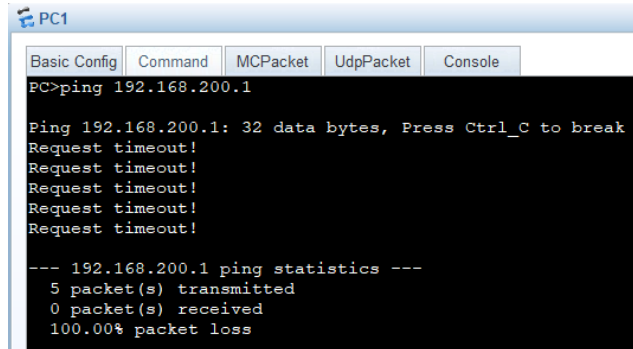
Figura 4.9: Pacchetti in uscita da AR3.

Nella figura 4.9 viene riportato un ping effettuato da PC4 verso l'interfaccia Gig0/0/0 di AR1.

4.1.4 Accesso a Internet

Un ulteriore test svolto sul Router 1 riguarda l'accessibilità ad internet da parte delle varie VLAN.

Anche in questo caso la verifica è stata abbastanza semplice, in quanto è stato sufficiente eseguire alcuni ping verso l'esterno della LAN. Come è possibile osservare solo i PC della VLAN 20 sono in grado di comunicare con l'esterno.

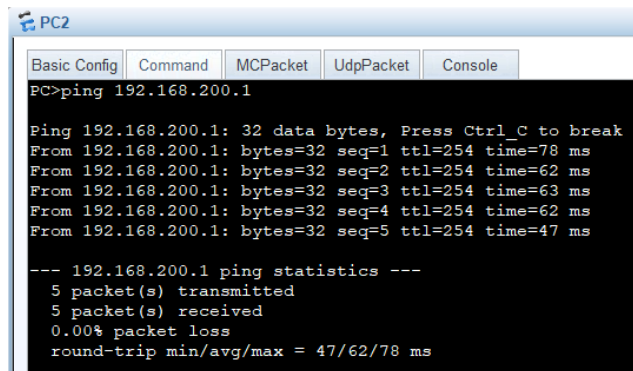


```
PC1
Basic Config | Command | MCPacket | UdpPacket | Console
PC>ping 192.168.200.1

Ping 192.168.200.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

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

Figura 4.10: Ping da PC1 verso AR2.

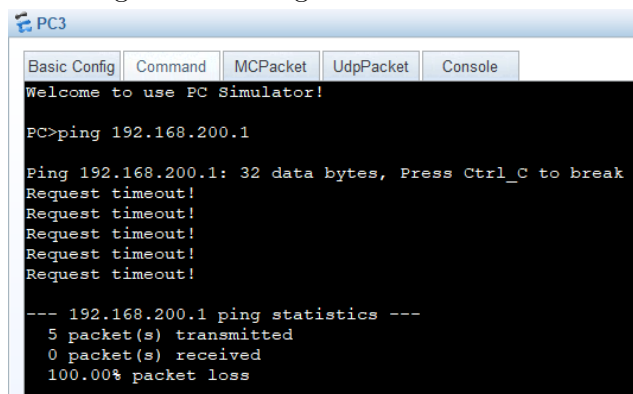


```
PC2
Basic Config | Command | MCPacket | UdpPacket | Console
PC>ping 192.168.200.1

Ping 192.168.200.1: 32 data bytes, Press Ctrl_C to break
From 192.168.200.1: bytes=32 seq=1 ttl=254 time=78 ms
From 192.168.200.1: bytes=32 seq=2 ttl=254 time=62 ms
From 192.168.200.1: bytes=32 seq=3 ttl=254 time=63 ms
From 192.168.200.1: bytes=32 seq=4 ttl=254 time=62 ms
From 192.168.200.1: bytes=32 seq=5 ttl=254 time=47 ms

--- 192.168.200.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 47/62/78 ms
```

Figura 4.11: Ping da PC2 verso AR2.



```
PC3
Basic Config | Command | MCPacket | UdpPacket | Console
Welcome to use PC Simulator!

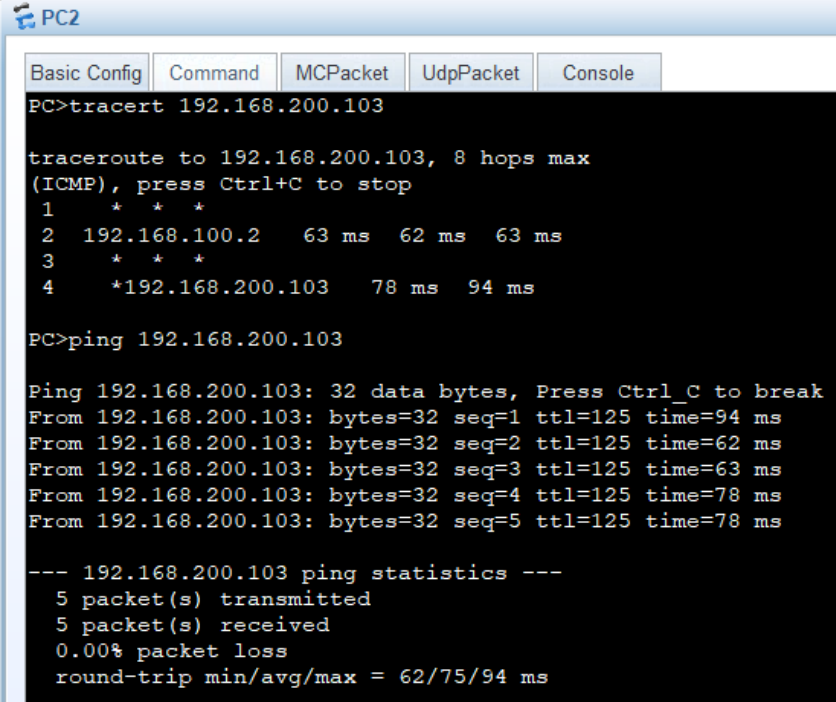
PC>ping 192.168.200.1

Ping 192.168.200.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

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

Figura 4.12: Ping da PC3 verso AR2.

L'ultima prova effettuata per quanto riguarda i test sulle funzionalità è stata la verifica della raggiungibilità di PC4 da un endpoint appartenente alla Vlan 20. Come negli altri casi è stato sufficiente effettuare un ping per verificare se il PC fosse raggiungibile o meno.



```
PC2
Basic Config Command MCPacket UdpPacket Console
PC>tracert 192.168.200.103

tracert to 192.168.200.103, 8 hops max
(ICMP), press Ctrl+C to stop
 1  * * *
 2  192.168.100.2  63 ms  62 ms  63 ms
 3  * * *
 4  *192.168.200.103  78 ms  94 ms

PC>ping 192.168.200.103

Ping 192.168.200.103: 32 data bytes, Press Ctrl_C to break
From 192.168.200.103: bytes=32 seq=1 ttl=125 time=94 ms
From 192.168.200.103: bytes=32 seq=2 ttl=125 time=62 ms
From 192.168.200.103: bytes=32 seq=3 ttl=125 time=63 ms
From 192.168.200.103: bytes=32 seq=4 ttl=125 time=78 ms
From 192.168.200.103: bytes=32 seq=5 ttl=125 time=78 ms

--- 192.168.200.103 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 62/75/94 ms
```

Figura 4.13: Ping da PC2 verso PC4.

4.2 Test di robustezza

4.2.1 Test su LSW3 e LSW4

Questi test sono stati svolti per osservare la reazione della topologia ad una serie di possibili guasti.

Per prima cosa ho simulato un **malfunzionamento sullo Switch LSW3** (Primary Switch) per testare la resistenza della rete a tale guasto. Spegnendo lo Switch è possibile osservare come l'STP adatti i collegamenti al topology-change andando a cambiare il ruolo delle porte. Ad esempio, a seguito dello shut-down di LSW3 tutte le porte degli switch sottostanti, le quali si trovavano in stato di Alternate, passano in stato di Root.

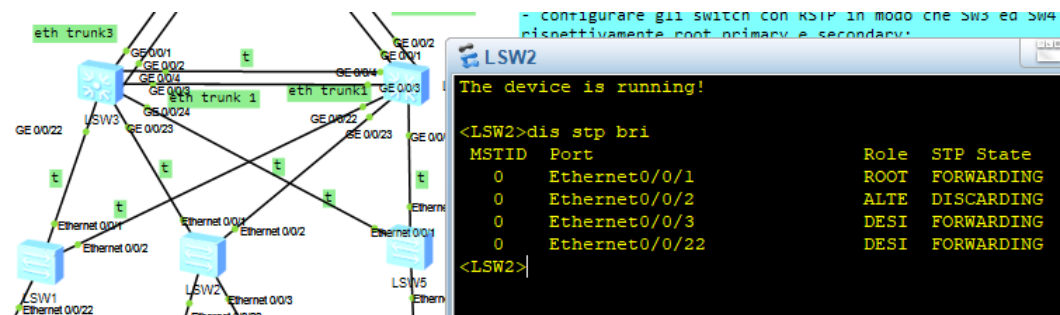


Figura 4.14: Ruolo porte LSW2 con LSW3 funzionante.

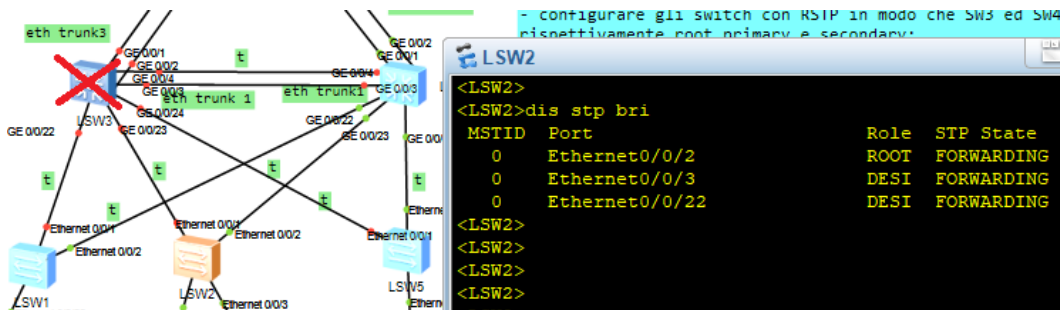


Figura 4.15: Ruolo porte LSW2 con LSW3 non funzionante.

Dopo che la topologia è tornata a convergere è stato possibile eseguire nuovamente alcuni test funzionali, per verificare l'effettivo funzionamento della rete. Eseguendo un ping da PC2 verso l'esterno della LAN, ho potuto accertarmi del fatto che i pacchetti continuavano a essere trasmessi attraverso lo Switch 4, e quindi che la topologia aveva resistito con successo al guasto.

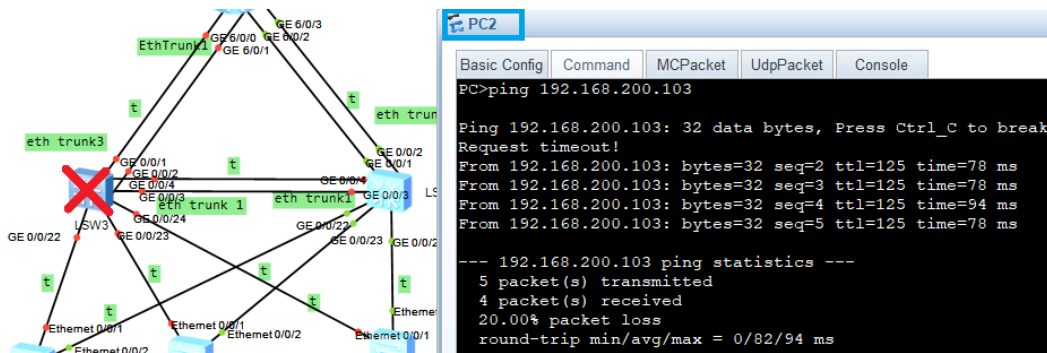


Figura 4.16: Ping da PC2 verso l'esterno con LSW3 fuori servizio.

4.2.2 Test sul link AR2-AR3

Come già descritto nel capitolo tre, il link fra i Router 2 e 3 consiste in un doppio collegamento Ethernet-PPPoE. La priorità delle rotte definite sui due Router dovrebbe fare in modo che se si dovesse verificare un guasto sulla linea Ethernet principale, il link PPPoE dovrà iniziare a far fluire il traffico, permettendo agli utenti di continuare ad usufruire della rete.

Perciò il secondo test effettuato per quanto riguarda la robustezza della rete, è stato proprio quello di verificare se la connettività fosse garantita anche dopo un malfunzionamento della linea Ethernet fra AR2 e AR3.

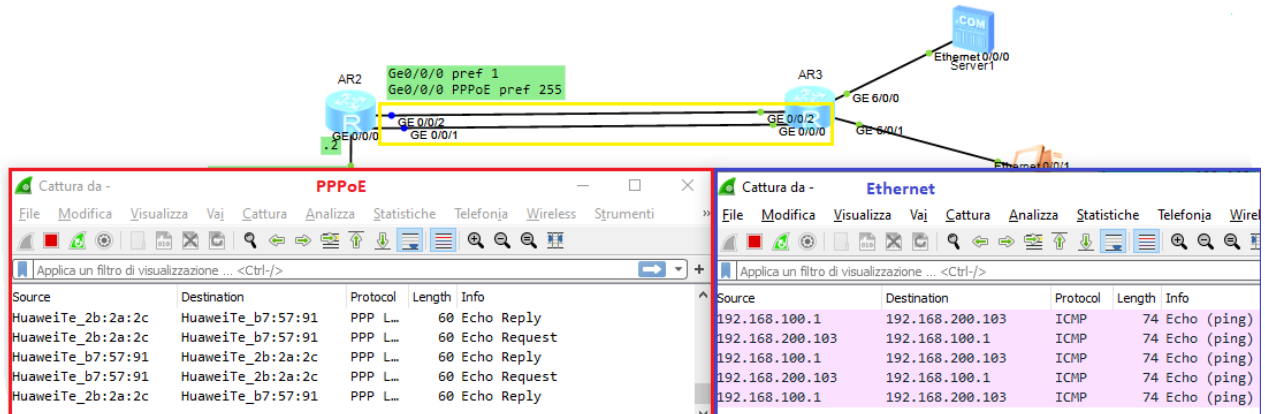


Figura 4.17: Traffico sul link AR2-AR3.

Come si può vedere nella figura 4.17, tutto il traffico, in situazioni di normale funzionamento, viene gestito dalla linea Ethernet.

Infatti eseguendo un ping fra le due LAN ci accorgiamo subito che tutti i pacchetti viaggiano su questo link (In blu nella figura).

Per simulare il guasto è bastato interrompere il collegamento Ethernet lanciando il comando *shut* su una delle due interfacce ai suoi capi.

A questo punto l'unica linea di collegamento fra AR2 e AR3 resta quella PPPoE e perciò è lì che sarà indirizzato il traffico (Figura 4.18).

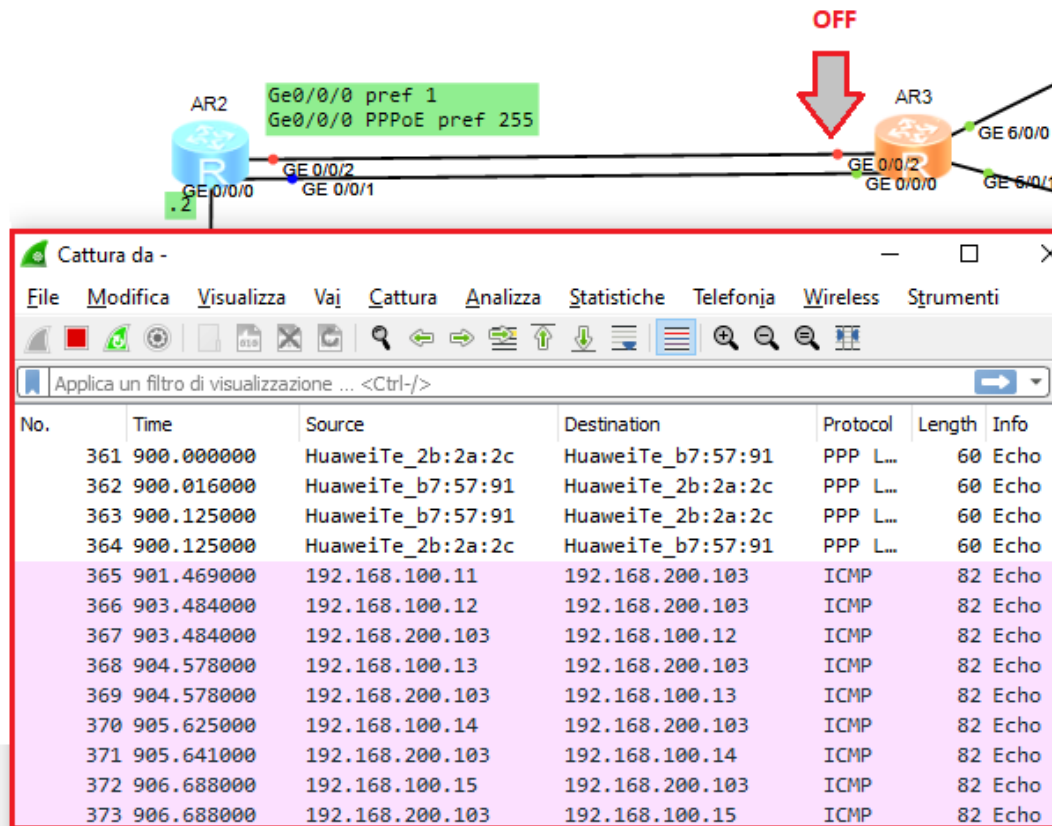


Figura 4.18: Traffico sul link PPPoE.

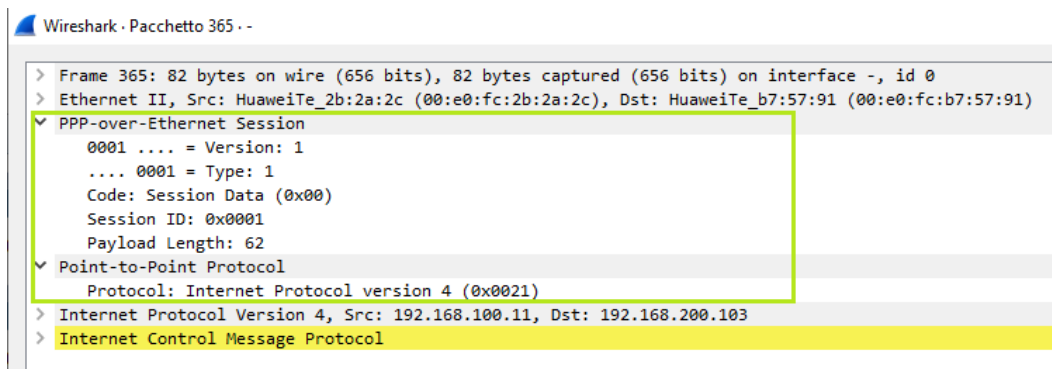


Figura 4.19: Incapsulamento operato dal PPPoE sul pacchetto ICMP.

4.3 Note sulle prestazioni

Durante lo svolgimento dei vari test, nello specifico quelli che includevano un ping dalla Vlan 20 al PC4, è stata notata una percentuale di **Packet-Loss** non indifferente.

Il problema sembra affliggere il link che collega il Router 2 al Router 3, ma la sua origine mi resta incompresa. La mole di pacchetti persi non rimane neanche su un valore costante, ma, al contrario, varia notevolmente.

Su un campione di 30 ping effettuati la percentuale di packet-loss media risulta pari al 34%.

```

PC>ping 192.168.200.103

Ping 192.168.200.103: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
From 192.168.200.103: bytes=32 seq=3 ttl=125 time=94 ms
From 192.168.200.103: bytes=32 seq=4 ttl=125 time=62 ms      40% P-L
From 192.168.200.103: bytes=32 seq=5 ttl=125 time=78 ms

--- 192.168.200.103 ping statistics ---
 5 packet(s) transmitted
 3 packet(s) received
40.00% packet loss
 round-trip min/avg/max = 0/78/94 ms

PC>ping 192.168.200.103

Ping 192.168.200.103: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
From 192.168.200.103: bytes=32 seq=5 ttl=125 time=79 ms      80% P-L

--- 192.168.200.103 ping statistics ---
 5 packet(s) transmitted
 1 packet(s) received
80.00% packet loss
 round-trip min/avg/max = 0/79/79 ms

PC>ping 192.168.200.103

Ping 192.168.200.103: 32 data bytes, Press Ctrl_C to break
From 192.168.200.103: bytes=32 seq=1 ttl=125 time=93 ms
From 192.168.200.103: bytes=32 seq=2 ttl=125 time=63 ms      20% P-L
From 192.168.200.103: bytes=32 seq=3 ttl=125 time=78 ms
From 192.168.200.103: bytes=32 seq=4 ttl=125 time=78 ms
Request timeout!

--- 192.168.200.103 ping statistics ---

```

Figura 4.20: Packet-Loss fra AR2 e AR3.

Capitolo 5

Note e Conclusioni

5.1 Note finali

Il progetto terminato rappresenta una topologia di rete ben configurata e funzionante.

Oltre al problema legato al packet-loss fra AR2 e AR3, i test effettuati non hanno rivelato nessun errore commesso nelle fasi di progettazione e per questo posso definire il progetto completato con successo.

Tutte le specifiche sono state rispettate e, come è osservato, la topologia presenta anche un buon grado di robustezza ai guasti.

L'unico anello debole della rete è rappresentato dal collegamento fra AR1 e AR2; quest'ultimo non presenta nessun meccanismo di recupero per fronteggiare un'eventuale interruzione del link, la quale di fatto andrebbe a rendere impossibile la comunicazione fra le due LAN collegate dai Router.

Un ultimo appunto sulla configurazione realizzata riguarda l'utilizzo di rotte statiche per l'instradamento dei pacchetti da parte dei tre Router; Nonostante questa sia una soluzione semplice e sicura, la definizione e l'aggiornamento delle Routing table di AR1, AR2 e AR3 sarebbero potuti essere gestiti in maniera dinamica, andando ad utilizzare il protocollo **OSPF**.

5.2 Conclusioni

Questo progetto in sé, è stato molto utile per andare a collegare ancor di più tutti gli argomenti che, durante il corso HAINA, sono stati affrontati in maniera più separata.

Portare a termine la configurazione ha richiesto una buona capacità di problem-solving e l'essere in grado di tradurre nella pratica le tematiche affrontate durante le lezioni teoriche; detto ciò reputo molto ben bilanciato il grado di difficoltà della consegna. Guardando indietro, se dovessi descrivere il progetto, lo definirei come una perfetta conclusione per il corso HAINA.

Quest'ultimo ci ha fornito una base solidissima per quanto riguarda il mondo del networking, una base che sarà fondamentale se, in futuro, qualcuno di noi dovesse decidere di approfondire queste tematiche con ulteriori studi.

Ringraziamenti

Le prime persone che mi sento di menzionare sono il mio relatore Gambi Ennio e correlatore Desantis Adelmo, i quali sono stati sempre davvero disponibili per ogni chiarimento in merito al progetto sviluppato.

Un ringraziamento particolare va anche alla mia famiglia, che mi ha aiutato e supportato dall'inizio alla fine del mio percorso di studi.

Mi sento anche in dovere di ringraziare i miei compagni di corso ed amici di tutti i giorni, i quali hanno reso questi tre anni di università veramente indimenticabili...

Ancona, Settembre 2021

Bedetta Alessandro

